KACE® Systemverwaltungs-Appliance 12.0

Administratorhandbuch

Inhaltsverzeichnis

Informationen zur KACE Systemverwaltungs-Appliance ... 28
Informationen zu Appliance-Komponenten ... 28
Informationen zur Administratorkonsole ... 30
Im Administratormodus ohne die Organisationskomponente verfügbare Komponenten ... 34
Im Administratormodus mit aktivierter Organisationskomponente verfügbare Komponenten ... 38
Im Systemmodus mit aktivierter Organisationskomponente verfügbare Komponenten ... 40
Verwenden der Komponente "Startseite" ... 41
Informationen zu Dashboards ... 41
Dashboard im Administratormodus anzeigen ... 42
Dashboard im Systemmodus anzeigen ... 42
Dashboard-Seiten anpassen ... 43
Informationen zu Dashboard-Widgets ... 44
Dashboard-Details anzeigen ... 57
Aufgabenpläne anzeigen ... 59
Version, Modell und Lizenzinformationen der Appliance anzeigen ... 59
Produktlizenzinformationen anzeigen ... 61
Informationen zum Aktualisieren der Appliance-Software ... 62
Informationen zu den Labels ... 62
Suchen nach Informationen und Filtern von Listen ... 63
Auf Administratorebene suchen ... 63
Auf Seitenebene suchen ... 64
Auf Seitenebene mit erweiterten Optionen suchen ... 64
Benutzerdefinierter Ansichten mithilfe von Kriterien für die Erweiterte Suche erstellen ... 67
Zugreifen auf die Produktdokumentation ... 68
Melden Sie sich bei der Administratorkonsole an: Erste Anmeldung nach der Erstkonfiguration des Netzwerks ... 71
Erste Schritte ... 74
Konfigurieren der Appliance ... 74
Anforderungen und Spezifikationen ... 74
Einschalten der Appliance und Anmelden bei der Administratorkonsole ... 74
Zugriff auf die Befehlszeilenkonsole ... 77
Verfolgen von Konfigurationsänderungen ... 78
Konfigurieren der allgemeinen Einstellungen auf System- und Verwaltungsebene ... 78
Allgemeine Appliance-Einstellungen bei aktivierter Organisationskomponente konfigurieren ... 78

Allgemeine Einstellungen auf Verwaltungs- oder organisationsspezifischer Ebene konfigurieren... 85
Allgemeine Appliance-Einstellungen ohne aktivierte Organisationskomponente konfigurieren... 91
Konfigurieren der Datum- und Uhrzeiteinstellungen der Appliance... 100
Zweifaktor-Authentifizierung für alle Benutzer aktivieren... 101
Überprüfen von Port-Einstellungen, NTP-Dienst und Website-Zugriff... 102
Porteinstellungen überprüfen... 102
Status des NTP-Dienstes überprüfen... 104
Erforderliche Websites für die Appliance verfügbar machen... 104
Konfigurieren von Netzwerk- und Sicherheitseinstellungen... 105
Netzwerkeinstellungen der Appliance ändern... 105
Lokale Routing-Tabellen konfigurieren... 109
Lokale Webservereinstellungen konfigurieren und Zugriff auf Hosts zulassen... 109
Sicherheitseinstellungen für die Appliance konfigurieren... 111
Active Directory als Methode für das einmalige Anmelden konfigurieren... 120
SSL-Zertifikate generieren... 122
Konfigurieren der Agenten-Einstellungen... 123
Informationen zu Konea... 123
Agenten-Einstellungen konfigurieren... 123
Konfigurieren der Einstellungen für Sitzungs-Timeout und automatische Aktualisierung... 125
Sitzungs-Timeouts festlegen... 125
Automatische Aktualisierung festlegen... 126
Konfigurieren der Gebietsschema-Einstellungen... 127
So werden Gebietsschema-Einstellungen angewendet:... 127
Gebietsschema-Einstellungen für die Administratorkonsole und die Befehlszeilenkonsole konfigurieren... 127
Konfigurieren von Gebietsschema-Einstellungen für die Benutzerkonsole... 128
Gebietsschema-Einstellungen für Organisationen konfigurieren... 129
Gebietsschema-Einstellungen für Benutzer konfigurieren... 130
Konfigurieren des Standard-Designs... 130
Ändern des Standard-Designs für die Appliance... 131
Konfigurieren des Standard-Designs für einen Benutzer... 131
Konfigurieren der Datenfreigabeeinstellungen... 132
Informationen zu den DIACAP-Compliance-Anforderungen... 133
Nutzungsrichtlinie aktivieren bzw. deaktivieren... 134
Konfigurieren des Mobilgerätezugriffs... 134
Mobilgerätezugriff für die Appliance aktivieren... 135
Mobilgerätezugriff für Benutzer aktivieren... 136

KACE GO herunterladen und verwenden....136
Mobilgerätezugriff auf der Appliance deaktivieren....137
Mobilgerätezugriff für Benutzer deaktivieren....137
Schnellen Wechsel von Organisationen und verknüpften Appliance aktivieren....138
Verknüpfen von Quest KACE Appliances....139
Appliance-Verknüpfung aktivieren....139
Namen und Schlüssel zu Appliances hinzufügen....140
Den Zugriff auf Federation-API-Einstellungen aktivieren....141
Appliance-Verknüpfungen deaktivieren....141
Konfigurieren der Verlaufseinstellungen....142
Informationen zu den Verlaufseinstellungen....142
Verwalten des Einstellungsverlaufs....142
Asset-Verlauf verwalten....144
Objektverlauf verwalten....145
Änderungsverlaufsinformationen verwenden....146
Einrichten und Verwenden von Labels für die Verwaltung von Elementgruppen....148
Informationen zu den Labels....148
Informationen zu Smart Labels....148
Informationen zu LDAP-Labels....149
Informationen zu Labelgruppen....149
Informationen zu Organisationsfiltern....149
Verfolgen von Änderungen an Labeleinstellungen....150
Verwalten manueller Labels....150
Manuelle Labels hinzufügen oder bearbeiten....150
Details zu manuellen Labels anzeigen....152
Manuelle Labels löschen....152
Verwalten von Smart Labels....153
Smart Labels hinzufügen....153
Beispiel: Smart Labels zum Identifizieren von Geräten kombinieren....154
Smart Labels bearbeiten....155
Labels für Benutzerkonten festlegen....156
Smart Labels für Patches verwenden....157
Smart Labels für Erkennungsergebnisse verwenden....160
Smart Labels für Geräte hinzufügen....161
Ausführungsreihenfolge von Smart Labels zuweisen....165
Smart Labels löschen....166
Verwalten von Labelgruppen....166
Labelgruppen hinzufügen, anzeigen oder bearbeiten....166

Label Labelgruppen zuweisen bzw. Labels von Labelgruppen entfernen..... 168
Labelgruppen löschen..... 168
Verwalten von LDAP-Labels..... 169
LDAP-Label hinzufügen oder bearbeiten..... 169
LDAP-Label aktivieren..... 171
LDAP-Label löschen..... 172
LDAP-Browser verwenden..... 172
Konfigurieren von Benutzerkonten, LDAP-Authentifizierung und SSO..... 174
Informationen zu Benutzerkonten und Benutzerauthentifizierung..... 174
Informationen zu Gebietsschema-Einstellungen..... 174
Verwalten von Benutzerkonten auf Systemebene..... 175
Benutzerkonten auf Systemebene hinzufügen oder bearbeiten..... 175
E-Mail-Benachrichtigungen des Appliance-Administrators verwalten..... 178
Benutzerkonten auf Systemebene löschen..... 179
Verwalten von Organisationsbenutzerkonten..... 179
Benutzerrollen hinzufügen oder bearbeiten..... 179
Benutzerrollen löschen..... 180
Organisationsbenutzerkonten hinzufügen oder bearbeiten..... 181
Benutzerinformationen anpassen..... 183
Benutzerkonten archivieren..... 184
Anzeigen oder Bearbeiten von Benutzerprofilen..... 185
Verwenden eines LDAP-Servers zur Benutzerauthentifizierung..... 187
Informationen zum Anmeldekonto für Ihren LDAP-Server..... 187
LDAP-Benutzerauthentifizierung einrichten und testen..... 188
Importieren von Benutzern aus einem LDAP-Server..... 191
Benutzerinformationen manuell importieren..... 191
Benutzerinformationen nach einem Zeitplan importieren..... 195
Informationen zur einmaligen Anmeldung (SSO)..... 200
Externe LDAP- oder Active Directory-Server für die einmalige Anmeldung verwenden..... 201
Aktivieren und Deaktivieren der einmaligen Anmeldung..... 201
Einmalige Anmeldung aktivieren..... 201
Einmalige Anmeldung deaktivieren..... 202
Verwenden von Active Directory für die einmalige Anmeldung..... 202
Active Directory als Methode für das einmalige Anmelden konfigurieren..... 202
Browsereinstellungen für die einmalige Anmeldung konfigurieren..... 204
Domänenbeitritt rückgängig machen und einmalige Anmeldung für Active Directory deaktivieren..... 206
SAML für die einmalige Anmeldung konfigurieren..... 206

Beispiel: Verwenden von Microsoft Active Directory in Azure als SAML Identity Provider....208
Bereitstellen des KACE Agent auf verwalteten Geräten....210
Verwenden von Replikationsfreigaben....211
Replikationsfreigaben erstellen....212
Details zu Replikationsfreigaben anzeigen....215
Verwalten von Anmeldeinformationen....216
Verfolgen von Änderungen in der Verwaltung der Anmeldeinformationen....216
Geheimschlüssel-Anmeldeinformationen hinzufügen und bearbeiten....216
Hinzufügen und Bearbeiten von Benutzer-/Kennwort-Anmeldeinformationen....218
Hinzufügen und Bearbeiten von LDAP-Benutzer-/Kennwort-Anmeldeinformationen....219
Hinzufügen und Bearbeiten von Google OAuth-Anmeldeinformationen....221
Hinzufügen und Bearbeiten von SNMP-Anmeldeinformationen....223
Microsoft Office 365 OAuth-Anmeldeinformationen hinzufügen und bearbeiten....225
Anzeigen der Nutzung der Anmeldeinformationen....228
Erstellen von Berichten aus der Liste "Verwaltung der Anmeldeinformationen"....229
Exportieren von Anmeldeinformationen....229
Löschen von Anmeldeinformationen....230
Konfigurieren von Assets....230
Informationen zur Komponente Asset Management....230
Das Asset Management-Dashboard verwenden....231
Informationen zu den Asset Management-Widgets im Dashboard....231
Das Asset Management-Dashboard anpassen....234
Informationen zum Verwalten von Assets....235
Unterschiede zwischen Asset- und Inventarinformationen....235
Nachzuverfolgende Assets festlegen....236
Assets anzeigen und nach Asset-Informationen suchen....236
Barcodes zu Assets hinzufügen....237
Gerätebesitzer ändern....238
Asset-Lebenszyklus-Einstellungen anzeigen und konfigurieren....238
Hinzufügen und Anpassen von Asset-Typen und Verwalten von Asset-Informationen....240
Informationen zu Asset-Typen....240
Asset-Typen anpassen....240
Informationen zu Asset-Untertypen, benutzerdefinierten Feldern und Gerätedetail-Voreinstellungen....248
Verwalten von Software-Assets....257
Software-Asset-Typ anpassen....257
Software-Assets hinzufügen....257
Verwalten physischer und logischer Assets....260

Physische Asset-Typen hinzufügen.....260
Gerätebestände archivieren.....262
Verwalten und Verwenden von manuellen Asset-Informationen.....263
Standorte verwalten.....264
Standorte verwalten.....264
Standorte hinzufügen oder bearbeiten.....265
Speicherortfelder anpassen.....266
Verwalten von Verträgen.....269
Verträge verwalten.....269
Verträge hinzufügen oder bearbeiten.....270
Verwalten von Lizenzen.....273
Lizenzen verwalten.....273
Lizenzen hinzufügen oder bearbeiten.....274
Kaufdatensätze verwalten.....280
Kaufdatensätze verwalten.....280
Kaufdatensätze hinzufügen oder bearbeiten.....281
Einrichten der Lizenz-Compliance.....284
Informationen zur Lizenz-Compliance für Anwendungen im Softwarekatalog.....284
Informationen zu Lizenz-Upgrades.....285
Informationen zu Lizenz-Downgrades.....285
Anpassen des Lizenz-Asset-Typs.....285
Hinzufügen von Lizenz-Assets für das Softwarekataloginventar.....287
Hinzufügen von Lizenz-Assets für das Inventar der Seite "Software".....293
Importieren von Lizenzdaten in CSV-Dateien.....300
Behandlung von Asset-Informationen während des Imports.....300
Asset-Daten mithilfe von CSV-Dateien importieren.....300
Verwalten der Lizenz-Compliance.....306
Anzeigen von Informationen zur Lizenz-Compliance für Anwendungen im Softwarekatalog.....306
Rückgewinnen ungenutzter Softwarelizenzen.....309
Manuelle Aktualisierung der Softwarelizenz-Compliance-Informationen.....309
Konfigurieren von Warnungsschwellenwerten für die Lizenznutzung.....310
Anzeigen von Informationen zur Lizenz-Compliance und -Konfiguration.....311
Einrichten des Service Desks.....312
Einrichten von Rollen für Benutzerkonten.....312
Informationen zu Standardrollen.....312
Rolle für Service Desk-Mitarbeiter erstellen.....314
Benutzerrollen zuweisen.....315
Labels und Rollen auf Service Desk-Mitarbeiter anwenden.....316

Konto "DefaultTicketOwners" erstellen... 317
Konfigurieren der E-Mail-Einstellungen... 318
Informationen zu E-Mail-Benachrichtigungen... 318
Informationen zu Ticketregeln... 319
Informationen zu POP3-E-Mail-Konten... 319
POP3-E-Mail-Konten erstellen und konfigurieren... 319
E-Mail-Voreinstellungen konfigurieren... 320
E-Mail-Auslöser und E-Mail-Vorlagen konfigurieren... 321
CC-Listen für Ticketkategorien konfigurieren... 332
E-Mail-Adressen automatisch zu Ticket-CC-Listenfeldern hinzufügen... 332
Adressen aus Ticket-CC-Listenfeldern ausschließen... 333
Verhindern von E-Mail-Schleifen... 334
Konfigurieren der Cache-Lebensdauer für Service Desk-Widgets... 335
Erstellen und Verwalten von Organisationen... 335
Informationen zu Organisationen... 336
Informationen zur Standardorganisation... 336
Verfolgen von Änderungen an Organisationseinstellungen... 336
Verwalten von Organisationsrollen und Benutzerrollen... 336
Verfügbare Standardrollen... 337
Organisationsrollen hinzufügen und bearbeiten... 338
Organisationsrollen duplizieren... 339
Rollen löschen... 340
Hinzufügen, Bearbeiten und Löschen von Organisationen... 340
Organisationen hinzufügen oder bearbeiten... 341
Zweifaktor-Authentifizierung für Organisationen konfigurieren... 349
Organisationen löschen... 350
Für die Benutzerkonsole und Organisationsberichte verwendete Logos anpassen... 350
Verwalten von Benutzerkonten für Organisationen... 350
Verwalten von Organisationsfiltern... 351
So funktionieren Organisationsfilter:... 351
Datenfilter für Organisationen hinzufügen oder bearbeiten... 352
LDAP-Filter für Organisationen hinzufügen oder bearbeiten... 353
Organisationsfilter testen... 355
Organisationsfilter löschen... 355
Verwalten von Geräten in Organisationen... 355
Verwenden der erweiterten Suche... 356
Geräte filtern... 356
Geräte umleiten... 356

Informationen zu Gerätedetails....356
Ausführen von Berichten für Einzelorganisationen sowie von konsolidierten Berichten....357
Importieren und Exportieren von Appliance-Ressourcen....357
Informationen zum Importieren und Exportieren von Anwendungsressourcen....357
Übertragen von Ressourcen zwischen Appliances mithilfe von Samba Freigabeverzeichnissen....358
Ressourcen aus einer Appliance exportieren....358
Ressourcen in eine Appliance importieren....359
Übertragen von Ressourcen zwischen Organisationen....359
Ressourcen aus Organisationen exportieren....360
Ressourcen in Organisationen importieren....360
Verwalten exportierter Ressourcen auf Systemebene....361
Freigegebene Ressourcen anzeigen oder löschen....361
Freigegebene Ressourcen von der lokalen Appliance in Netzwerkstandorte verschieben....361
Status von Ressourcenexporten anzeigen oder löschen....361
Verwalten des Inventars....363
Verwenden des Bestandsaufnahme-Dashboards....363
Informationen über die Bestandsaufnahme-Dashboard-Widgets....363
Dashboard „Bestand“ anpassen....366
Verwenden der Geräteerkennung....366
Informationen zu Geräteerkennung und -verwaltung....366
Nachverfolgen von Änderungen an Erkennungseinstellungen....367
Erkennen von Geräten im Netzwerk....367
Erkennungszeitplan für die Durchführung eines schnellen „Was und wo“-Scans in Ihrem Netzwerk hinzufügen....368
Erkennungszeitplan für einen umfassenden Scan von verwalteten Windows, Mac, Linux und UNIX Computern hinzufügen....382
Client-ID und geheimen Client-Schlüssel für die Erkennung von Chrome-Geräten abrufen....388
Hinzufügen eines Erkennungszeitplans für ein KACE Cloud Mobile Device Manager-Gerät....389
Erkennungszeitplan für ein G-Suite-Gerät hinzufügen....392
Erkennungszeitplan für ein Workspace ONE-Gerät hinzufügen....395
Hinzufügen eines Erkennungszeitplans für einen VMware ESXi-Host oder vCenter-Server....398
Erkennungszeitplan für Microsoft Hyper-V oder System Center Virtual Machine Manager hinzufügen....401
Zugangsdatenanforderungen für System Center Virtual Machine Manager....404
Hinzufügen eines Erkennungszeitplans für SNMP-fähige computerfremde Geräte....404
Informationen zu Erkennungsergebnissen....409

Erkennungsergebnisse anzeigen und durchsuchen.....409
Agent über die erkannte IP-Adresse oder den erkannten Hostnamen provisionieren.....410
Laufenden Erkennungsscan anhalten.....410
Erkennungszeitpläne löschen.....411
Verwalten des Geräteinventars.....411
Informationen zur Geräteverwaltung.....411
Funktionen, die für jede einzelne Geräteverwaltungsmethode zur Verfügung stehen.....412
Informationen zu Inventarinformationen.....429
Erfassen von Änderungen an Inventareinstellungen.....429
Verwalten von Inventarinformationen.....430
Benutzerdefinierte Datenfelder hinzufügen.....430
Inventardatensammlung für verwaltete Geräte planen.....431
Geräteinventar und Details anzeigen.....433
Informationen zu Geräten anzeigen, die bei KACE Cloud MDM registriert sind.....434
Elementegruppen und -abschnitte in Gerätedetails.....435
Informationen zu Dell Data Protection | Encryption (DDP|E) und Verschlüsselungsinformationen in Gerätedetails.....479
Dump Inventory-Registrierungsschlüssel zur Inventarerfassung von Windows DDP|E-Client-Geräten hinzufügen.....485
Informationen zu Intel AMT in Gerätedetails.....490
Suchen und Verwalten von Geräten.....491
Suche nach Geräten im Inventar.....491
Geräte mithilfe von Labels gruppieren.....492
Aktionen auf Geräten ausführen.....493
Manuell hinzugefügte Geräte anzeigen.....494
Geräte aus dem Inventar löschen.....495
Registrieren des KACE Agent bei der Appliance.....495
Verwalten von KACE Agent-Token.....495
In Quarantäne befindliche KACE Agenten überprüfen.....497
Provisionierung des KACE Agent.....499
Dateifreigabe aktivieren.....500
KACE Agent mithilfe des Tools für die Gruppenrichtlinienobjekt-Agenten-Provisionierung für Windows Geräte bereitstellen.....502
KACE Agent mithilfe der integrierten Provisionierung bereitstellen.....504
Provisionierungszeitpläne verwalten.....510
Kommunikation des Agenten verwalten.....513
KACE Agent auf verwalteten Geräten aktualisieren.....521
Manuelle Bereitstellung des KACE Agent.....524
Agenteninstallationsdateien abrufen.....525

KACE Agent auf Windows-Geräten manuell bereitstellen.....525
KACE Agent auf Linux-Geräten manuell bereitstellen und aktualisieren.....529
Agentenvorgänge auf Linux Geräten ausführen.....531
KACE Agent auf Mac-Geräten manuell bereitstellen und aktualisieren.....532
Andere Agenten-Vorgänge auf Mac Geräten ausführen.....534
Vom Agenten gesammelte Informationen anzeigen.....536
Verwenden der Verwaltung ohne Agent.....536
Informationen zur Verwaltung ohne Agent.....536
Geräte ohne Agent verwalten.....537
Erkennen bestimmter, dem Inventar hinzuzufügender SNMP-Objekte und Nicht-Computer-Geräte mithilfe von SNMP-Inventarkonfigurationen.....547
Manuelles Hinzufügen von Geräten in der Administratorkonsole oder mithilfe der API.....551
Informationen zur Geräteverwaltung.....551
Erfassen von Änderungen an Inventareinstellungen.....551
Geräte mit der Administratorkonsole manuell hinzufügen.....552
Geräte mithilfe der API manuell hinzufügen.....556
Erzwingen von Inventaraktualisierungen.....564
Inventaraktualisierungen von der Appliance erzwingen.....565
Inventaraktualisierungen von Windows-Geräten erzwingen.....565
Inventaraktualisierungen von Mac OS X Geräten erzwingen.....566
Inventaraktualisierungen von unter Linux laufenden Geräten erzwingen.....566
Verwalten ausstehender Geräte.....566
Einstellungen ausstehender Geräte konfigurieren.....566
Labels ausstehenden Geräten zuweisen.....567
Ausstehende Geräte manuell löschen.....568
Fehler beheben an Geräten, die nicht im Inventar angezeigt werden.....568
Abrufen von Informationen zum Service von Dell.....570
Sofortiges Abrufen von Informationen zum Service von Dell für ein einzelnes Gerät von Dell.....570
Services von Dell erneuern.....571
Berichte über den Service von Dell ausführen.....571
Verwalten von Anwendungen auf der Seite "Software".....571
Informationen zur Seite "Software".....571
Elemente im Inventar der Seite "Software" anzeigen.....572
Erfassen von Änderungen an Inventareinstellungen.....572
Hinzufügen und Löschen von Anwendungen im Inventar der Seite "Software".....572
Anwendungen manuell dem Inventar der Seite "Software" hinzufügen.....572
Anwendungen löschen.....574
Erstellen von Software-Assets.....575

Software-Assets im Abschnitt "Inventar" hinzufügen..... 575
Software-Assets im Abschnitt "Assets" hinzufügen..... 575
Digitale Assets an Anwendungen anhängen und unterstützte Betriebssysteme auswählen..... 576
Dateien kopieren und auf dem Client-Drop-Speicherort der Appliance ablegen.....577
Verwenden von Bedrohungsstufen und Kategorien für Software.....578
Anwendungen Bedrohungsstufen zuweisen..... 578
Anwendungen Kategorien zuweisen.....579
Auffinden und Labeling von Anwendungen..... 579
Informationen zum Auffinden von Anwendungen mithilfe der erweiterten Suche..... 579
Manuelle Softwarelabels hinzufügen..... 579
Manuelle Labels zuweisen oder Labels von Software entfernen.....580
Smart Labels für Software erstellen.....580
Verwalten des ITNinja-Feed..... 581
ITNinja-Feed aktivieren..... 582
ITNinja-Informationen anzeigen..... 582
ITNinja-Feed deaktivieren..... 583
Verwalten des Softwarekataloginventars.....583
Informationen zum Softwarekatalog..... 584
Anwendungsklassifizierungen..... 584
Informationen zu katalogisierten Anwendungen..... 585
Informationen zu lokal katalogisierten Anwendungen.....585
Informationen zu nicht zulässigen Anwendungen.....585
Anwendungskategorien..... 585
Informationen zur Erfassung von Softwarekataloginformationen.....585
Informationen zur Verwendung des Softwarekatalogs mit der Organisationskomponente..... 586
Informationen zur Lokalisierung von Softwarekataloginformationen.....586
Informationen dazu, wie Sie helfen können, den Softwarekatalog zu verbessern..... 586
Unterschiede zwischen den Seiten "Software" und "Softwarekatalog".....586
Anzeigen von Informationen im Softwarekatalog..... 588
Listen von erkannten und nicht erkannten Anwendungen anzeigen..... 589
Liste der nicht katalogisierten Anwendungen anzeigen.....590
Liste der lokal katalogisierten Anwendungen anzeigen.....591
Details zu Anwendungen im Softwarekatalog anzeigen.....592
Hinzufügen von Anwendungen zum Softwarekatalog..... 597
Beim Senden von Katalogisierungsanforderungen werden die Anwendungen automatisch zum lokalen Softwarekatalog hinzugefügt..... 597
So werden lokal katalogisierte Anwendungen zu katalogisierten Anwendungen.....597

Informationen zur Auflösung von benutzerdefinierten Namen beim Hinzufügen von lokal katalogisierten Anwendungen zum Softwarekatalog....598
Katalogisierungsanforderungen senden....598
Katalogisierungsanforderungen stornieren und lokale Katalogisierungen entfernen... 600
Verwalten von Lizenz-Assets für Anwendungen im Softwarekatalog....600
Hinzufügen von Lizenz-Assets für das Softwarekataloginventar.... 601
Lizenz-Assets zu Anwendungen im Softwarekatalog migrieren.... 607
Verknüpfen verwalteter Installationen mit katalogisierter Software.... 608
Verwenden der Erfassung der Softwarenutzung....608
Informationen zur Erfassung der Softwarenutzung....608
Informationen zu Erfassungsinformationen....609
Erfassung von Geräten und Anwendungen aktivieren und konfigurieren.... 610
Softwarekatalog-Erfassungsinformationen anzeigen.... 616
Erfassung von Anwendungen im Softwarekatalog sowie verwalteten Geräten deaktivieren....619
Nutzungserfassung verwalten und Inventarerfassung planen.... 620
Verwenden der Anwendungssteuerung....621
Voraussetzungen für das Blockieren von Anwendungen.... 622
Vorgehensweise zur Blockierung von Anwendungen....622
Informationen zum Blockieren von Anwendungseditionen, die ausführbare Dateien gemeinsam nutzen.... 622
Anwendungen, die nicht blockiert werden können.... 622
Anwendungssteuerungslabel zu Geräten zuweisen.... 623
Anwendungen und Suites als "Nicht zulässig" kennzeichnen.... 623
Anwendungen und Suites anzeigen, die als "Nicht zulässig" gekennzeichnet sind..... 624
Berichte mit als "Nicht zulässig" gekennzeichneten Anwendungen erstellen.... 624
Kennzeichnung "Nicht zulässig" von Anwendungen entfernen....625
Softwarekatalog aktualisieren oder neu installieren.... 626
Verwalten des Prozess-, Startprogramm- und Dienstinventars.... 627
Verwalten des Prozessinventars....627
Prozessdetails anzeigen und bearbeiten.... 627
Labels für Prozesse hinzufügen....628
Prozessen Labels zuweisen oder Labels aus Prozessen entfernen....628
Prozesse kategorisieren....629
Prozessen Bedrohungsstufen zuweisen.... 629
Prozesse löschen.... 629
Verwalten des Startprogramm-Inventars.... 630
Startprogrammdetails anzeigen und bearbeiten.... 630
Labels Startprogrammen hinzufügen.... 630

Startprogrammen Labels zuweisen oder Labels aus Startprogrammen entfernen..... 631
Startprogramme kategorisieren..... 631
Bedrohungsstufen Startprogrammen zuweisen..... 631
Startprogramme löschen..... 632
Verwalten des Dienstinventars..... 632
Dienstdetails anzeigen und bearbeiten..... 632
Labels Diensten hinzufügen..... 633
Diensten Labels zuweisen oder Labels aus Diensten entfernen..... 633
Dienste kategorisieren..... 634
Bedrohungsstufen Diensten zuweisen..... 634
Dienste löschen..... 634
Erstellen benutzerdefinierter Inventarregeln..... 635
Informationen zu benutzerdefinierten Inventarregeln..... 635
Arten von benutzerdefinierten Inventarregeln..... 635
Regeln für benutzerdefinierte Inventarisierung erstellen..... 636
Regeln für benutzerdefinierte Inventarisierung implementieren..... 637
Syntax für Regeln für benutzerdefinierte Inventarisierung..... 638
Überprüfen von Bedingungen (Bedingungsregeln)..... 639
Abrufen von Werten von einem Gerät (Benutzerdefiniertes Inventarfeld)..... 648
Zuordnen von Dateinamen zu regulären Ausdrücken..... 651
Die regulären Ausdrücke..... 652
Referenz zu Regeln mit regulären Ausdrücken..... 654
Definieren von Regelargumenten..... 655
Benutzerdefinierte Inventarregeln testen..... 660
Bereitstellen von Paketen auf verwalteten Geräten..... 661
Verteilen von Software und Verwenden von Wake on LAN..... 661
Informationen zur Softwareverteilung..... 661
Informationen zum Testen der Softwareverteilung..... 662
Nachverfolgen von Änderungen der Verteilungseinstellungen..... 663
Arten von Verteilungspaketen..... 663
Digitale Assets an Anwendungen anhängen und unterstützte Betriebssysteme auswählen..... 663
Verteilen von Paketen aus der Appliance..... 663
Verteilen von Paketen über alternative Download-Quellen und Replikationsfreigaben..... 664
Informationen zu alternativen Download-Quellen..... 664
Informationen zu Replikationsfreigaben..... 664
Verteilen von Software auf Mac OS X Geräten..... 664
Verwenden verwalteter Installationen..... 665
Anwendungen zum Inventar hinzufügen..... 665

Informationen zu verwalteten Installationen....666
Informationen zu Installationsparametern....666
Von Installationsprogrammdateien unterstützte Parameter identifizieren....667
Verwaltete Installationen für Windows Geräte erstellen....667
Beispiele für gängige Bereitstellungen unter Windows....673
Verwaltete Installationen für ZIP-Dateien erstellen....674
Verwaltete Installationen für RPM-Dateien erstellen....675
Verwaltete Installationen für TAR.GZ-Dateien erstellen....682
Verwaltete Installationen für Mac OS X Geräte erstellen....683
Dateisynchronisierungen erstellen und verwenden....689
Verwenden von Wake on LAN....692
Wake on LAN-Anforderungen ausgeben....692
Wake on LAN-Anforderungen planen....693
Fehlerbehebung bei Wake on LAN....696
Exportieren von verwalteten Installationen....696
Senden von Warnungen an verwaltete Geräte....696
Zu sendende Warnungen erstellen....696
Ausführen von Skripten auf verwalteten Geräten....699
Informationen zu Skripten....699
Skriptabhängigkeiten abrufen....700
Änderungsnachverfolgung für Skripteinstellungen....701
Informationen zu Standardskripten....701
Hinzufügen und Bearbeiten von Skripten....703
Token-Ersetzungsvariablen....703
Offline-KScripts, Online-KScripts oder Online-Shellskripte hinzufügen....705
Skripte bearbeiten....715
Skripte auf der Seite "Skripte" löschen....716
Skripte auf der Seite "Skriptdetail" löschen....716
Struktur für importierbare Skripte....716
Skripte importieren....717
Skripte duplizieren....718
Verwenden der Befehle "Ausführen" und "Jetzt ausführen"....718
Skripte über die Seite "Jetzt ausführen" ausführen....719
Skripte über die Skriptdetailseite ausführen....720
Skripte über die Seite Skripte ausführen....720
Den Status von "Jetzt ausführen" überwachen und Skriptdetails anzeigen....720
Informationen zu den Konfigurationsrichtlinienvorlagen....721
Verwenden der Windows Konfigurationsrichtlinien....722

Informationen zum Starten von automatischen Windows Updates auf Windows-Geräten ... 722
Skripte für automatische Updates hinzufügen ... 723
Informationen zu Dell Command | Monitor ... 724
Dell Command | Monitor-Skripte hinzufügen ... 728
Skripte für Desktop-Hintergrundbild hinzufügen ... 729
Skripte für Desktop-Verknüpfungen hinzufügen ... 730
Ereignisprotokoll-Reporter-Skripte hinzufügen ... 731
MSI-Installationsskripte hinzufügen ... 732
Informationen zur Energieverwaltung und zum Stromverbrauch ... 734
Energieverwaltungsskripte für Windows Geräte hinzufügen ... 734
Registrierungsskripte hinzufügen ... 735
Skripte für die Fehlerbehebung per Remote-Desktop-Steuerung hinzufügen ... 735
UltraVNC-Skripte hinzufügen ... 736
Deinstallationsskripte hinzufügen ... 738
Verwenden der Mac OS X Konfigurationsrichtlinien ... 739
Skripte für Active Directory hinzufügen ... 739
Energieverwaltungsskripte hinzufügen ... 740
VNC-Skripte hinzufügen ... 741
Richtlinien und Skripte bearbeiten ... 742
Die Skriptprotokolle durchsuchen ... 742
Exportieren von Skripten ... 744
Verwalten von Mac Profilen ... 744
Verfolgen von Änderungen an Mac Profileinstellungen ... 744
Hinzufügen, Bearbeiten und Hochladen von Mac Profilen ... 745
Mac Benutzerprofile hinzufügen oder bearbeiten ... 745
Mac Systemprofile hinzufügen oder bearbeiten ... 753
Mac Profile zu vorhandenen Profilen als Vorlage hinzufügen ... 759
Mac Profile in die Appliance hochladen ... 759
Installieren und Verwalten von Mac Profilen ... 760
Mac Profile per Zeitplan verteilen ... 760
Mac Profile auf Geräten mit der Option "Ausführen" installieren ... 762
Geräte mit installierten Mac Profilen identifizieren ... 763
Mac Profile anzeigen ... 763
Mac Profil-Listen exportieren ... 764
Entfernen und Löschen von Mac Profilen ... 765
Mac Profile von verwalteten Geräten entfernen ... 765
Beispiel: Profil entfernen, das für bestimmte Geräte bereitgestellt wurde ... 768
Mac Profile aus der Appliance löschen ... 769

Verwenden von Aufgabenabfolgen....770
Aufgabenabfolgen hinzufügen und bearbeiten....770
Patchen von Geräten und Aufrechterhalten der Sicherheit....774
Verwenden des Sicherheits-Dashboards....774
Informationen über die Sicherheits-Dashboard-Widgets....774
Sicherheits-Dashboard anpassen....777
Informationen zur Patch-Verwaltung....778
Patch-Workflow....778
Informationen zu Patch-Signaturdateien....780
Informationen zu Patch-Paketen....780
Informationen zu Patch-Tests und Sicherheit....780
Informationen zur Patch-Testumgebung....781
Informationen zum Prozess der Patch-Qualitätsprüfung....781
Best Practices für den Patch-Vorgang....782
Abonnieren und Herunterladen von Patches....784
Informationen zu Patch-Abonnements und -Downloads....785
Websites, die für die Appliance zugänglich sein müssen....785
Übersicht über den Workflow beim ersten Patch-Abonnement....788
Details zu Betriebssystemen und Anwendungen anzeigen....788
Abonnieren von Patches und Konfigurieren von Downloadeinstellungen....789
Patches abonnieren....789
Download-Einstellungen für Patch- und Funktionsaktualisierungen auswählen....792
Anzeigen von verfügbaren Patches und Download-Status....796
Verfügbare Patches anzeigen....796
Patch-Download-Status anzeigen....796
Best Practices für die Behebung von Problemen mit Patch-Abonnements....797
Erstellen und Verwalten von Patch-Zeitplänen....799
Informationen zum Planen von kritischen Betriebssystem-Patches für Desktops und Server....799
Workflow für kritische Betriebssystem-Patches für Desktops und Server....799
Informationen zum Planen von kritischen Patches für Notebooks....800
Workflow für kritische Patches für Notebooks....800
Informationen zum Planen von nicht kritischen Patches....800
Konfigurieren von Patch-Zeitplänen....801
Felder auf den Detailseiten des Patch-Zeitplans....801
Konfigurieren von Patch-Zeitplänen....812
Fehlercodes aufgrund von Patching und Skripterstellung....814
Anzeigen von Patch-Zeitplänen, -Status und -Berichten....816
Liste der Patch-Zeitpläne anzeigen....816

Überprüfen von Details zu Patch-Zeitplänen ... 818
Patching-Status-Definitionen ... 824
Patch-Status anzeigen ... 826
Patch-Status nach Gerät anzeigen ... 826
In Patches enthaltene Dateien anzeigen ... 826
Patch-Berichte anzeigen ... 827
Verwalten von Patch-Rollbacks ... 827
Ermitteln, ob für ein Patch ein Rollback möglich ist ... 827
Letzten Patch-Job rückgängig machen ... 828
Verwalten des Patch-Inventars ... 828
Voraussetzungen für die Verwaltung des Patch-Inventars ... 828
Anzeigen von Patch-Informationen ... 828
Heruntergeladene Patches anzeigen ... 829
Patch-Details anzeigen ... 831
Anzahl von Patch-Bereitstellungsversuchen zurücksetzen ... 831
Patch-Informationen für Geräte im Inventar anzeigen ... 832
Geräte mit fehlenden Patches anzeigen ... 833
Anzeigen von statistischen Daten und Protokollen zu Patches ... 833
Statistische Daten zu Patches anzeigen ... 833
Patch-Protokoll anzeigen ... 834
Patches als inaktiv markieren ... 834
Patchen von Mac OS X Geräten ... 834
Windows-Funktionsaktualisierungen verwalten ... 835
Windows-Funktionsaktualisierungen abonnieren ... 835
Zeitpläne für Windows-Funktionsaktualisierungen konfigurieren ... 836
Zeitpläne für Windows-Funktionsaktualisierung anzeigen ... 842
Details zu Windows-Funktionsupdate-Zeitplänen prüfen ... 842
Verfügbare Windows-Funktionsaktualisierungen anzeigen ... 847
Status von Windows-Funktionsupdates anzeigen ... 848
Verwalten von Dell Geräten und Aktualisierungen ... 848
Unterschiede zwischen Patchen und Dell Aktualisierungen ... 849
Download-Einstellungen für Dell Aktualisierung auswählen ... 850
Dell Aktualisierungszeitpläne konfigurieren ... 852
Dell Aktualisierungszeitpläne anzeigen ... 858
Details zum Dell Aktualisierungszeitplan prüfen ... 858
Anzeigen verfügbarer Dell Aktualisierungen ... 862
Anzeigen des Dell Aktualisierungsstatus ... 863
Verwalten von Linux-Paket-Upgrades ... 863

Zeitpläne für Linux-Paket-Upgrades anzeigen..... 864
Konfigurieren der Upgrade-Zeitpläne für Linux-Pakete..... 864
Zeitplandetails der Linux-Paket-Upgrades überprüfen..... 869
Linux-Paket-Upgrades überprüfen..... 871
Aufrechterhalten der Geräte- und Appliance-Sicherheit.....872
Testen der Gerätesicherheit..... 873
Informationen zu OVAL-Sicherheitsprüfungen.....873
Informationen zu OVAL-Tests und -Definitionen..... 873
Informationen zu SCAP.....879
Informationen zu Benchmarks..... 882
Funktionsweise eines SCAP-Scans.....883
SCAP-Scanzeitpläne bearbeiten.....886
Windows Sicherheitsprobleme beheben, die die Agenten-Provisionierung verhindern..... 889
Aufrechterhalten der Appliance-Sicherheit..... 890
Security Run Output (Sicherheitsbericht).....890
Verwenden von Berichten und Zeitplanung für Benachrichtigungen.....891
Informationen zu Berichten und Benachrichtigungen.....891
Informationen zu Berichten.....891
Informationen zu Benachrichtigungen..... 891
Änderungsnachverfolgung für die Berichteinstellungen.....892
Erstellen und Ändern von Berichten.....892
Erstellen von Berichten.....892
Berichte mit dem Berichts-Assistenten erstellen.....892
Berichte mithilfe von SQL-Abfragen erstellen.....895
Berichte über Listenseiten erstellen.....897
Berichte duplizieren.....898
SQL-SELECT-Anweisungen in mit dem Berichts-Assistenten erstellten Berichten bearbeiten..... 898
Berichte aus Verlaufslisten erstellen.....899
Ändern von Berichten..... 899
Berichte bearbeiten..... 899
Berichte löschen.....900
Anpassen von Logos für Berichte..... 900
Planen von Berichten und Benachrichtigungen..... 900
Ausführen von Berichten für Einzelorganisationen sowie von konsolidierten Berichten.....901
Berichte für Einzelorganisationen ausführen..... 901
Konsolidierte Berichte für Organisationen ausführen..... 901
Planen von Berichten.....902

Zeitpläne für Berichte hinzufügen.... 902
Berichtszeitpläne löschen....905
Zeitplanung für Benachrichtigungen.... 905
Benachrichtigungszeitpläne über den Bereich "Berichterstellung" hinzufügen.... 905
Benachrichtigungszeitpläne über Listenseiten hinzufügen.... 907
Benachrichtigungszeitpläne bearbeiten.... 908
Benachrichtigungszeitpläne löschen.... 909
Überwachen von Servern.... 910
Erste Schritte bei der Serverüberwachung.... 912
Überwachung für Geräte aktivieren....912
Überwachung für einen oder mehrere Server über die Geräte-Inventarliste aktivieren....913
Überwachung für einen Server über dessen Gerätedetail-Seite aktivieren.... 914
Erwerben eines neuen Lizenzschlüssels für höhere Server-Überwachungskapazität....914
Übernehmen eines neuen Lizenzschlüssels für höhere Server-Überwachungskapazität... 915
Verwenden von Überwachungsprofilen....915
Profile bearbeiten....916
SNMP-Trap-Meldungen und Warnmeldungskriterien konfigurieren.... 918
Neue Profile basierend auf einem Standardprofil erstellen.... 921
Profil-Protokollpfade für MySQL und Apache....923
Hochladen eines Profils, das von einem anderen Benutzer erstellt wurde....923
Herunterladen eines Profils, damit es von anderen verwendet werden kann....923
Zusätzliche Profile an ein Gerät binden.... 924
Nicht standardmäßige Protokolldatumsformate definieren....924
Konfigurieren der Anwendungs- und Schwellenwertüberwachung mit Log Enablement Packages (LEP)....925
LEPs auf überwachten Geräten installieren.... 926
Geräte mit Windows Server 2003 mit einem Log Enablement Package (LEP) von ITNinja einrichten....926
Überwachungs-Protokollaktivierungspaket (Log Enablement Package, LEP) für Geräte unter Windows Server 2008 oder höher bearbeiten.... 928
Überwachungs-Protokollaktivierungspaket (Log Enablement Package, LEP) für Geräte unter Windows Server 2003 bearbeiten....930
Verwalten der Geräteüberwachung....931
Überwachung für ein Gerät anhalten.... 932
Überwachung für mehrere Geräte anhalten oder fortsetzen....932
Abrufintervall und Einstellungen für das automatische Verwerfen oder Löschen von Warnungen festlegen....933
Ping-Test deaktivieren.... 933
Warnungen bei Gerätekonfigurationsänderungen empfangen....934

Wartungsfenster planen, während dessen keine Alarme von einem Gerät erfasst werden... 934
Überwachungsspezifische Rollen erstellen und zuweisen... 935
Deaktivieren der Überwachung für ein oder mehrere Geräte... 938
Aktivieren der Überwachung für ein oder mehrere Geräte... 939
Arbeiten mit Warnungen... 939
Hinzufügen von Benachrichtigungszeitplänen über die Listenseite "Überwachungswarnungen"... 940
Service-Desk-Tickets aus Warnungen erstellen... 941
Mit erweiterten Suchkriterien nach Warnungen suchen... 947
Filtern von Warnungen mit der Einschluss- und Ausschlusstext-Funktion... 947
Herausfiltern von Warnmeldungen mit der Einschluss- und Ausschlusstext-Funktion auf der Seite "Profil-Details"... 948
Warnungen mit der Ausschlusstext-Funktion auf der Listenseite "Überwachungswarnungen" filtern... 948
Beispiele für Einschluss- und Ausschlusstext für Überwachungsprofile... 949
Warnungen verwerfen... 952
Verworfene Warnungen in der Warnungsliste abrufen und überprüfen... 952
Warnungen löschen... 952
Verwenden des Service Desks... 953
Konfigurieren des Service Desks... 953
Systemanforderungen... 953
Informationen zum Service Desk... 953
Überblick über Setup-Aufgaben... 954
Importieren von Tickets aus einem anderen System... 955
Konfigurieren der Service Desk-Geschäftszeiten und -Feiertage... 958
Service Desk-Geschäftszeiten konfigurieren... 959
Service Desk-Feiertage konfigurieren... 959
Konfigurieren von Service Level-Vereinbarungen... 960
Service Level-Vereinbarungen aktivieren... 960
Konigurieren von Service Desk-Ticketwarteschlangen... 961
Ticketwarteschlangen konfigurieren... 961
Warteschlangen-spezifische E-Mail-Einstellungen konfigurieren... 966
Umbenennen von Service Desk-Titeln und Labels... 972
Aktivieren oder Deaktivieren der Konfliktwarnung... 973
Antwortvorlagen anzeigen und bearbeiten... 974
Konfigurieren der Ticketeinstellungen... 975
Seite Details zum Ticket anpassen... 976
Anpassen der Startseite der Benutzerkonsole... 978
Benutzerkonsolen-Logo und -Text auf Systemebene ändern... 978

Benutzerkonsole-Logo und Anmeldetext auf Verwaltungsebene ändern..... 980
Interaktive Schaltflächen und Widgets auf der Startseite der Benutzerkonsole ein- oder ausblenden.....983
Links zu Knowledge Base-Artikeln auf der Startseite der Benutzerkonsole ein- oder ausblenden.....984
Benutzerkonsole-Ankündigungen hinzufügen, bearbeiten, ausblenden oder löschen.....985
Benutzerkonsole Ankündigungen priorisieren oder Ankündigung als dringend kennzeichnen.....987
Benutzerdefinierte Links auf der Startseite der Benutzerkonsole hinzufügen, bearbeiten oder löschen..... 988
Ticket-Links zur Startseite der Benutzerkonsole hinzufügen..... 989
Schnellaktions-Link für die Meldung von Problemen auf der Startseite der Benutzerkonsole hinzufügen..... 990
Informationen zur Zeitspanne für den Sitzungs-Timeout..... 990
Verwenden der Zufriedenheitsumfrage.....990
Standardverhalten der Zufriedenheitsumfrage ändern..... 991
Aktivieren oder Deaktivieren der Sicherheitsfunktionen für Service Desk-Anhänge.....992
Verwenden des Service Desk-Dashboards.....993
Info über die Service Desk-Dashboard-Widgets..... 993
Anpassen des Service Desk-Dashboards..... 995
Verwalten von Service Desk-Tickets, -Prozessen und -Berichten..... 995
Übersicht über den Lebenszyklus von Service Desk-Tickets.....996
Erstellen von Tickets über die Administratorkonsole und Benutzerkonsole..... 996
Erstellen von Tickets in der Benutzerkonsole.....996
Erstellen von Tickets auf der Ticketseite der Administratorkonsole.....999
Tickets über die Seite "Gerätedetail" erstellen..... 1008
Tickets über die Seite "Asset-Detail" erstellen.....1009
Service-Desk-Tickets aus Warnungen erstellen..... 1010
Erstellen und Verwalten von Tickets per E-Mail.....1015
Informationen zu Anhängen für per E-Mail erstellte Tickets..... 1016
Ticketerstellung per E-Mail aktivieren..... 1016
Ticket per E-Mail erstellen..... 1016
Ticketattribute per E-Mail ändern.....1017
Ticketfeld per E-Mail löschen.....1017
Ticketfelder per E-Mail ändern.....1017
Ticketgenehmigungsfelder per E-Mail ändern..... 1018
Anzeigen von Tickets und Verwalten von Kommentaren, Arbeit und Anhängen.....1019
Zwischen Tickets, dazugehörigen Geräten und Assets navigieren..... 1019
Arbeitsinformationen zu Tickets hinzufügen..... 1020

Benutzerdefinierte Ansichten für Tickets verwenden....1021
Benutzerdefinierte Ansichten für Tickets erstellen....1023
Ansicht als Standardeinstellung für Tickets festlegen....1024
Tickets Kommentare hinzufügen....1024
Tickets Kommentare nur für Besitzer hinzufügen....1026
Ticket-Kommentare anzeigen....1026
Screenshots und Anhänge zu Service-Desk-Tickets hinzufügen oder aus ihnen löschen....1027
Ticketaktivitätsverlauf anzeigen....1028
Ticketinformationen per E-Mail senden....1029
Geräteaktionen über Tickets ausführen....1029
Zusammenführen von Tickets....1030
Tickets über die Seite „Ticketliste“ zusammenführen....1030
Tickets über die Seite „Ticketdetail“ zusammenführen....1030
Verwenden des Prozesses zur Eskalation von Tickets....1031
Informationen zu Ticketstatusangaben....1032
Informationen zur Eskalationsfrist....1032
Informationen zur Eskalation....1032
Einstellungen für die Eskalation von Tickets ändern....1032
Liste der Empfänger von Eskalations-E-Mails ändern....1032
Eskalationsfrist ändern....1033
Standardmäßige Eskalations-E-Mail-Nachricht ändern....1033
Verwenden von Service Desk-Prozessen....1034
Hinzufügen, Bearbeiten und Aktivieren von Prozessvorlagen....1034
Prozesstypen definieren....1042
Prozesstickets zur Verwaltung zugehöriger Aufgaben erstellen....1043
Prozesstickets per E-Mail erstellen....1043
Prozessinformationen anzeigen....1044
Prozesstickets abbrechen oder abschließen....1045
Prozessvorlagen löschen....1046
Prozesstickets in reguläre Tickets umwandeln....1046
Reguläre Tickets in Prozesstickets umwandeln....1047
Verwenden von Ticketregeln....1047
Systemticketregeln verwenden und konfigurieren....1047
Informationen zu den Systemticketregeln und Anpassen der Regeln....1048
Benutzerdefinierte Ticketregeln erstellen....1049
Benutzerdefinierte Ticketregeln duplizieren....1052
Benutzerdefinierte Ticketregeln löschen....1052
Ticketregeln von einer Warteschlange in eine andere verschieben....1053

Ausführen von Service Desk-Berichten....1053
Archivieren, Wiederherstellen und Löschen von Tickets....1054
Ticketarchivierung aktivieren....1054
Einstellungen für die Warteschlangenarchivierung konfigurieren....1056
Ausgewählte Tickets archivieren....1057
Archivierte Tickets wiederherstellen....1058
Archivierte Tickets löschen....1058
Verwalten der Ticketlöschung....1058
Einstellungen für die Ticketlöschung konfigurieren....1058
Tickets löschen....1059
Verwalten von Warteschlangen für Service-Desk-Tickets....1059
Informationen zu Service Desk-Ticketwarteschlangen....1059
Hinzufügen und Löschen von Warteschlangen....1060
Warteschlangen hinzufügen....1060
Warteschlangen durch Duplizieren einer vorhandenen Warteschlange hinzufügen....1061
Warteschlangen löschen....1061
Anzeigen von Tickets in Warteschlangen....1062
Ticket warteschlangenübergreifend anzeigen....1062
Einrichten der Standardwarteschlange....1062
Standardwarteschlangen auf Systemebene festlegen....1062
Standardwarteschlangen auf Benutzerebene festlegen....1063
Standardwerte für die Ticketliste "Alle Warteschlangen" festlegen....1064
Verschieben von Tickets zwischen Warteschlangen....1065
Informationen zu Benutzerdownloads und Knowledge Base-Artikeln....1066
Verwalten von Benutzerdownloads....1066
Benutzerdownloads hinzufügen....1066
Benutzerdownloads Labels zuweisen....1070
Labels bei Benutzerdownloads entfernen....1070
Benutzerdownloads löschen....1070
Verwalten von Knowledge Base-Artikeln....1071
Knowledge Base-Artikel hinzufügen, bearbeiten oder duplizieren....1071
Knowledge Base-Artikel löschen....1073
Benutzerbewertungen und Häufigkeit der Anzeige von Knowledge Base-Artikeln anzeigen....1073
Anpassen von Einstellungen für Service-Desk-Tickets....1074
Informationen zum Anpassen von Einstellungen für Service-Desk-Tickets....1074
Erstellen von Ticketkategorien und -unterkategorien....1074
Anpassen von Ticketwerten....1077
Ticketstatuswerte anpassen....1077

Ticketprioritätswerte anpassen....1078
Ticketauswirkungswerte anpassen.... 1080
Anpassen des Ticketlayouts.... 1081
Ticket-Layoutfelder und zugehörige Ticketfelder anpassen....1081
Kommentar-Feldoptionen konfigurieren.... 1084
Benutzerdefinierte Ticketfelder definieren....1084
Ticketlayout anpassen....1087
Ticketvorlagen verwalten....1087
Ticketvorlage konfigurieren.... 1088
Ticketlayoutvorschau....1093
Verwendung von über- und untergeordneten Ticketbeziehungen....1094
Beziehungen zwischen über-/untergeordneten Tickets für eine Warteschlange aktivieren....1095
Option zum Abschließen untergeordneter Tickets durch übergeordnete Tickets aktivieren....1095
Untergeordnete Tickets für ein beliebiges Ticket erstellen.... 1096
Tickets als übergeordnete Tickets festlegen und vorhandene Tickets als untergeordnete Tickets hinzufügen....1097
Übergeordnetes Ticket als Aufgabenliste verwenden....1097
Übergeordnete Tickets zum Organisieren doppelter Tickets verwenden.... 1098
Verwenden von Ticketgenehmigern.... 1098
Ticketgenehmiger konfigurieren....1099
Tickets per E-Mail genehmigen.... 1100
Konfigurieren von SMTP-E-Mail-Servern.... 1100
E-Mail-Server mit der Appliance verbinden....1100
Verwenden eines internen und externen SMTP-Servers.... 1101
Internen SMTP-Server verwenden....1101
Externen SMTP-Server oder sicheren SMTP-Server verwenden....1102
Wartung und Fehlerbehebung.... 1105
Warten der Appliance....1105
Nachverfolgen von Änderungen der Einstellungen.... 1105
Informationen zu Appliance-Sicherungen....1105
Zeitplan der täglichen Sicherung und die Anzahl der beizubehaltenden Sicherungen einrichten....1106
Appliance manuell sichern.... 1107
Administratorkonsole Sicherungsdateien herunterladen....1107
Auf Sicherungsdateien über FTP zugreifen....1108
Informationen zum Löschen von Appliance-Sicherungsdaten....1108
Offboard-Backup-Übertragung konfigurieren.... 1109
Wiederherstellen der Appliance....1111

Appliance anhand der letzten Sicherung wiederherstellen.....1111
Sicherungsdateien in die Appliance hochladen.....1112
Appliance von Sicherungskopien wiederherstellen.....1113
Werkseinstellungen der Appliance wiederherstellen.....1114
Aktualisieren der Appliance-Software.....1114
Auf beworbene Appliance-Aktualisierungen prüfen und diese anwenden.....1114
Aktualisierungsdatei manuell in die Appliance hochladen.....1115
Aktualisierungen überprüfen.....1116
Lizenzschlüssel der Appliance aktualisieren.....1116
Appliance neu starten oder herunterfahren.....1116
OVAL-Definitionen über KACE aktualisieren.....1117
Informationen zu "Daily Run Output".....1117
Status des Datenträgers.....1118
Netzwerkschnittstellen-Status der Appliance.....1118
Betriebszeit und durchschnittliche Belastung der Appliance.....1119
Zustand der E-Mail-Systeme.....1119
Sicherungsstatus der Appliance.....1120
Status der RAID-Laufwerke.....1120
Fehlerbehebung auf der Appliance.....1120
Verwenden von Tools zur Fehlerbehebung.....1120
Status von Geräten im Netzwerk überprüfen.....1120
Identifizieren von Geräteproblemen.....1121
Tether zum Support von Quest KACE aktivieren.....1121
Fehlerbehebung bei Problemen mit der Appliance.....1122
Appliance-Protokolle anzeigen.....1122
Aktivitätsprotokolle der Appliance herunterladen.....1127
"Daily Run Output" (Täglicher Systembericht) anzeigen.....1127
Fehlerbehebung und Debuggen des KACE Agent.....1128
Windows Sicherheitsprobleme beheben, die die Agenten-Provisionierung verhindern.....1128
Testen der E-Mail-Kommunikation und Fehlerbehebung.....1128
Ausgehende E-Mail-Nachrichten testen.....1129
Eingehende E-Mails testen.....1129
Telnet zum Testen eingehender E-Mails verwenden.....1130
Zum Anzeigen von Microsoft Exchange Server-Fehlern auf Appliance-Protokolle zugreifen.....1130
E-Mail-Fehler beheben.....1131
Über die Zweifaktor-Authentifizierung der Diagnosekonsole.....1131
Anhang.....1133

Namen von Datenbanktabellen..... 1133
Hinzufügen von Schritten zu Aufgabenbereichen von Skripten..... 1150
LDAP-Variable.....1167
Glossar.....1170
A..... 1170
Ä..... 1173
B..... 1174
C..... 1175
D..... 1176
E..... 1177
F..... 1178
G.....1179
I..... 1180
K..... 1181
L..... 1182
M..... 1183
N.....1184
O.....1185
P..... 1187
R.....1188
S..... 1189
T..... 1191
Ü.....1192
V..... 1193
W..... 1194
Über uns..... 1195
Ressourcen für den technischen Support..... 1195
Rechtliche Hinweise.....1196
Index.....1198

Informationen zur KACE Systemverwaltungs-Appliance

Quest® KACE®**Appliance für Systemverwaltung** ist eine virtuelle Appliance, die zur Automatisierung der Geräteverwaltung, der Anwendungsbereitstellung, des Patchings, des Asset Managements, der Berichterstellung und der Service Desk-Ticketverwaltung entwickelt wurde.

Weitere Informationen zu Appliances der **KACE** Serie finden Sie auf der Quest Website unter https://www.quest.com/products/kace-systems-management-appliance/.

KACE Systemverwaltungs-Appliance ist eine eingeschränkte Version der KACE Systemverwaltungs-Appliance für die Verwaltung von Endbenutzertickets und -Assets. Sie verwendet den KACE Agent zur Verwaltung von einzelnen Geräteknoten und bis zu 250 Knoten ohne Agenten. Anders als die KACE Systemverwaltungs-Appliance bietet sie keine Patching- und Skriptfunktionen und keine Software Asset Management-Funktionen. Sie finden Informationen zu diesen Funktionen in diesem Handbuch, sie sind jedoch in **KACE Systemverwaltungs-Appliance** deaktiviert. Ein Upgrade von **KACE Systemverwaltungs-Appliance** auf die KACE Systemverwaltungs-Appliance ist problemlos möglich, um den vollen Funktionsumfang der Endpunktverwaltung zu nutzen. Um vollständige Informationen über dieses Produkt, seine technischen Spezifikationen und Referenzmaterialien zu erhalten, besuchen Sie die Dokumentationsseite unter https://support.quest.com/kace-systems-management-appliance/technical-documents.

Informationen zu Appliance-Komponenten

Zu den Appliance-Komponenten zählen Software, Hardware, webbasierte Schnittstellen und die Oberfläche einer mobilen App.

Appliance-Komponenten

Komponente	Beschreibung
Virtual Appliance	Die Appliance wird in einer virtuellen Umgebung ausgeführt, die eine VMware®- oder Microsoft® Hyper-V®-Infrastruktur verwendet. Aktuelle Informationen zu den Anforderungen für verwaltete Geräte und zu den Browseranforderungen für den Zugriff auf die **Administratorkonsole** finden Sie in den *technischen Daten* auf der Produktdokumentationsseite: https://support.quest.com/kace-systems-management-appliance/technical-documents.
Befehlszeilenkonsole	Die **Befehlszeilenkonsole** ist ein Terminalfenster für die Appliance. Die Schnittstelle ist hauptsächlich für die Konfiguration der Appliance und die Richtlinienerzwingung gedacht. Siehe Einschalten der Appliance und Anmelden bei der Administratorkonsole.

Komponente	Beschreibung
Administratorkonsole	Die **Administratorkonsole** ist die webbasierte Oberfläche zur Steuerung der Appliance. Auf die **Administratorkonsole** können Sie unter `http://`**appliance_hostname**`/admin` zugreifen, wobei **appliance_hostname** der Hostname Ihrer Appliance ist. Wenn die Organisationskomponente aktiviert ist, können Sie über die **Administratorkonsole** unter `http://`**appliance_hostname**`/system` auf die Einstellungen auf Systemebene zugreifen. Um die vollständigen Pfade von URLs in der **Administratorkonsole** anzuzeigen, fügen Sie der URL, die Sie zur Anmeldung verwenden, `ui` hinzu. Dies kann nützlich sein, wenn Sie die Datenbank durchsuchen oder Links freigeben. Zum Beispiel: `http://`**appliance_hostname**`/admin`.
Benutzerkonsole	Die **Benutzerkonsole** ist die webbasierte Oberfläche, die Benutzern Anwendungen auf Self-Service-Basis zur Verfügung stellt. Außerdem ermöglicht sie Benutzern das Einsenden von Service Desk Support-Tickets, mit denen sie Hilfe anfordern oder Fehler melden können. Auf die **Benutzerkonsole** können Sie unter `http://`**appliance_hostname**`/user` zugreifen, wobei **appliance_hostname** der Hostname Ihrer Appliance ist. Die **Benutzerkonsole** bietet Folgendes: • Ein Repository mit Softwareanwendungen, die Benutzer je nach Bedarf herunterladen können • Eine Möglichkeit für Benutzer, Tickets zu senden, mit denen sie Hilfe anfordern können • Unterstützung für Routineaufgaben wie die Softwareinstallation und Zugriff auf die **Quest Support Knowledge Base**, https://support.quest.com/kace-systems-management-appliance/kb. Informationen zur Anpassung der **Benutzerkonsole** finden Sie hier: • Allgemeine Appliance-Einstellungen bei aktivierter Organisationskomponente konfigurieren. • Allgemeine Appliance-Einstellungen ohne aktivierte Organisationskomponente konfigurieren.
KACE Agent	Der KACE Agent ist eine Anwendung, die auf Geräten installiert werden kann, um die Geräteverwaltung über die Appliance zu ermöglichen. Auf verwalteten Geräten installierte Agenten kommunizieren über das AMP (Agenten-Messaging-Protokoll) mit der Appliance. Agenten

Komponente	Beschreibung
	führen geplante Aufgaben durch, beispielsweise das Erfassen von Inventarinformationen auf verwalteten Geräten und das Verteilen von Software an verwaltete Geräte. Die Verwaltung ohne Agent ist bei Geräten verfügbar, auf denen die Agenten-Software nicht installiert werden kann, beispielsweise bei Druckern und Geräten mit vom Agenten nicht unterstützten Betriebssystemen. Siehe Provisionierung des KACE Agent.
KACE GO	KACE GO ist eine App, mit der Administratoren über ihre Smartphones oder Tablets auf Service-Desk-Tickets, Inventarinformationen sowie die Anwendungsbereitstellungsfunktionen zugreifen können. Mit der App können auch Benutzer ohne Administratorberechtigungen auf ihrem Mobilgerät Service-Desk-Tickets senden, den Status von gesendeten Tickets anzeigen und Knowledge Base-Artikel lesen. Sie können KACE GO für iOS-Geräte aus dem Apple® App Store℠ oder für Android™-Geräte aus dem Google Play™ Store herunterladen. Siehe Konfigurieren des Mobilgerätezugriffs.

Informationen zur Administratorkonsole

Die in der **Administratorkonsole** verfügbaren Komponenten können je nach Lizenzschlüssel, Organisationseinstellungen, Appliance-Einstellungen und Benutzerrolle abweichen.

Wird die Organisationskomponente aktiviert, verfügt die Administratorkonsole über zwei Ebenen: die Verwaltungsebene, auf der organisationsbezogene Funktionen angezeigt werden, und die Systemebene, auf der auf die Appliance bezogene Funktionen angezeigt werden.

Ist die Organisationskomponente nicht aktiviert, stehen Funktionen auf Verwaltungs- und Systemebene auf der Verwaltungsebene zur Verfügung.

HINWEIS: Ihr Lizenzschlüssel bestimmt, ob die Organisationskomponente aktiviert oder deaktiviert ist. Siehe Produktlizenzinformationen anzeigen und Informationen zu Organisationen.

Es gibt drei Anmeldemodi:

- **Administratormodus ohne aktivierte Organisationskomponente**: Wenn die Organisationskomponente für Ihre Appliance nicht aktiviert ist, können Sie sich unter `http://`**appliance_hostname**`/admin` bei diesem Modus anmelden. **appliance_hostname** steht hierbei für den Hostnamen Ihrer Appliance. Die in diesem Modus verfügbaren Komponenten finden Sie unter Im Administratormodus ohne die Organisationskomponente verfügbare Komponenten.
- **Administratormodus mit aktivierter Organisationskomponente**: Wenn die Organisationskomponente für Ihre Appliance aktiviert ist, können Sie sich unter `http://`**appliance_hostname**`/admin` bei der Standardorganisation anmelden. **appliance_hostname** steht hierbei für den Hostnamen Ihrer Appliance. Im Administratormodus können Sie die für die ausgewählte Organisation verfügbaren Komponenten verwalten. Die in diesem Modus verfügbaren Komponenten finden Sie unter Im Administratormodus mit aktivierter Organisationskomponente verfügbare Komponenten.

Wenn die Option *Organisation anmelden* in den Appliance-Einstellungen aktiviert ist, wird das Feld *Organisation* angezeigt. Sie können den Namen einer Organisation in das Feld *Organisation* eingeben, um sich direkt bei dieser Organisation anzumelden.

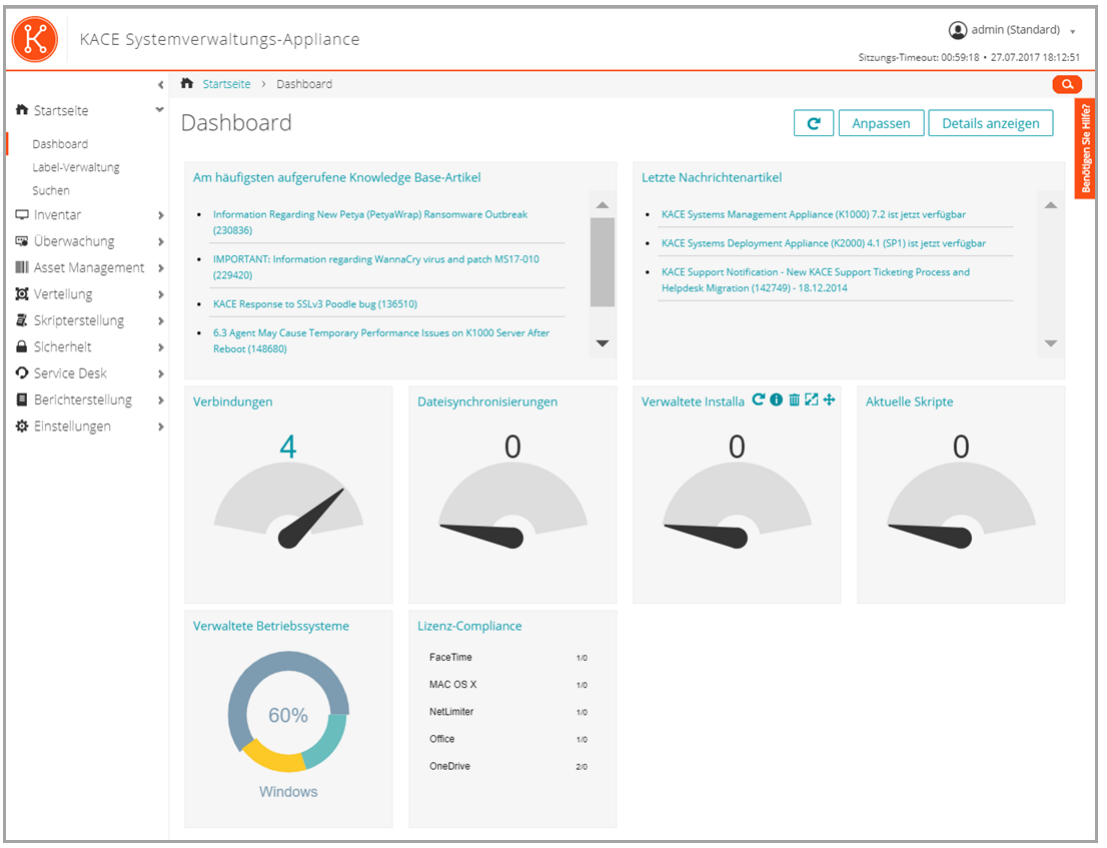
Wenn mehrere Organisationen vorhanden sind und die Option *Schneller Wechsel* aktiviert ist, können Sie mithilfe der Dropdown-Liste in der oberen rechten Ecke neben den Anmeldeinformationen zwischen den Organisationen und der Systemstufe umschalten. Siehe Schnellen Wechsel von Organisationen und verknüpften Appliance aktivieren.

- **Systemmodus mit aktivierter Organisationskomponente**: Wenn die Organisationskomponente für Ihre Appliance aktiviert ist, können Sie sich unter `http://`**appliance_hostname**`/system` im Systemmodus anmelden. **appliance_hostname** steht hierbei für den Hostnamen Ihrer Appliance. In diesem Modus können Sie die auf Systemebene verfügbaren Komponenten verwalten. Die in diesem Modus verfügbaren Komponenten finden Sie unter Im Systemmodus mit aktivierter Organisationskomponente verfügbare Komponenten.

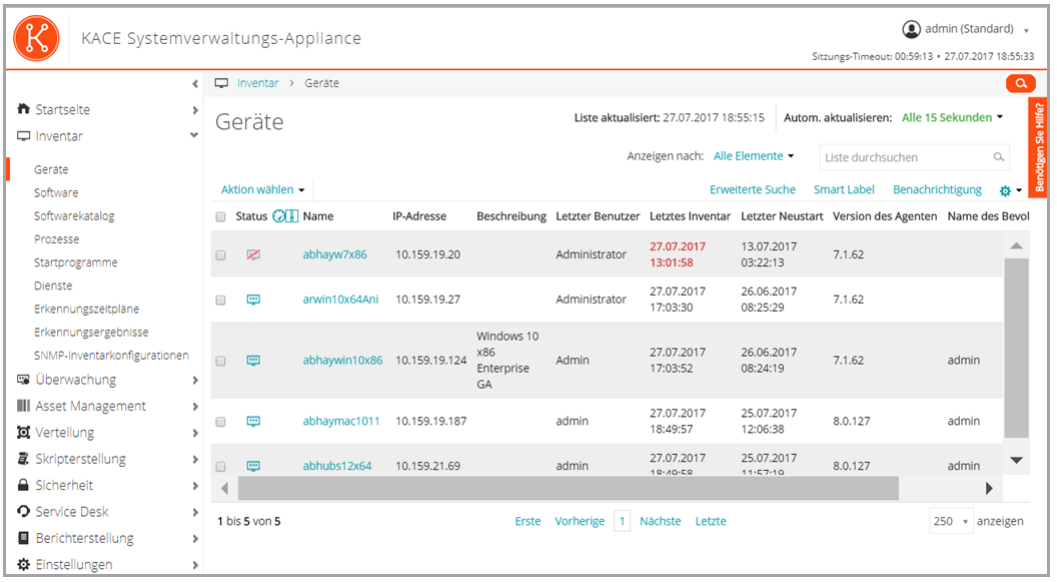
  Wenn *Schneller Wechsel* aktiviert ist und die Kennwörter für die Standard-Administratorkonten der Organisationen dieselben sind, können Sie außerdem mithilfe der Dropdown-Liste in der oberen rechten Ecke der Seite zwischen Organisationen umschalten. Siehe Schnellen Wechsel von Organisationen und verknüpften Appliance aktivieren.

Jeder Modus hat die folgenden Seitentypen:

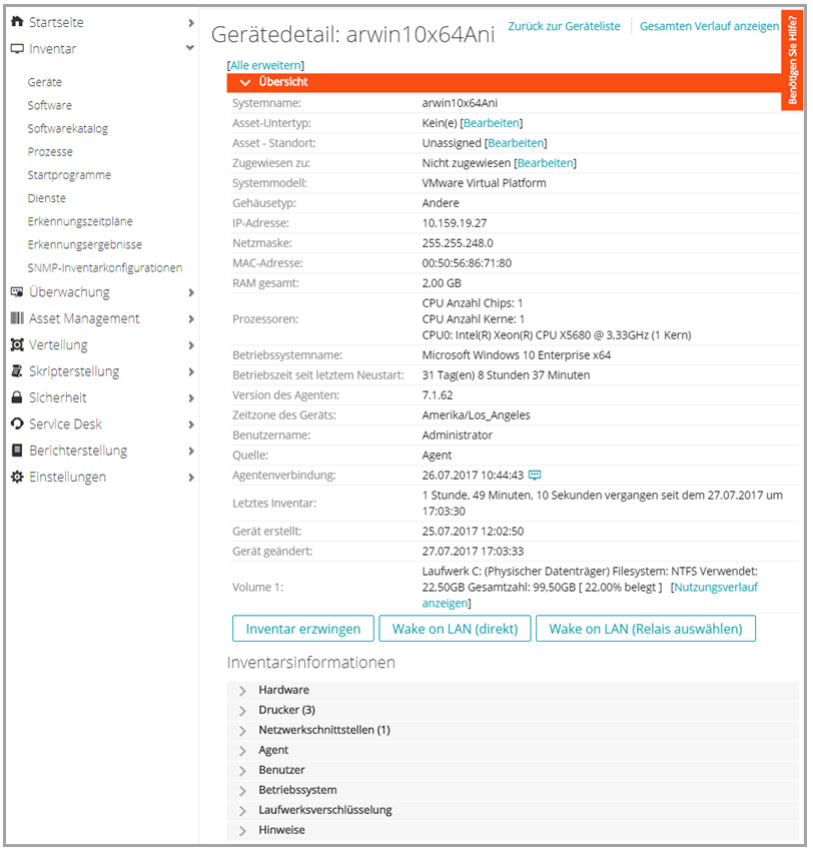
- **Dashboards**. Auf dieser Seite sehen Sie die Statusinformationen der Appliance. Wenn die Organisationskomponente aktiviert ist, sind die Dashboards auf Organisations- und Systemebene verfügbar.



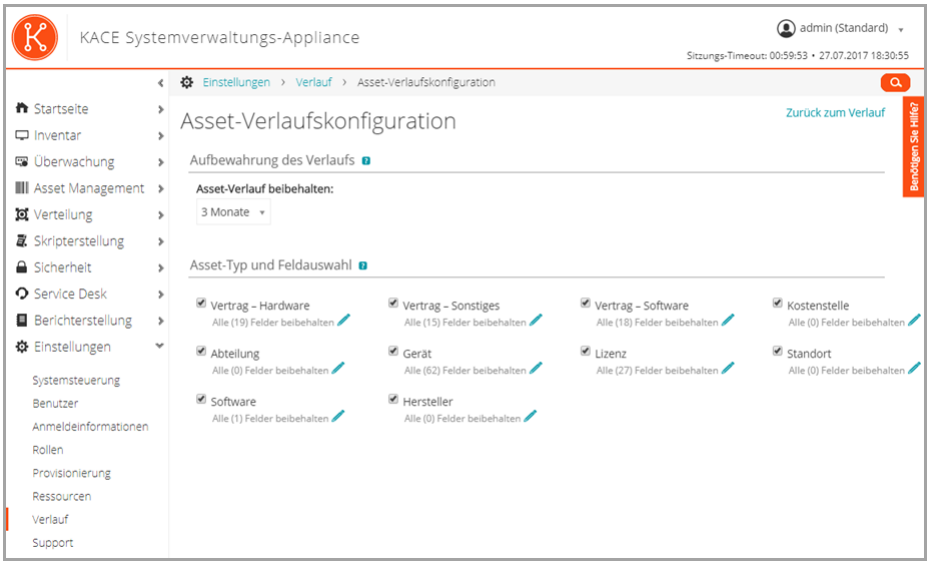
- **Listenseiten**. Auf diesen Seiten sehen Sie die auf der Appliance verfügbaren Elemente, bzw. falls die Organisationskomponente installiert ist, die für die ausgewählte Organisation verfügbaren Elemente.



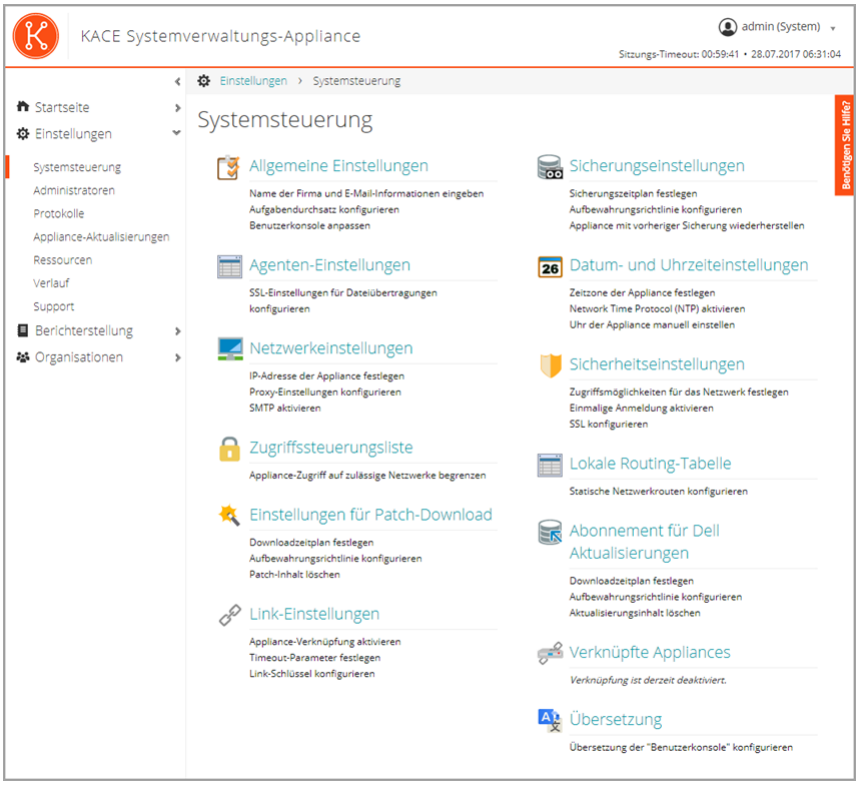
- **Detailseiten**. Auf diesen Seiten sehen und bearbeiten Sie die Details des ausgewählten Elements.



- **Konfigurationsseiten**. Auf diesen Seiten konfigurieren Sie die Einstellungen.

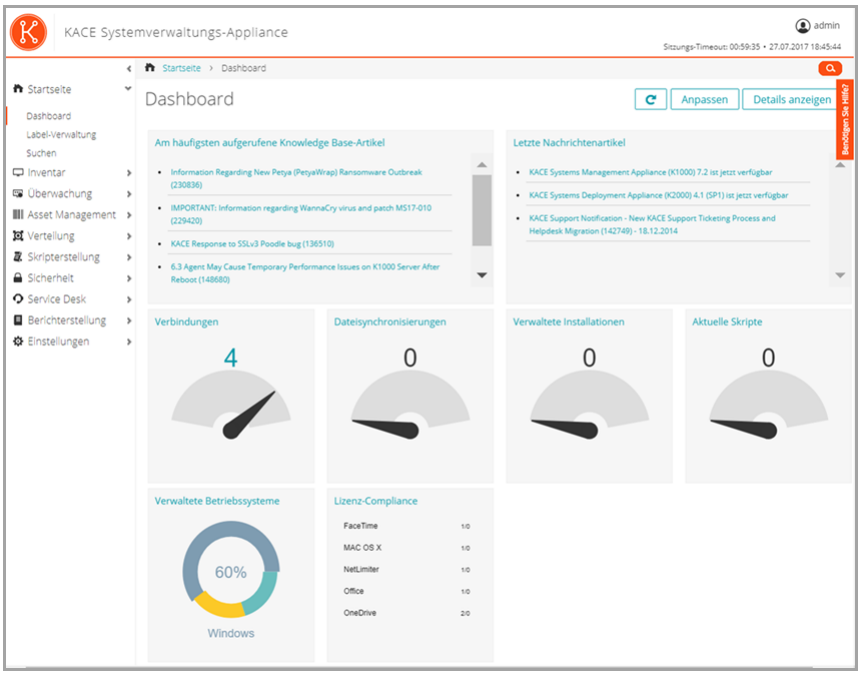


- **Bedienfelder**. Auf diesen Seiten erhalten Sie Zugriff auf zugehörige Komponenten und Einstellungen.



Im Administratormodus ohne die Organisationskomponente verfügbare Komponenten

Wenn die Organisationskomponente nicht aktiviert ist, sehen Sie im Administratormodus alle Komponenten der Verwaltungsebene und alle Einstellungen der Systemebene (Appliance-Ebene).



Im Administratormodus ohne die Organisationskomponente verfügbare Komponenten

Komponente	Seite der Benutzeroberfläche	Verwendung
Startseite	• Dashboard • Label-Verwaltung • Suchen	Einsehen von Appliance-Statistiken, Verwalten von Labels, Anzeigen von Verlaufsinformationen und die Suche nach Daten. Siehe

Komponente	Seite der Benutzeroberfläche	Verwendung
		Verwenden der Komponente "Startseite".
Inventar	• Geräte • Software • Softwarekatalog • Prozesse • Startprogramme • Dienste • Erkennungszeitpläne • Erkennungsergebnisse • SNMP-Inventarkonfigurationen	Verwalten der Geräte, Software, Prozesse, Dienste, Scans sowie weiterer Elemente in Ihrem Netzwerk. Siehe: • Verwalten des Geräteinventars • Verwalten von Anwendungen auf der Seite "Software" • Verwalten des Softwarekataloginventars • Verwalten des Prozess-, Startprogramm- und Dienstinventars • Verwenden der Geräteerkennung • Erkennen bestimmter, dem Inventar hinzuzufügender SNMP-Objekte und Nicht-Computer-Geräte mithilfe von SNMP-Inventarkonfigurationen
Überwachung	• Geräte • Warnungen • Profile • Wartungsfenster • Log Enablement Packages	Verwalten Sie mit Ihrer Standardlizenz die allgemeine Ereignisüberwachung für bis zu fünf Server. Erfassen Sie dazu Ereignisdaten aus Protokollen zu wichtigen Windows® Ereignissen, Systemprotokollen und Anwendungsprotokollen. Mit der Überwachungsmodullizenz verwalten Sie die Ereignisüberwachung für bis zu 200 Server.

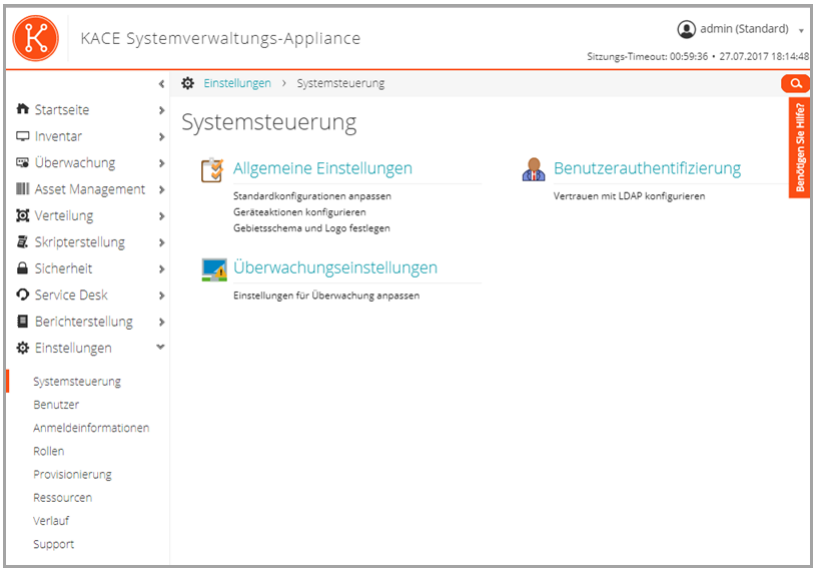
Komponente	Seite der Benutzeroberfläche	Verwendung
		Siehe Überwachen von Servern
Assets	• Assets • Asset-Typen • Verträge • Lizenzen • Lizenz-Compliance • Standorte • Assets importieren	Mit diesen Registerkarten können Sie physische Assets wie Geräte, Software, Drucker usw. verfolgen sowie den Verlauf von Assets und ihre Konfiguration anzeigen. Siehe: • Verwalten des Inventars • Verwalten der Lizenz-Compliance
Verteilung	• Verwaltete Installationen • Dateisynchronisierungen • Wake on LAN • Replikation • Warnungen	Remote-Verteilung und -Verwaltung von Software, einschließlich Aktualisierungen von Quest. Siehe Bereitstellen von Paketen auf verwalteten Geräten.
Skripterstellung	• Skripte • Jetzt ausführen • 'Jetzt ausführen'-Status • Skriptprotokolle durchsuchen • Konfigurationsrichtlinien • Sicherheitsrichtlinien • Mac Profile	Aufgaben automatisieren, die auf verwalteten Geräten durchgeführt wurden. Siehe Ausführen von Skripten auf verwalteten Geräten.
Sicherheit	• Patch-Verwaltung • OVAL-Scan • SCAP-Scan • Dell Aktualisierungen	Mit diesen Registerkarten reduzieren Sie die Risiken durch Malware, Spyware und Viren. Bei OVAL-Tests (Open Vulnerability Assessment Language) handelt es sich um eine Reihe von Tests, mit deren Hilfe Sicherheitsrisiken auf verwalteten Geräten identifiziert werden können.

Komponente	Seite der Benutzeroberfläche	Verwendung
		Siehe Patchen von Geräten und Aufrechterhalten der Sicherheit.
Service Desk (bei Appliances, für die von einer früheren Version ein Upgrade ausgeführt wurde, auch *Helpdesk* genannt)	• Tickets • Benutzerdownloads • Knowledge Base • Ankündigungen • Archiv (nur verfügbar, wenn die Ticket-Archivierung aktiviert ist) • Konfiguration	Bereitstellen eines Repositorys für Softwareressourcen und -dokumentationsmaterialien, die Benutzer aufrufen und herunterladen können. Außerdem steht ein Service Desk mit umfassenden Funktionen zum Erstellen und Nachverfolgen von Tickets zur Verfügung. Siehe Verwenden des Service Desks.
Berichterstellung	• Berichte • Berichtszeitpläne • Benachrichtigungen	Über diese Registerkarten führen Sie zuvor gepackte Berichte und Tools zum Erstellen von Berichten aus, um Ihre Appliance-Implementierung zu überwachen. Siehe Verwenden von Berichten und Zeitplanung für Benachrichtigungen.
Einstellungen	• Systemsteuerung • Benutzer • Anmeldeinformationen • Rollen • Protokolle • Appliance-Aktualisierungen • Provisionierung • Ressourcen • Verlauf • Support	Verwalten Sie Ihre Appliance und die Agenten-Provisionierung. Siehe: • Konfigurieren der Appliance • Konfigurieren von Benutzerkonten, LDAP-Authentifizierung und SSO • Verwalten von Anmeldeinformationen • Warten der Appliance • Provisionierung des KACE Agent • Importieren und Exportieren von Appliance-Ressourcen • Verwalten des Einstellungsverlaufs • Verwenden von Tools zur Fehlerbehebung

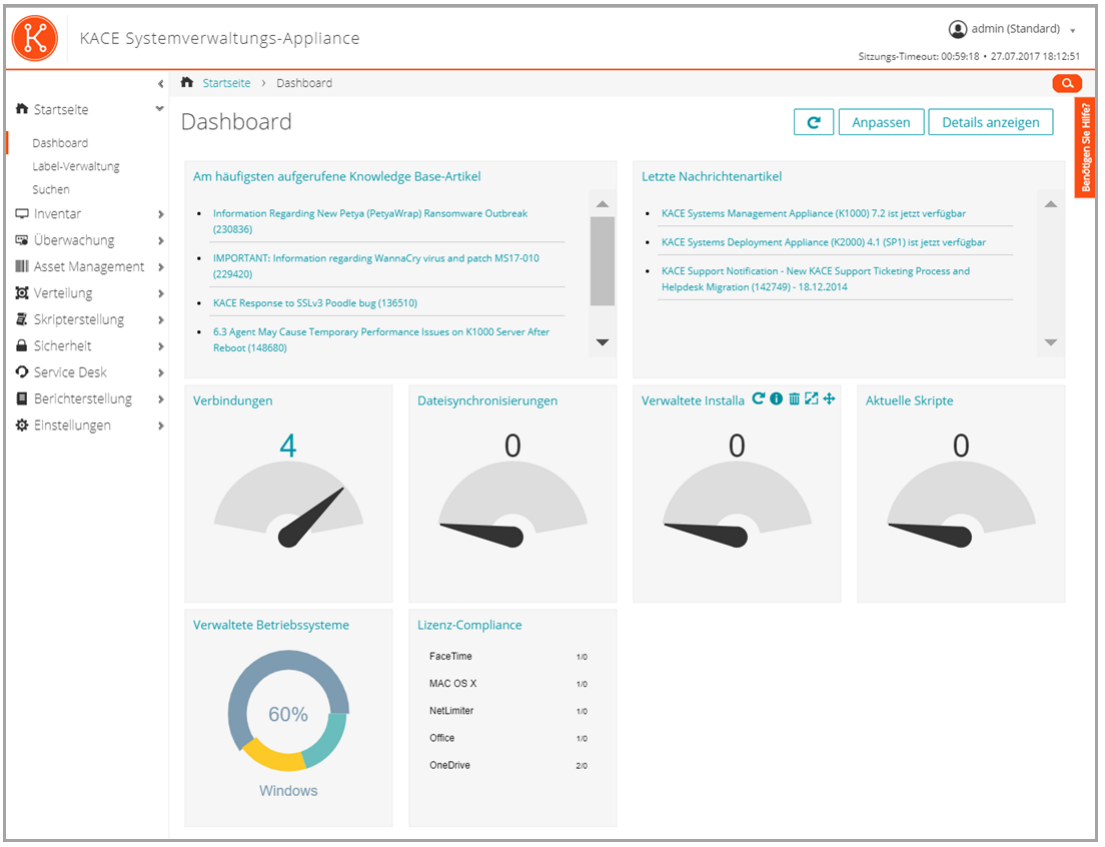
Im Administratormodus mit aktivierter Organisationskomponente verfügbare Komponenten

Bei aktivierter Organisationskomponente sehen Sie im Administratormodus nur Komponenten und Einstellungen für die aktuelle Organisation. Komponenten auf Appliance-Ebene sind im Systemmodus verfügbar.

Wenn die Organisationskomponente auf Ihrer Appliance aktiviert ist und Sie sich bei `http://`**appliance_hostname**`/admin` anmelden, zeigt die Komponente *Einstellungen* Funktionen an, die nur für die ausgewählte Organisation verfügbar sind.



Alle anderen Komponenten sind identisch, egal ob die Organisationskomponente aktiviert ist oder nicht. Informationen zu Komponenten finden Sie unter Im Administratormodus ohne die Organisationskomponente verfügbare Komponenten und in der folgenden Abbildung.



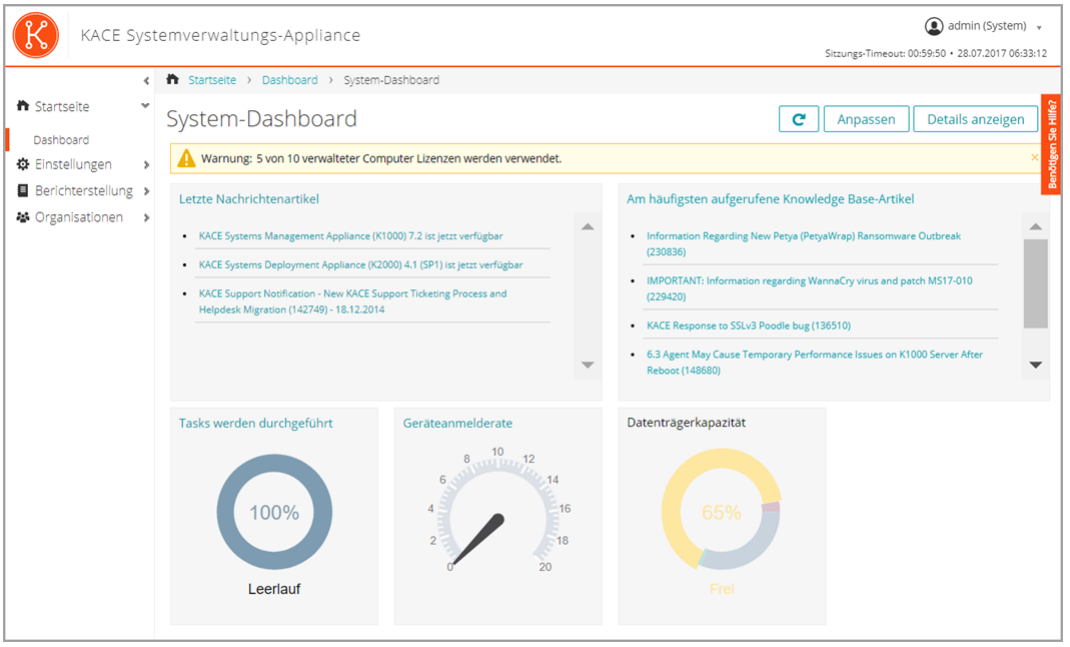
Im Administratormodus mit aktivierter Organisationskomponente verfügbare Komponenten

Komponente	Seite der Benutzeroberfläche	Verwendung
Einstellungen	• Systemsteuerung • Benutzer • Anmeldeinformationen • Rollen • Provisionierung • Ressourcen • Verlauf • Support	Verwalten Sie allgemeine Einstellungen für die Organisation, beispielsweise die Benutzerauthentifizierung und die Agenten-Provisionierung. Siehe: • Konfigurieren der Appliance • Konfigurieren von Benutzerkonten, LDAP-Authentifizierung und SSO • Verwalten von Anmeldeinformationen • Provisionierung des KACE Agent • Importieren und Exportieren von Appliance-Ressourcen • Verwalten des Einstellungsverlaufs • Verwenden von Tools zur Fehlerbehebung

Im Systemmodus mit aktivierter Organisationskomponente verfügbare Komponenten

Wenn die Organisationskomponente aktiviert ist, zeigt der Systemmodus zu den Appliance-Einstellungen gehörende Komponenten. Komponenten auf Organisationsebene sind im Administratormodus verfügbar.

Wenn Sie sich unter `http://`**appliance_hostname**`/system` bei der Systemadministratorkonsole anmelden oder **System** in der Dropdown-Liste oben rechts in der **Administratorkonsole** auswählen, sind folgende Komponenten verfügbar.



Im Systemmodus mit aktivierter Organisationskomponente verfügbare Komponenten

Komponente	Unterregisterkarten	Verwendung
Startseite	• Dashboard	Zeigen Sie zusammenfassende Statistiken zur Appliance an.

Komponente	Unterregisterkarten	Verwendung
		Siehe Verwenden der Komponente "Startseite".
Einstellungen	• Systemsteuerung • Administratoren • Protokolle • Appliance-Aktualisierungen • Ressourcen • Verlauf • Support	Verwalten Sie die Appliance und greifen Sie auf Ressourcen wie den **Quest Support** zu. Siehe: • Konfigurieren der Appliance • Warten der Appliance • Importieren und Exportieren von Appliance-Ressourcen • Verwalten des Einstellungsverlaufs • Verwenden von Tools zur Fehlerbehebung
Berichterstellung	• Berichte • Berichtszeitpläne	Über diese Registerkarten führen Sie zuvor gepackte Berichte und Tools zum Erstellen von Berichten aus, um Ihre Appliance-Implementierung zu überwachen. Siehe Verwenden von Berichten und Zeitplanung für Benachrichtigungen.
Organisationen	• Organisationen • Rollen • Filter • Geräte	Organisationen hinzufügen und verwalten (erfordert die Organisationskomponente). Siehe Erstellen und Verwalten von Organisationen.

Verwenden der Komponente "Startseite"

Die Komponente "Startseite" enthält Dashboard-, Labelverwaltungs- und Suchfunktionen.

Informationen zu Dashboards

Dashboards bieten einen Überblick über Aktivitäten von Organisationen und Appliances. Sie zeigen außerdem Warnungen und Links zu Neuigkeiten und Knowledge-Base-Artikeln an.

Wenn auf der Appliance die Organisationskomponente aktiviert ist und Sie bei der Administratorkonsole angemeldet sind (`http://`**appliance_hostname**`/admin`), zeigt das Dashboard Informationen zur ausgewählten Organisation an. Wenn Sie an der Systemverwaltungskonsole angemeldet sind (`http://`**appliance_hostname**`/system`), zeigt das Dashboard Informationen zur Appliance an, einschließlich aller Organisationen.

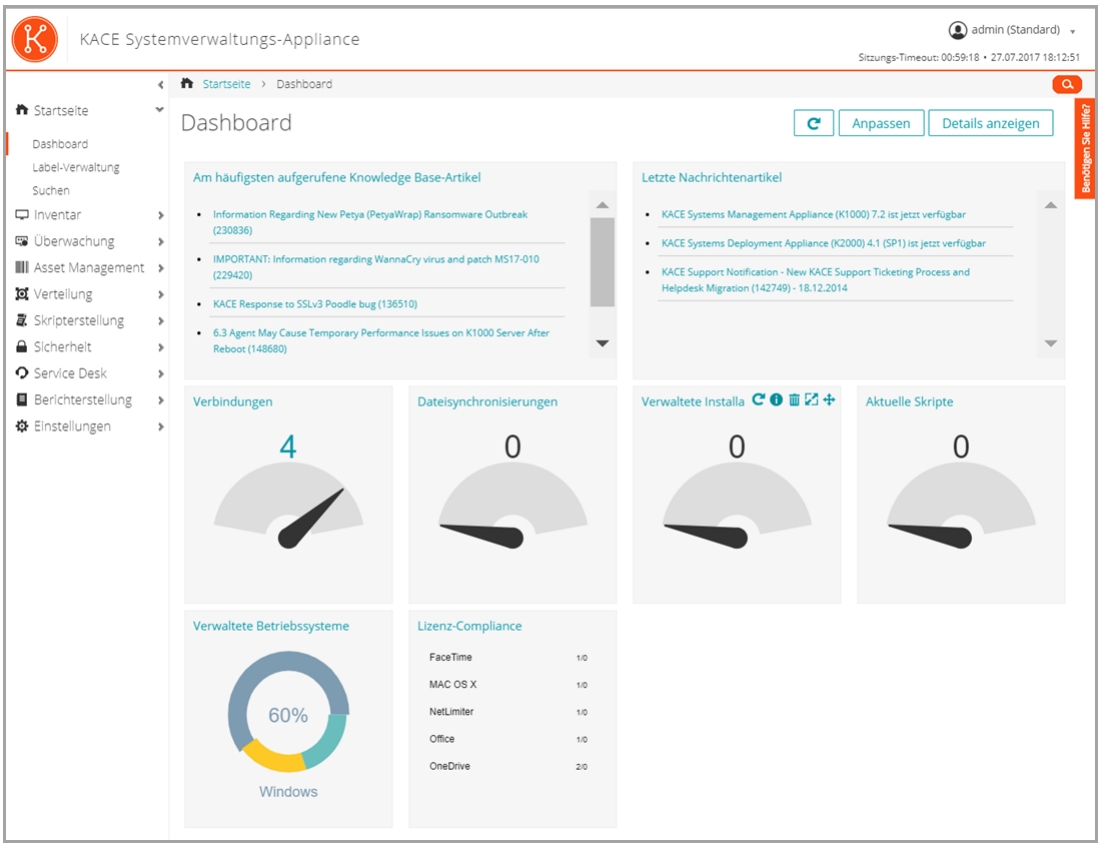
TIPP: Die Appliance aktualisiert die Übersichtswidgets regelmäßig. Um alle Widgets zu aktualisieren, klicken Sie auf die Schaltfläche **Aktualisieren** in der oberen rechten Seite: . Um einzelne Widgets zu aktualisieren, zeigen Sie mit dem Mauszeiger auf das Widget und klicken Sie oberhalb des Widgets auf die Schaltfläche **Aktualisieren**.

Dashboard im Administratormodus anzeigen

Auf dem Dashboard im Administratormodus können Sie Übersichtsinformationen für die Appliance oder für die ausgewählte Organisation (sofern die Organisationskomponente aktiviert ist) anzeigen.

- Melden Sie sich beim Administratorkonsole `http://`**appliance_hostname**`/admin` an. Oder wählen Sie in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus, wenn die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist.

Die Seite *Dashboard* wird angezeigt.

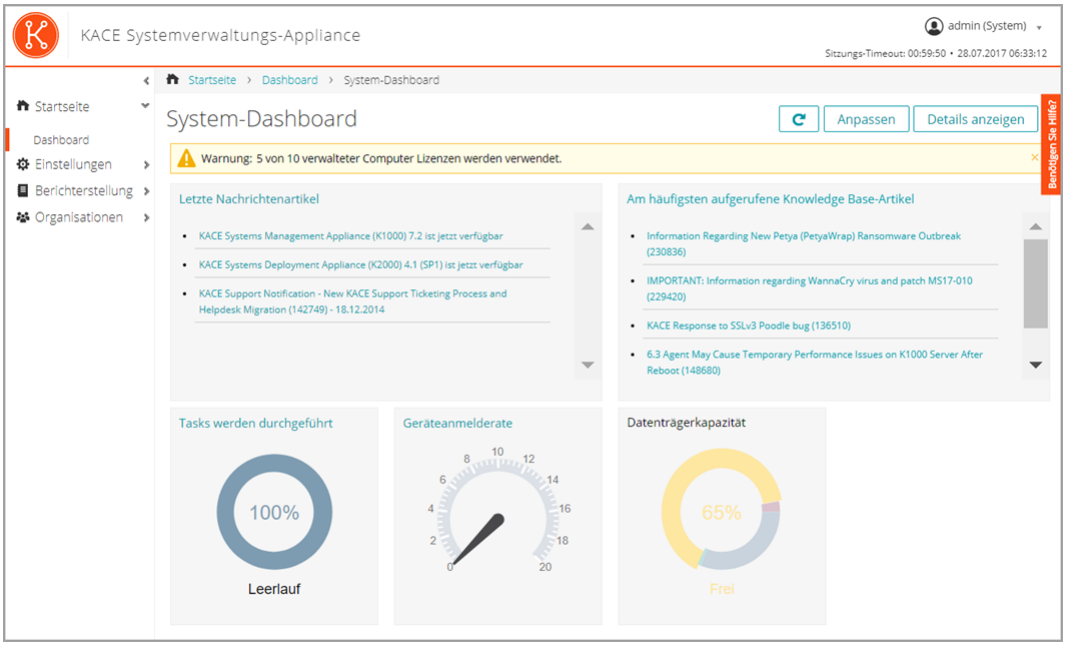


Dashboard im Systemmodus anzeigen

Wenn die Organisationskomponente auf der Appliance aktiviert ist, zeigt das System-Dashboard eine Übersicht über die Appliance an.

- Melden Sie sich bei der Systemadministratorkonsole der Appliance an: `https://`**appliance_hostname**`/system`. Oder wählen Sie in der Dropdown-Liste rechts oben auf der Seite den Eintrag **System** aus.

Die Seite *System-Dashboard* wird angezeigt.



Dashboard-Seiten anpassen

Sie können Dashboard-Seiten anpassen und Widgets nach Bedarf ein- oder ausblenden.

1. Führen Sie einen der folgenden Schritte aus:

   - **Melden Sie sich bei der Administratorkonsole der Appliance an: `https://appliance_hostname/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option** *Organisationsmenü in Verwaltungskopfzeile anzeigen* **aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.**

   - **Melden Sie sich bei der Systemadministratorkonsole der Appliance an: `https://appliance_hostname/system`. Oder wählen Sie in der Dropdown-Liste rechts oben auf der Seite den Eintrag System aus.**

   Die Seite *Dashboard* oder *System-Dashboard* wird angezeigt.

2. Fahren Sie mit dem Mauszeiger über das Widget und verwenden Sie anschließend die folgenden Schaltflächen:

   - : Die Informationen im Widget aktualisieren
   - : Die Informationen zum Widget anzeigen
   - : Das Widget ausblenden
   - : Die Größe des Widgets ändern
   - : Das Widget an eine andere Position auf der Seite ziehen.

3. Einige Widgets sind bearbeitbar, sodass Sie die angezeigten Informationen filtern können. Klicken Sie zum Bearbeiten des Widgets auf , und geben Sie die erforderlichen Informationen in das Dialogfeld ein. In einigen Fällen können Sie ggf. auch zwischen Balkendiagramm- und Donut-Ansicht wechseln.

4. Klicken Sie auf die Schaltfläche **Anpassen** in der oberen rechten Ecke der Seite, um die verfügbaren Widgets anzuzeigen.

5. Um alle installierten Widgets anzuzeigen klicken Sie auf **Anzeigen nach** > **Alle Elemente**
6. Um nur die Service Desk-Widgets anzuzeigen klicken Sie auf **Anzeigen nach** > **Service Desk**
7. Um nur die Geräte-Widgets anzuzeigen klicken Sie auf **Anzeigen nach** > **Geräte**
8. Um nur die Asset Management-Widgets anzuzeigen klicken Sie auf **Anzeigen nach** > **Asset Management**
9. Um nur die Sicherheits-Widgets anzuzeigen, klicken Sie auf **Anzeigen nach** > **Sicherheit**.
10. Um ein Widget anzuzeigen, das derzeit ausgeblendet ist, klicken Sie auf **Installieren**.

Informationen zu Dashboard-Widgets

Dashboard-Widgets bietet einen Überblick über Aktivitäten von Organisationen und Appliances.

In diesem Abschnitt werden die im *Dashboard* verfügbaren Widgets beschrieben. Wenn die Organisationskomponente in Ihrer Appliance aktiviert ist, zeigen Widgets die Informationen für die ausgewählte Organisation auf Administratorebene und die Informationen für das Gerät auf Systemebene.

Widget	Beschreibung
Allgemeine Widgets	Dieser Abschnitt enthält einen groben Überblick über Ihre Appliance-Aktivität. Anhand der in diesen Widgets angezeigten Informationen können Sie sich auf spezifische Indikatoren konzentrieren, anhand derer Sie mögliche Probleme besser nachvollziehen können.
Neueste Nachrichtenartikel und am häufigsten aufgerufene Knowledge Base-Artikel	Diese Widgets liefern Links zu Nachrichten und Informationen von Quest. Die Nachrichtenartikel werden nach Datum oder Wichtigkeit angezeigt. Knowledge Base-Artikel werden nach ihrer Priorität im System des technischen Supports angezeigt.
Verbindungen	Dieses Widget zeigt die Anzahl der Verbindungen zum Webserver der Appliance an. Eine hohe Anzahl zeigt an, dass der Server stark ausgelastet ist, wodurch sich die Reaktionszeit der Appliance verschlechtern kann. Wenn für Ihre Appliance die Organisationskomponente aktiviert ist, zeigt das Widget Informationen für die jeweils ausgewählte Organisation an.
Dateisynchronisierungen	Dieses Widget zeigt die Anzahl der Dateisynchronisierungen an, die derzeit auf vom Agenten verwalteten Geräten vorgenommen werden. Wenn für Ihre Appliance die Organisationskomponente aktiviert ist, zeigt das Widget Informationen für die jeweils ausgewählte Organisation an.
Verwaltete Installationen	Dieses Widget zeigt die Anzahl der verwalteten Installationen an, die derzeit auf vom Agenten verwalteten Geräten vorgenommen werden. Wenn

Widget	Beschreibung
	für Ihre Appliance die Organisationskomponente aktiviert ist, zeigt das Widget Informationen für die jeweils ausgewählte Organisation an.
Aktuelle Skripte	Dieses Widget zeigt die Anzahl der Skripte an, die derzeit auf agentenverwalteten Geräten ausgeführt werden können. Wenn für Ihre Appliance die Organisationskomponente aktiviert ist, zeigt das Widget Informationen für die jeweils ausgewählte Organisation an.
Lizenz-Compliance	Wenn Sie Lizenz-Assets für Software erstellt haben, zeigt dieses Widget die Anzahl der vom Agenten verwalteten Geräte, auf denen eine bestimmte lizenzierte Software installiert ist, sowie die Anzahl verfügbarer Lizenzen an. Wenn für Ihre Appliance die Organisationskomponente aktiviert ist, zeigt das Widget Informationen für die jeweils ausgewählte Organisation an. Lizenz-Assets können für auf den Seiten *Software* oder *Softwarekatalog* aufgeführte Anwendungen erstellt werden. Der Lizenzmodus für Anwendungen muss *Lizenz für Einheit* oder *Unternehmen* lauten, damit Lizenzinformationen in diesem Widget angezeigt werden. Anwendungen mit anderen Lizenzmodi, wie z. B. *Shareware*, *Freeware* oder *Nicht angegeben*, werden in diesem Widget nicht angezeigt. Dieses Widget dient lediglich zu Informationszwecken. Bei der Appliance wird die Lizenz-Compliance nicht erzwungen. Sie verhindert beispielsweise nicht, dass Software auf vom Agenten verwalteten Geräten installiert wird, wenn eine Lizenz abgelaufen ist oder anderweitig gegen die Compliance-Vorgaben verstoßen wird. Diese Farben stehen für die folgenden Schwellenwerte: • **Rot**: Die Nutzung hat den kritischen Schwellenwert erreicht oder überschritten. • **Orange**: Die Nutzung hat den Warnungsschwellenwert erreicht oder überschritten, liegt aber unter dem kritischen Schwellenwert. • **Grün**: Die Nutzung liegt unter dem Warnungsschwellenwert. Informationen zum Ändern der Schwellenwerte finden Sie unter Allgemeine Appliance-Einstellungen ohne aktivierte Organisationskomponente konfigurieren. Weitere Informationen zum Verwalten von Lizenz-Assets finden Sie unter Verwalten des Inventars.
Provisionierung	Dieses Widget zeigt den Status von Provisionierungs- oder Installationsaufgaben des

Widget	Beschreibung
	KACE Agenten an. Wenn für Ihre Appliance die Organisationskomponente aktiviert ist, zeigt das Widget Informationen für die jeweils ausgewählte Organisation an.
Provisionierte Plattformen	Dieses Widget zeigt den Prozentsatz der installierten Betriebssysteme auf durch den Agenten verwalteten Geräten. Wenn für Ihre Appliance die Organisationskomponente aktiviert ist, zeigt das Widget Informationen für die jeweils ausgewählte Organisation an.
Aufgaben werden durchgeführt	Dieses Widget zeigt die Anzahl der derzeit in der Appliance ausgeführten Aufgaben an. Dazu zählen Aufgaben wie Skripterstellung, Inventarisierung, Nutzungserfassung, Replikation, Patching, Bootstrapping und Cache-Abfragen. Sie können den Lastdurchschnitt auf der Appliance anzeigen und den Aufgabendurchsatz bei Bedarf ändern. Siehe Agentenkommunikation und Protokolleinstellungen konfigurieren. Wenn die Organisationskomponente für Ihre Appliance aktiviert wird, ist das Widget auf der Seite *System-Dashboard* verfügbar.
Geräteanmelderate	Diese Auswahl zeigt die Anzahl der Geräte an, die sich während der letzten 60 Minuten mit der Appliance verbunden haben. Wenn die Organisationskomponente in Ihrer Appliance aktiviert ist, ist dieses Widget auf Systemebene verfügbar.
Softwarelizenz-Konfiguration	Wenn Sie Lizenz-Assets für Software einrichten und den Lizenztyp angeben, wie z. B. Standortlizenz, Abonnement oder Einheit, werden diese Informationen in diesem Widget angezeigt. Wenn für Ihre Appliance die Organisationskomponente aktiviert ist, zeigt das Widget Informationen für die jeweils ausgewählte Organisation an.
Datenträgerkapazität	Dieses Widget zeigt an, wie viel Speicherplatz derzeit verwendet wird und wie viel auf der Appliance noch frei ist. Wenn die Organisationskomponente in Ihrer Appliance aktiviert ist, ist dieses Widget auf Systemebene verfügbar.
Softwareherausgeber	Dieses Widget zeigt die im Softwarekatalog definierten Herausgeber mit der höchsten Anzahl an Softwaretiteln an, die auf verwalteten Geräten installiert sind. Wenn für Ihre Appliance die Organisationskomponente aktiviert ist, zeigt das Widget Informationen für die jeweils ausgewählte Organisation an.

Widget	Beschreibung
Softwaretitel	Dieses Widget zeigt die im Softwarekatalog definierten Softwaretitel mit der höchsten Anzahl an Installationen auf verwalteten Geräten an. Wenn für Ihre Appliance die Organisationskomponente aktiviert ist, zeigt das Widget Informationen für die jeweils ausgewählte Organisation an.
Ablaufende Dell Services	Dieses Widget zeigt Informationen zu allen Services von Dell und Links zur Seite mit der *Berichtsliste* für Berichte zum Service von Dell an. Wenn für Ihre Appliance die Organisationskomponente aktiviert ist, zeigt das Widget Informationen für die jeweils ausgewählte Organisation an.
Übersicht über Überwachungswarnungen	Dieses Widget zeigt die Anzahl nicht bestätigter Warnungen gruppiert nach Warnstufe an. Die folgenden Symbole geben die Warnstufe an: • : **Kritisch** • : **Fehler** • : **Warnung** • : **Information** • : **Wiederhergestellt** Wenn für Ihre Appliance die Organisationskomponente aktiviert ist, zeigt das Widget Informationen für die jeweils ausgewählte Organisation an. **Warnungen bei niedrigen Ressourcen.**Wenn nicht mehr genügend Appliance-Ressourcen zur Verfügung stehen, werden im Dashboard kritische Warnungen mit der empfohlenen Vorgehensweise angezeigt, wie beispielsweise Kontaktaufnahme mit dem Support. Diese Warnungen werden generiert, wenn festgestellt wurde, dass die Appliance eine große Menge an Festplattenspeicher CPU und Speicherressourcen beansprucht oder wenn eine große Anzahl von E-Mails eingeht. Kritische Warnungen bei niedrigen Ressourcen werden angezeigt, wenn die betreffende Bedingung innerhalb der letzten zehn Minuten erkannt wurde und vor der Anzeige bereits eine Stunde lang bestand. Die Einstellungen für diese Warnungen werden in den Verlaufseinstellungen verfolgt. Sie können sie durch Löschen einer der Optionen unter *Warnungen bei niedrigen Ressourcen* auf der Seite *Konfiguration der Verlaufseinstellungen* deaktivieren. Weitere Informationen hierzu finden Sie unter Einstellungsverlaufsabonnements auf Systemebene

Widget	Beschreibung
	mit aktivierter Organisationskomponente konfigurieren.
Überwachte Geräte	Dieses Widget zeigt den Status der Geräte an, für die die Überwachung aktiviert wurde. Wenn für Ihre Appliance die Organisationskomponente aktiviert ist, zeigt das Widget Informationen für die jeweils ausgewählte Organisation an.
Überwachungswarnungen	Dieses Widget zeigt die Warnmeldungen für die überwachten Geräte an. Wenn für Ihre Appliance die Organisationskomponente aktiviert ist, zeigt das Widget Informationen für die jeweils ausgewählte Organisation an.
Service Desk-Widgets	Dieser Abschnitt enthält einen groben Überblick über Ihre Service Desk-Ticket-Performance. Nutzen Sie ihn, um schnell den Status Ihrer Tickets zu überprüfen und nach Indikatoren zu suchen, mit denen Sie die Zufriedenheit Ihrer Kunden verbessern können. Sie können zum Beispiel die Anzahl überfälliger Tickets überprüfen und sich nach Bedarf auf bestimmte Probleme konzentrieren. **HINWEIS:** Service Desk-Widgets zeigen Daten für die Standardwarteschlange an, die dem angemeldeten Benutzer zugeordnet ist. Wenn für den Benutzer kein Standard festgelegt ist oder *Alle Warteschlangen* als Standard eingestellt ist, zeigt das Widget Daten von allen Warteschlangen im Besitz dieses Benutzers an. **HINWEIS:** Wenn der Benutzer keine Warteschlange besitzt oder seine Standardwarteschlange nicht mehr gültig ist, zeigen die Widgets keine Daten an.
Verknüpfungen	Dieses Widget enthält Links zu allgemeinen Service Desk-Aktionen. Verwenden Sie es, um bestimmte Aufgaben schnell zu initiieren, z. B. das Erstellen eines neuen KB-Artikels (Knowledge Base), die Planung eines Berichts usw.
Ansichten	Dieses Widget enthält Links zu allgemeinen Service Desk-Seiten und -Assistenten, einschließlich benutzerdefinierten Ansichten, die Sie erstellt haben. Verwenden Sie es, um schnell zu bestimmten Seiten zu navigieren, wie z. B. *Meine letzten Tickets*, *Nicht zugewiesene Tickets* und *Heute fällige Tickets.* Außerdem wird der Link zu benutzerdefinierten Ansichten angezeigt. Die Liste der benutzerdefinierten Ansichten ist alphabetisch sortiert. Wenn die benutzerdefinierten Ansichten in einer bestimmten Reihenfolge angezeigt werden sollen, können Sie ihre Namen bei Bedarf mit Nummern versehen.

Widget	Beschreibung
Berichte	Dieses Widget enthält Links zu allgemeinen Service Desk-Berichten. Verwenden Sie sie, um schnell einen bestimmten Bericht zu erstellen, z. B. *Offene Tickets der letzten 7 Tagen nach Eigentümer*, *Blockierte/offene Tickets nach Eigentümer* und andere.
Heute geöffnete Tickets	Dieser Assistent enthält die Anzahl der heute geöffneten Service-Desk-Tickets.
Aktive Tickets nach Benutzer Aktive Tickets nach Kategorie Aktive Tickets nach Priorität Aktive Tickets Abgeschlossene Tickets Überfällige Tickets Überfällige Tickets nach Benutzer Heute überfällige Tickets Heute fällige Tickets Erneut geöffnete Tickets	Diese Widgets zeigen die Anzahl der aktiven, geschlossenen, überfälligen, heute überfälligen, fälligen, heute fälligen oder erneut geöffneten Service-Desk-Tickets, die nach einem der folgenden Parameter gruppiert sind: • Kategorie • Priorität • Besitzer • Warteschlange • Bereich Die resultierenden Daten können in einem *Balkendiagramm* oder einem *Ringdiagramm* angezeigt werden. Um den Widget-Titel zu ändern, wählen Sie, wie Sie die Tickets gruppieren möchten, oder wählen Sie den Diagrammtyp aus und klicken Sie auf im Widget. Nehmen Sie im daraufhin angezeigten Dialogfeld Ihre Änderungen vor und klicken Sie auf **Speichern**.
Durchschnittliche Ticket-Auflösungszeit	Dieses Widget zeigt die durchschnittlichen Auflösungszeiten eines Tickets nach einer der folgenden Kategorien an: • Kategorie • Priorität • Besitzer • Warteschlange • Monat Die resultierenden Daten können in einem *Balkendiagramm* oder einem *Ringdiagramm* angezeigt werden. Um den Widget-Titel zu ändern, wählen Sie, wie Sie die Tickets gruppieren möchten, oder wählen Sie den Diagrammtyp aus und klicken Sie auf im Widget. Nehmen Sie im daraufhin angezeigten Dialogfeld Ihre Änderungen vor und klicken Sie auf **Speichern**.

Widget	Beschreibung
Überfällige Tickets	Dieses Widget zeigt die Anzahl der derzeit überfälligen Service-Desk-Tickets an.
Geräte-Widgets	Dieser Abschnitt enthält einen groben Überblick über Ihre verwalteten Geräte. Verwenden Sie ihn, um den Status Ihrer Geräte schnell zu überprüfen und nach Indikatoren zu suchen, die ihre Leistung verbessern können. Sie können beispielsweise den verfügbaren Speicherplatz in Prozent überprüfen und sich nach Bedarf auf bestimmte Probleme konzentrieren.
Geräte nach Speicher	Dieses Widget zeigt ein Balkendiagramm an, in dem jeder Balken für eine Reihe von Geräten steht, auf denen eine angegebene RAM-Größe installiert ist.
Geräte nach Prozessor	Dieses Widget zeigt ein Balkendiagramm an, in dem jeder Balken für eine Reihe von Geräten steht, die eine bestimmte Prozessorkonfiguration aufweisen.
Geräte nach Datenträgerkapazität	Dieses Widget zeigt eine Ringdiagramm an, in dem die einzelnen „Tortenstücke“ des Diagramms den freien Speicherplatz in Prozent auf den verwalteten Geräten angeben. Durch Klicken auf den Widget-Titel wird ein Bericht mit Links zu den zugeordneten Geräten angezeigt. Wenn Sie mit der Maus über die einzelnen „Tortenstücke“ des Diagramms fahren, kann der prozentuale Anteil an verwalteten Geräten angezeigt werden, die über den ausgewählten prozentualen Anteil an freiem Speicherplatz verfügen. Wenn Sie beispielsweise über das rote „Tortenstück“ im Diagramm fahren, zeigt das Widget den Prozentsatz an Geräten an, deren freier Speicherplatz unter 25 % liegt.
Verwaltete Betriebssysteme	Dieses Widget zeigt den Prozentsatz der verwalteten Geräte an, die mit dem jeweiligen Betriebssystem laufen. Wenn für Ihre Appliance die Organisationskomponente aktiviert ist, zeigt dieses Widget die Anzahl der Geräte für die jeweils ausgewählte Organisation als Prozentsatz an.
Geräte nach Hersteller	Dieses Widget zeigt die wichtigsten Gerätehersteller aus dem Geräteinventar an. Wenn für Ihre Appliance die Organisationskomponente aktiviert ist, zeigt dieses Widget die Anzahl der Geräte für die jeweils ausgewählte Organisation als Prozentsatz an.
Geräte nach Modell	Dieses Widget zeigt die wichtigsten Gerätemodelle aus dem Geräteinventar an. Wenn für Ihre Appliance die Organisationskomponente aktiviert ist, zeigt dieses Widget die Anzahl der Geräte für die jeweils ausgewählte Organisation als Prozentsatz an.

Widget	Beschreibung
Geräte nach Untertyp	Dieses Widget zeigt ein Ringdiagramm an, in dem die Abschnitte des Diagramms den Prozentsatz der verwalteten Geräte nach Geräte-Untertyp angeben.
VMware-Geräteanzahl	Dieses Widget zeigt die Anzahl der einzelnen VMware-Gerätetypen an, z. B. vCenter, ESXi-Hosts, virtuelle Maschinen und bereitgestellte virtuelle Maschinen. Wenn Sie auf den Titel des Widgets klicken, wird die Seite mit der *Geräteliste* angezeigt.
VMware-Geräteberichte	Dieses Widget enthält Links zu fünf beliebten VMware-Inventarberichten. Wenn Sie auf den Titel des Widgets klicken, wird die Seite mit der Liste der *Berichte* angezeigt, auf der der Filter für die *virtuelle Infrastruktur* angewendet wird.
VMware ESXi-Gerät nach Status	Dieses Widget zeigt ein Ringdiagramm an, das den aktuellen Status von ESXi-Geräten darstellt. Es gibt vier mögliche Werte: *OK*, *Warnung*, *Fehler* und *Unbekannt*. Wenn Sie auf den Widget-Titel klicken, wird ein neuer VMware-Bestandsbericht angezeigt, in dem alle ESXi-Geräte nach aktuellem Status aufgelistet sind.
Anzahl der VMware ESXi-Versionen	Dieses Widget zeigt die Anzahl der fünf wichtigsten ESXi-Versionen an. Wenn Sie auf den Widget-Titel klicken, wird ein neuer VMware-Bestandsbericht angezeigt, der alle ESXi-Geräte nach Version auflistet.
Asset Management-Widgets	Dieser Abschnitt enthält einen groben Überblick über Ihre Asset-Nutzung. Nutzen Sie es, um schnell den Status Ihrer Assets zu überprüfen und nach Indikatoren zu suchen, mit denen Sie Ihre Asset-Konfiguration verbessern können. Zum Beispiel, können Sie sich darauf konzentrieren, wie Ihre Softwarelizenzen verwendet werden, und ermitteln, für welche Softwaretitel die Lizenz erneuert werden muss.
Assets nach Typ	Dieses Widget zeigt ein Ringdiagramm an, bei dem jeder Abschnitt des Diagramms den Prozentsatz Ihrer Assets nach Asset-Typ angibt, wie Gerät, Software, Standort, Lizenz und andere. Wenn Sie den Mauszeiger über die einzelnen Abschnitte des Diagramms bewegen, wird der Prozentsatz der Assets des ausgewählten Typs angezeigt.
Assets nach Status	Dieses Widget zeigt ein Ringdiagramm an, bei dem jeder Abschnitt des Diagramms den Prozentsatz Ihrer Assets nach Status angibt, wie z. B. aktiv, entsorgt, fehlt oder andere. Wenn Sie mit der Maus über die einzelnen Abschnitte des Diagramms fahren, wird der Prozentsatz an Assets mit dem ausgewählten Status angezeigt.

Widget	Beschreibung
Kosten ($) von ungenutzten Lizenzen nach Produkt	Dieses Widget zeigt ein Balkendiagramm, wobei jeder Balken für die Kosten der jeweils ungenutzten Lizenzen für ein Produkt steht. Sie können diese Informationen verwenden, um ungenutzte Lizenzen neu zuzuweisen oder zu stornieren und zur Umleitung der Ressourcen an die Stellen, wo sie am meisten gebraucht werden.
Lizenz-Compliance	Wenn Sie Lizenz-Assets für Software erstellt haben, zeigt dieses Widget die Anzahl der vom Agenten verwalteten Geräte, auf denen eine bestimmte lizenzierte Software installiert ist, sowie die Anzahl verfügbarer Lizenzen an. Wenn für Ihre Appliance die Organisationskomponente aktiviert ist, zeigt das Widget Informationen für die jeweils ausgewählte Organisation an. Lizenz-Assets können für auf den Seiten *Software* oder *Softwarekatalog* aufgeführte Anwendungen erstellt werden. Der Lizenzmodus für Anwendungen muss *Lizenz für Einheit* oder *Unternehmen* lauten, damit Lizenzinformationen in diesem Widget angezeigt werden. Anwendungen mit anderen Lizenzmodi, wie z. B. *Shareware*, *Freeware* oder *Nicht angegeben*, werden in diesem Widget nicht angezeigt. Dieses Widget dient lediglich zu Informationszwecken. Bei der Appliance wird die Lizenz-Compliance nicht erzwungen. Sie verhindert beispielsweise nicht, dass Software auf vom Agenten verwalteten Geräten installiert wird, wenn eine Lizenz abgelaufen ist oder anderweitig gegen die Compliance-Vorgaben verstoßen wird. Diese Farben stehen für die folgenden Schwellenwerte: • **Rot**: Die Nutzung hat den kritischen Schwellenwert erreicht oder überschritten. • **Orange**: Die Nutzung hat den Warnungsschwellenwert erreicht oder überschritten, liegt aber unter dem kritischen Schwellenwert. • **Grün**: Die Nutzung liegt unter dem Warnungsschwellenwert. Informationen zum Ändern der Schwellenwerte finden Sie unter Allgemeine Appliance-Einstellungen ohne aktivierte Organisationskomponente konfigurieren. Weitere Informationen zum Verwalten von Lizenz-Assets finden Sie unter Verwalten des Inventars.
Softwaretitel	Dieses Widget zeigt die im Softwarekatalog definierten Softwaretitel mit der höchsten Anzahl an Installationen auf verwalteten Geräten an. Wenn für Ihre Appliance die Organisationskomponente

Widget	Beschreibung
	aktiviert ist, zeigt das Widget Informationen für die jeweils ausgewählte Organisation an.
Softwareherausgeber	Dieses Widget zeigt die im Softwarekatalog definierten Herausgeber mit der höchsten Anzahl an Softwaretiteln an, die auf verwalteten Geräten installiert sind. Wenn für Ihre Appliance die Organisationskomponente aktiviert ist, zeigt das Widget Informationen für die jeweils ausgewählte Organisation an.
Assets nach Standort	Dieses Widget zeigt ein Ringdiagramm an, in dem die Abschnitte des Diagramms den Prozentsatz der Assets nach Standort angeben. Wenn Sie mit der Maus über die einzelnen Abschnitte des Diagramms fahren, wird der Prozentsatz an Assets mit dem ausgewählten Standort angezeigt.
Installierte, aber in 60 Tagen nicht verwendete Software	Dieses Widget zeigt ein Balkendiagramm an, wobei jeder Balken einen Softwaretitel und die entsprechende Anzahl der Instanzen des jeweiligen Produkts darstellt, die in den letzten 60 Tagen nicht genutzt wurden. Sie können diese Informationen verwenden, um weiter zu untersuchen, ob diese Titel erforderlich sind, zum erneuten Zuweisen oder Deinstallieren nicht verwendeter Software und zur Umleitung der Ressourcen an die Stellen, wo sie am meisten gebraucht werden.
Wartung ablaufender Software-Lizenzen	Dieses Widget zeigt ein vertikales Balkendiagramm an, wobei jeder Balken für die Anzahl der Softwarelizenzen steht, die in einem bestimmten Zeitraum ablaufen werden.
Wartung abgelaufener Software-Lizenzen	Dieses Widget zeigt ein Ringdiagramm an, das das Verhältnis der abgelaufenen zu den aktuellen Lizenzen darstellt. Wenn Sie den Mauszeiger über die einzelnen Abschnitte des Diagramms bewegen, wird je nach Auswahl der Prozentsatz der abgelaufenen oder aktuellen Softwarelizenzen angezeigt.
Ablaufende Verträge	Dieses Widget zeigt ein vertikales Balkendiagramm an, wobei jeder Balken für die Anzahl der Verträge steht, die in einem bestimmten Zeitraum ablaufen werden.
Abgelaufene Verträge	Dieses Widget zeigt ein Ringdiagramm an, das das Verhältnis der abgelaufenen zu den aktuellen Verträgen darstellt. Wenn Sie den Mauszeiger über die einzelnen Abschnitte des Diagramms bewegen, wird je nach Auswahl der Prozentsatz der abgelaufenen oder aktuellen Verträge angezeigt.
Softwarelizenz-Konfiguration	Wenn Sie Lizenz-Assets für Software einrichten und den Lizenztyp angeben, wie z. B. Standortlizenz,

Widget	Beschreibung
	Abonnement oder Einheit, werden diese Informationen in diesem Widget angezeigt. Wenn für Ihre Appliance die Organisationskomponente aktiviert ist, zeigt das Widget Informationen für die jeweils ausgewählte Organisation an.
Sicherheits-Widgets	Dieser Abschnitt bietet einen Überblick über die Patch-Compliance in Ihrer Umgebung und die Informationen über Patching-Prozesse. Dadurch können Sie schnell die Stufe der auf den verwalteten Geräten installierten System-Patches überprüfen und nach Indikatoren suchen, mit denen Sie die Systemsicherheit verbessern können.
Compliance der kritischen Patches	Dieses Widget zeigt den Fortschritt in der Bereitstellung der Patches an, die als kritisch gekennzeichnet sind. Wenn für Ihre Appliance die Organisationskomponente aktiviert ist, zeigt das Widget Informationen für die jeweils ausgewählte Organisation an.
Dell Aktualisierungen	Dieses Widget zeigt die Anzahl der Dell Anwendungen, die BIOS-Anzahl und die Anzahl der Firmwareaktualisierungen, die auf verwaltete Geräte angewendet werden können. Die Aktualisierungen werden abhängig von der Priorität der Aktualisierung als *Angemessen*, *Wichtig* oder *Kritisch* kategorisiert. Nach dem Erstellen eines Dell Aktualisierungszeitplans werden Daten im Widget angezeigt. Siehe Dell Aktualisierungszeitpläne konfigurieren. Wenn für Ihre Appliance die Organisationskomponente aktiviert ist, zeigt das Widget Informationen für die jeweils ausgewählte Organisation an.
Compliance nach Computer	Dieses Widget zeigt ein Ringdiagramm an, in dem die einzelnen Abschnitte des Diagramms den freien Speicherplatz in Prozent auf den verwalteten Geräten angeben. Wenn Sie den Mauszeiger über die einzelnen Abschnitte des Diagramms bewegen, wird der Prozentsatz der Patch-Compliance des ausgewählten Geräts angezeigt. Sie können die im Widget angezeigten Informationen ändern, indem Sie den Patch-Herausgeber, das Betriebssystem, das Label, die Klassifizierung, den Schweregrad, die KB-Nummer und das Verfügbarkeitsdatum auswählen. Sie können je nach Bedarf auch zwischen Balkendiagramm- und Ringdiagramm-Ansichten wechseln. Sie können auch mehrere Instanzen des Widgets auf dem Sicherheits-Dashboard installieren, wobei in jeder Instanz ein anderer Parametersatz verwendet wird.

Widget	Beschreibung
Compliance nach Patch	Dieses Widget zeigt ein Ringdiagramm an, in dem die Abschnitte des Diagramms den Prozentsatz der Compliance für die einzelnen anwendbaren Patches angeben. Wenn Sie den Mauszeiger über die einzelnen Abschnitte des Diagramms bewegen, wird der Prozentsatz der Compliance für den ausgewählten Patch angezeigt. Sie können die im Widget angezeigten Informationen ändern, indem Sie den Patch-Herausgeber, das Betriebssystem, das Label, die Klassifizierung, den Schweregrad, die KB-Nummer und das Verfügbarkeitsdatum auswählen. Sie können je nach Bedarf auch zwischen Balkendiagramm- und Ringdiagramm-Ansichten wechseln. Sie können auch mehrere Instanzen des Widgets auf dem Sicherheits-Dashboard installieren, wobei in jeder Instanz ein anderer Parametersatz verwendet wird.
Patch-Installationsfortschritt	Dieses Widget zeigt den Fortschritt der Patch-Aufgaben an, die derzeit auf verwalteten Geräten laufen. Wenn für Ihre Appliance die Organisationskomponente aktiviert ist, zeigt das Widget Informationen für die jeweils ausgewählte Organisation an.
Bereitgestellte Patches	Dieses Widget zeigt die Anzahl der derzeit bereitgestellten Patches an. Sie können die im Widget angezeigten Informationen ändern, indem Sie den Patch-Herausgeber, das Betriebssystem, das Label, die Klassifizierung, den Schweregrad, die KB-Nummer und das Verfügbarkeitsdatum auswählen. Sie können je nach Bedarf auch zwischen Balkendiagramm- und Ringdiagramm-Ansichten wechseln. Sie können auch mehrere Instanzen des Widgets auf dem Sicherheits-Dashboard installieren, wobei in jeder Instanz ein anderer Parametersatz verwendet wird.
Fehlerhafte Patches	Dieses Widget zeigt die Anzahl der Patches an, die nicht bereitgestellt werden konnten. Sie können die im Widget angezeigten Informationen ändern, indem Sie den Patch-Herausgeber, das Betriebssystem, das Label, die Klassifizierung, den Schweregrad, die KB-Nummer und das Verfügbarkeitsdatum auswählen. Sie können je nach Bedarf auch zwischen Balkendiagramm- und Ringdiagramm-Ansichten wechseln. Sie können auch mehrere Instanzen des Widgets auf dem Sicherheits-Dashboard installieren, wobei in jeder Instanz ein anderer Parametersatz verwendet wird.

Widget	Beschreibung
Freigegebene Patches	Dieses Widget zeigt die Anzahl der Patches an, die freigegeben und für die Bereitstellung verfügbar sind. Sie können die im Widget angezeigten Informationen ändern, indem Sie den Patch-Herausgeber, das Betriebssystem, das Label, die Klassifizierung, den Schweregrad, die KB-Nummer und das Verfügbarkeitsdatum auswählen. Sie können je nach Bedarf auch zwischen Balkendiagramm- und Ringdiagramm-Ansichten wechseln. Sie können auch mehrere Instanzen des Widgets auf dem Sicherheits-Dashboard installieren, wobei in jeder Instanz ein anderer Parametersatz verwendet wird.
Patch-Aufgaben abgeschlossen	Dieses Widget zeigt den Fortschritt der Patch-Aufgaben wie Erkennungs-, Bereitstellungs- und Rollback-Aufgaben an, die derzeit auf verwalteten Geräten laufen. Wenn für Ihre Appliance die Organisationskomponente aktiviert ist, zeigt das Widget Informationen für die jeweils ausgewählte Organisation an.
Berichte	Dieses Widget enthält Links zu häufig verwendeten Patching-Berichten. Sie können damit schnell Berichte zu bestimmten Themen erstellen wie *Liste mit kritischen und aktuellen Bulletins*, *Nicht kompatible Geräte nach Patch* und andere.
SCAP-Zusammenfassung	Dieses Widget liefert Informationen zu den SCAP-Scans, die an Geräten durchgeführt wurden. Wenn für Ihre Appliance die Organisationskomponente aktiviert ist, zeigt das Widget Informationen für die jeweils ausgewählte Organisation an.
Ansichten	Dieses Widget enthält Links zu allgemeinen Patching-Seiten und -Assistenten, einschließlich benutzerdefinierten Ansichten, die Sie erstellt haben. Sie können damit schnell zu bestimmten Seiten navigieren, z. B. zum *Patch-Katalog*. Wenn Sie benutzerdefinierte Ansichten angelegt haben, werden diese alphabetisch sortiert. Wenn die benutzerdefinierten Ansichten in einer bestimmten Reihenfolge angezeigt werden sollen, können Sie ihre Namen bei Bedarf mit Nummern versehen.
Windows 10 Versionen	Dieses Widget zeigt ein Balkendiagramm an, wobei jedes Element im Diagramm eine bestimmte Windows 10-Version und die Anzahl der verwalteten Geräte darstellt, auf denen diese Version ausgeführt wird. So können Sie sich ein Bild davon machen, wie viele Geräte für veröffentlichte Windows 10-Aktualisierungen geeignet sind.

Dashboard-Details anzeigen

In den Dashboard-Details sehen Sie Statistiken für die Appliance oder die ausgewählte Organisation.

Wenn auf der Appliance die Organisationskomponente aktiviert ist und Sie an der Administratorkonsole angemeldet sind (`http://`**appliance_hostname**`/admin`), werden für die ausgewählte Organisation statistische Daten angezeigt. Wenn Sie an der Systemadministratorkonsole angemeldet sind (`http://`**appliance_hostname**`/system`), werden die statistischen Daten für die Appliance, einschließlich aller Organisationen, angezeigt.

Auf neuen Appliances ohne verwaltete Geräte zeigt die Seite *Dashboad-Detail* null oder keine Datensätze an.

1. Führen Sie einen der folgenden Schritte aus:
   - **Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`appliance_hostname`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option** *Organisationsmenü in Verwaltungskopfzeile anzeigen* **aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.**
   - **Melden Sie sich bei der Systemadministratorkonsole der Appliance an: `https://`appliance_hostname`/system`. Oder wählen Sie in der Dropdown-Liste rechts oben auf der Seite den Eintrag System aus.**
2. Klicken Sie auf **Startseite** > **Dashboard**.

   Die Seite *Dashboard* oder *System-Dashboard* wird angezeigt.
3. Klicken Sie in der oberen rechten Ecke der Seite auf **Details anzeigen**.

   Die *Dashboard-Detailseite* wird angezeigt. Sie enthält folgende Informationen:

Abschnitt in der Übersicht	Beschreibung
Warnungen	Informationen zur Lizenzkapazität und -verwendung für verwaltete Geräte im Inventar.
Geräte	Informationen über verwaltete Geräte mit einer Übersicht über die verwendeten Betriebssysteme. Zudem werden Sie hier benachrichtigt, wenn die Anzahl der verwalteten Geräte die Anzahl der gemäß Ihrem Lizenzschlüssel zulässigen überschreitet.
Software	Eine Übersicht über die Anwendungen, die im Inventar der Appliance verfügbar sind. Hierzu zählen Anwendungen, die auf der Seite *Software* und auf der Seite *Softwarekatalog* aufgeführt sind.
Verteilungen	Die Anwendungen, die auf die verwalteten Geräte verteilt und von der Verteilungsmethode getrennt wurden. In diesem Abschnitt wird auch die Anzahl der Pakete angezeigt, die aktiviert und deaktiviert wurden.
Übersicht über Überwachungswarnungen	Die Anzahl nicht bestätigter Warnungen für überwachte Geräte gruppiert nach Warnstufe.

Abschnitt in der Übersicht	Beschreibung
	Die folgenden Symbole geben die Warnstufe an: • : **Kritisch** • : **Fehler** • : **Warnung** • : **Information** • : **Wiederhergestellt**
Übersicht über die Benachrichtigungen	Die Alarmfunktionen, die auf verwaltete Geräte verteilt wurden, sind nach Alarmtyp getrennt. In dieser Zusammenfassung wird auch die Anzahl der Benachrichtigungen angegeben, die aktiv oder abgelaufen sind. Der *IT-Tipp* bezieht sich auf die Anzahl der Knowledge Base-Artikel in der **Benutzerkonsole**.
Patches	Die von Softwareanbietern wie Microsoft® und Apple bereitgestellten Patches. In der Übersicht werden Datum und Uhrzeit des letzten Patches (erfolgreich und versucht), die Gesamtzahl der Patches und die Gesamtzahl der heruntergeladenen Pakete angezeigt.
OVAL	Informationen zu OVAL-Tests (Open Vulnerability Assessment Language), die ausgeführt werden können, um Sicherheitsrisiken auf verwalteten Geräten zu identifizieren. Die OVAL-Informationen umfassen: • Empfangene Definitionen • Datum und Uhrzeit des letzten OVAL-Downloads (erfolgreich und versucht) • Anzahl der OVAL-Tests in der Appliance • Die Anzahl der überprüften Geräte • Die Anzahl der Sicherheitslücken, die auf verwalteten Geräten erkannt wurden
Erkennung (Netzwerk-Scan)	Die Ergebnisse von Erkennungsscans, die im Netzwerk durchgeführt werden, einschließlich der Anzahl der überprüften IP-Adressen, der Anzahl der erkannten Dienste sowie der Anzahl der durchgeführten Scans.

HINWEIS: Mit jedem Aktualisieren der Seite wird die Datenzählung aktualisiert. Neue Appliance-Installationen enthalten null Datensätze.

Weitere Informationen zu OVAL finden Sie unter Aufrechterhalten der Geräte- und Appliance-Sicherheit.

Aufgabenpläne anzeigen

Auf der Seite *Aufgabenplanung* wird eine Liste der Aufgaben angezeigt, die entsprechend der Auswahl für die aktuelle Stunde, den Tag oder die Woche geplant sind. Die Anzeige erfolgt anhand der Startzeiten und einer geschätzten Dauer basierend auf den Maschinenwerten und Aufgabentypen. Alle Aufgaben, denen Detailseiten zugeordnet sind, z. B. Skripte, können durch Anklicken des Aufgabennamens in der Tabelle aufgerufen werden.

Das **Administratorkonsole** zeigt die Aufgaben an, die der ausgewählten Organisation zugeordnet sind, sowie alle Systemaufgaben, wie etwa das *Sicherungsfenster*. Wenn Sie diese Seite in der **Systemverwaltungskonsole** anzeigen, werden alle Aufgaben von allen Organisationen (getrennt nach Organisation) zusammen mit allen verfügbaren Systemaufgaben angezeigt.

Alle Aufgabenabfolgen, die auf der Seite erscheinen, werden mit Verbindungslinien dargestellt. Weitere Informationen über Aufgabenabfolgen finden Sie unter Verwenden von Aufgabenabfolgen.

Aufgaben, die mit mehreren Agenten und Geräten verknüpft sind, werden in einer Verlaufslinie angezeigt, wobei die Länge der Linie die Dauer der Aufgabe oder historische Daten nicht widerspiegelt. Durchgehende Farblinien weisen auf Aufgaben mit einer festen Dauer hin. Ein blauer vertikaler Balken im Diagramm steht für das aktuelle Datum und die aktuelle Uhrzeit.

1. Führen Sie einen der folgenden Schritte aus:
   - **Melden Sie sich bei der Administratorkonsole der Appliance an: `https://appliance_hostname/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option** *Organisationsmenü in Verwaltungskopfzeile anzeigen* **aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.**
   - **Melden Sie sich bei der Systemadministratorkonsole der Appliance an: `https://appliance_hostname/system`. Oder wählen Sie in der Dropdown-Liste rechts oben auf der Seite den Eintrag System aus.**

   Die Seite *Dashboard* oder *System-Dashboard* wird angezeigt.
2. Klicken Sie in der linken Navigationsleiste im Abschnitt **Startseite** auf **Aufgabenplanung**.

   Die Seite *Aufgabenplanung* wird angezeigt.
3. Um zwischen verschiedenen Detailebenen zu wechseln, klicken Sie je nach Bedarf auf **Stunde**, **Tag** oder **Woche**.

Version, Modell und Lizenzinformationen der Appliance anzeigen

Unter dem Link **Informationen zur Appliance** im Bereich *Hilfe* finden Sie die Version, das Modell und die Lizenzinformationen der Appliance.

1. Melden Sie sich an der Benutzerkonsole, Administratorkonsole oder der Systemkonsole an.
2. Klicken Sie in der oberen rechten Ecke der Administratorkonsole auf **Benötigen Sie Hilfe?**.

   Auf der rechten Seite wird ein Hilfefenster mit allgemeinen Informationen über die zugehörige **Administratorkonsole**-Seite angezeigt. Am unteren Rand des Hilfebereichs befinden sich die folgenden Schaltflächen:
   - **Appliance Administratorhandbuch**(📖): Bietet Zugriff auf den Hilfeinhalt der KACE Systemverwaltungs-Appliance.
   - **Knowledge-Base** (🎓): Ermöglicht Ihnen, nach Knowledge Base-Artikeln zu suchen, die sich auf die zugehörige **Administratorkonsole**-Seite beziehen.

> **HINWEIS:** Diese Option ist nur in der **Administratorkonsole** und der Systemkonsole verfügbar. Sie erscheint nicht in der **Benutzerkonsole**.

- **Video Knowledge Base** (): Ermöglicht Ihnen, nach weiteren Schulungsvideos zu suchen, die sich auf die zugehörige **Administratorkonsole**-Seite beziehen. Sie können ein Video im Hilfebereich, in einem kleineren Fenster außerhalb der Seite oder auf der Knowledge Base-Seite des Ziels wiedergeben, auf der das Video gehostet wird.

  > **HINWEIS:** Diese Option ist nur verfügbar, wenn zugehörige Videos im Support-Portal verfügbar sind. Sie wird zudem nur in der **Administratorkonsole** und der Systemkonsole angezeigt. Sie erscheint nicht in der **Benutzerkonsole**.

- **Live-Chat** (): Startet einen Chat mit einem Produktspezialisten für die KACE Systemverwaltungs-Appliance.

  > **HINWEIS:** Diese Option ist nur in der **Administratorkonsole** und der Systemkonsole verfügbar. Sie erscheint nicht in der **Benutzerkonsole**.

- **Ticket öffnen** (): Stellt Links zur Support-Seite (https://support.quest.com/create-service-request) her, auf der Sie eine Serviceanfrage erstellen können.

  > **HINWEIS:** Diese Option ist nur in der **Administratorkonsole** und der Systemkonsole verfügbar. Sie erscheint nicht in der **Benutzerkonsole**.

- **Support** (): Stellt Links zur Seite **Einstellungen > Support** her. Auf dieser Seite sehen Sie Ressourcen zur Fehlerbehebung bei Systemverwaltungsproblemen und zur Kontaktaufnahme mit dem **Quest Support**.

  > **HINWEIS:** Diese Option ist nur in der **Administratorkonsole** und der Systemkonsole verfügbar. Sie erscheint nicht in der **Benutzerkonsole**.

- **KACE GO Mobile App** (): Zeigt ein Dialogfeld mit Links zum Herunterladen der KACE GO Mobile App an. Die App ist für iOS- und Android-Plattformen verfügbar.

  > **HINWEIS:** Diese Option ist verfügbar, wenn die Appliance für die Interaktion mit der K1 GO Mobile App konfiguriert wurde. Sie erscheint nur in der **Administratorkonsole** und der Systemkonsole. Sie erscheint nicht in der **Benutzerkonsole**. Weitere Informationen zum Aktivieren des mobilen Zugriffs finden Sie unter Konfigurieren des Mobilgerätezugriffs.

- **Info** (): Zeigt Informationen zu Ihrer Installation der KACE Systemverwaltungs-Appliance an.

  > **HINWEIS:** Diese Option ist nur in der **Administratorkonsole** und der Systemkonsole verfügbar. Sie erscheint nicht in der **Benutzerkonsole**.

3. Klicken Sie unten rechts auf der Seite auf den Link **Info**.

   Die Lizenzinformationen der Appliance werden angezeigt.

   - Version, Modell und Seriennummern der Appliance.
   - Das Ablaufdatum der Lizenz im Format `Jahr/Monat/Tag`.
   - Die Anzahl der verwalteten Computer, überwachten Server und Assets, die Sie mit Ihrer Lizenz verwalten können.

     Verwaltete Computer sind Geräte im Appliance-Inventar, 1) auf denen Windows, Mac, Linux oder UNIX Betriebssysteme installiert sind, 2) die als PCs oder Server eingestuft werden und 3) die dem Inventar nicht manuell, über die WSAPI oder mithilfe der Verwaltung von Mobilgeräten hinzugefügt wurden.
     Überwachte Server sind Server, 1) die die Anforderungen für verwaltete Computer erfüllen und 2) auf denen die Überwachung aktiviert ist.
     Zu den **Assets**, die auf das Lizenzlimit angerechnet werden, zählen Geräte, die 1) dem Appliance-Inventar hinzugefügt wurden, aber nicht der Definition verwalteter Computer oder überwachter Server entsprechen und 2) dem Inventar nicht manuell, über die WSAPI oder mithilfe der Verwaltung von

Mobilgeräten hinzugefügt wurden. Beispiele für Assets: Drucker, Projektoren, Netzwerkausrüstung und Speichergeräte. Die mit der Asset Management-Komponente erstellten und verwalteten Assets werden nicht auf das Lizenzlimit angerechnet.

> **HINWEIS:** Mit Ihrer Produktlizenzvereinbarung können Sie eine festgelegte Anzahl von Geräten verwalten. Beachten Sie, dass Geräte auf diese Limits angerechnet werden, selbst wenn die Geräte als "Ausstehend" (MIA, Missing in Action) eingestuft sind oder nicht mehr verwendet werden. Geräte, die dem Inventar manuell oder über die API hinzugefügt wurden, werden bei den Lizenzlimits dagegen nicht berücksichtigt. Weitere Informationen hierzu finden Sie unter https://quest.com/docs/Product_Guide.pdf.
>
> **HINWEIS:** Rufen Sie zum Erhöhen der Lizenzkapazität die Quest Website auf: https://quest.com/buy.

- Lizenzbedingungen.
- Code von Drittanbietern.

Optional: Zeigen Sie die Lizenzinformationen der Appliance mit aktivierten Komponenten an. Siehe Produktlizenzinformationen anzeigen.

Produktlizenzinformationen anzeigen

Die Lizenzinformationen der Appliance werden im Abschnitt *Appliance-Aktualisierungen* der **Administratorkonsole** angezeigt.

1. Navigieren Sie zur *Systemsteuerung* der Appliance:
   - **Wenn die Organisationskomponente nicht für die Appliance aktiviert ist, melden Sie sich bei der Administratorkonsole an: `https://appliance_hostname/admin`, und wählen Sie dann Einstellungen > Systemsteuerung aus.**
   - **Wenn die Organisationskomponente für die Appliance aktiviert ist, melden Sie sich bei der Systemverwaltungskonsole der Appliance an: `https://appliance_hostname/system`. Oder wählen Sie in der Dropdown-Liste rechts oben auf der Seite den Eintrag System aus, und klicken Sie dann auf Einstellungen > Systemsteuerung.**
2. Klicken Sie auf **Appliance-Aktualisierungen**.
3. Klicken Sie im Abschnitt *Lizenzinformationen* auf die Schaltfläche **Hilfe**: ?.

   Die folgenden Informationen werden angezeigt:

   - **Verwaltete Computer**: Die Anzahl der verwalteten Computer, die Sie mit Ihrer Lizenz verwalten dürfen. **Verwaltete Computer** sind Geräte im Inventar, 1) auf denen Windows, Mac, Linux oder UNIX Betriebssysteme installiert sind, 2) die als PCs oder Server eingestuft werden und 3) die dem Inventar nicht manuell, über die WSAPI oder mithilfe der Verwaltung von Mobilgeräten hinzugefügt wurden.
   - **Überwachte Server**: Die Anzahl der überwachten Server, die Sie mit Ihrer Lizenz verwalten dürfen. **Überwachte Server** sind Server, 1) die die Anforderungen für verwaltete Computer erfüllen und 2) auf denen die Überwachung aktiviert ist.
   - **Assets**: Zu den **Assets**, die auf das Lizenzlimit angerechnet werden, zählen Geräte, die 1) dem Inventar hinzugefügt wurden, aber nicht der Definition verwalteter Computer oder überwachter Server entsprechen und 2) dem Inventar nicht manuell, über die WSAPI oder mithilfe der Verwaltung von Mobilgeräten hinzugefügt wurden. Beispiele für Assets: Drucker, Projektoren, Netzwerkausrüstung und Speichergeräte. Die mit der Asset Management-Komponente erstellten und verwalteten Assets werden nicht auf das Lizenzlimit angerechnet.

> **HINWEIS:** Mit Ihrer Produktlizenzvereinbarung können Sie eine festgelegte Anzahl von Geräten verwalten. Beachten Sie, dass Geräte auf diese Limits angerechnet werden, selbst wenn die Geräte als "Ausstehend" (MIA, Missing in Action) eingestuft sind oder nicht mehr verwendet werden. Geräte, die dem Inventar manuell oder über die API hinzugefügt wurden, werden bei den Lizenzlimits dagegen nicht berücksichtigt. Weitere Informationen hierzu finden Sie unter http://quest.com/docs/Product_Guide.pdf.
>
> **HINWEIS:** Rufen Sie zum Erhöhen der Lizenzkapazität die Quest Website auf: https://quest.com/buy.

- **Gültig bis**: Das Ablaufdatum der Lizenz im Format `Jahr/Monat/Tag`.

> **HINWEIS:** Wenn die Appliance-Wartung abläuft, stehen einige Funktionen, wie z. B. Patching-Support, nicht mehr zur Verfügung. Dadurch wird eine Fehlerwarnung auf dem Home-Dashboard angezeigt. Um Ihre Lizenz zu erneuern, gehen Sie zu https://support.quest.com/contact-us/renewals. Weitere Informationen zum Dashboard finden Sie unter Verwenden der Komponente "Startseite".

- **Komponenten**: Die Komponenten, die unter Ihrer Lizenz aktiviert sind.

Optional: Anzeigen der Seriennummer, Modellnummer, Lizenzbedingungen sowie von Drittanbietercode. Siehe Version, Modell und Lizenzinformationen der Appliance anzeigen.

Informationen zum Aktualisieren der Appliance-Software

Die Appliance überprüft täglich die Server von Quest auf Softwareaktualisierungen. Diese Aktualisierungen werden als beworbene Aktualisierungen bezeichnet.

Wenn Updates verfügbar sind, wird eine Benachrichtigung auf der *Startseite* der **Administratorkonsole** angezeigt, sobald Sie sich das nächste Mal mit einem Konto mit Administratorrechten anmelden.

Verwandte Themen

Aktualisierungsdatei manuell in die Appliance hochladen.

Informationen zu den Labels

Labels sind Container zum Organisieren und Kategorisieren von Elementen wie etwa Geräten, sodass diese als Gruppe verwaltet werden können.

Beispielsweise können Sie Labels verwenden, um Geräte mit dem gleichen Betriebssystem oder am gleichen geografischen Standort zu kennzeichnen. Sie können dann Aktionen wie das Verteilen von Software oder das Bereitstellen von Patches auf allen Geräten mit diesem Label initiieren. Labels können entweder spezifischen Elementen manuell zugewiesen werden oder sie können Elementen durch Zuweisung zu Kriterien wie SQL- oder LDAP-Abfragen automatisch zugewiesen werden.

Sie können Labels aus dem Bereich *Labels* hinzufügen, aber auch aus anderen Bereichen der **Administratorkonsole**, in denen Labels verwendet werden, z. B. von der Seite *Geräte*.

Folgende Labels sind verfügbar:

- **Labels**: Labels, die manuell angewendet und u.a. zum Organisieren von Benutzern, Geräten, Software und verwalteten Installationen verwendet werden. Siehe Verwalten manueller Labels.
- **Smart Labels**: Labels werden auf der Grundlage der von Ihnen festgelegten Kriterien automatisch zugewiesen und entfernt. Wenn Sie zum Beispiel Notebooks in einer bestimmten Niederlassung nachverfolgen möchten, können Sie ein Label mit der Bezeichnung "Niederlassung in San Francisco" und dann ein Smart Label auf Basis des IP-Adressbereichs oder des Subnetzes für Geräte verwenden, die sich in der Niederlassung in San Francisco befinden. Bei jeder Inventarisierung eines Geräts aus dem IP-Adressbereich wird automatisch das Smart Label "San Francisco" zugewiesen. Wenn das Gerät den IP-

Adressbereich verlässt und danach erneut inventarisiert wird, wird das Label automatisch entfernt. Siehe Verwalten von Smart Labels.

- **LDAP-Labels**: Labels, die auf Basis von LDAP- oder Active Directory®-Abfragen automatisch auf Geräte oder Benutzer angewendet werden können. Siehe Verwalten von LDAP-Labels.

Verwandte Themen

Verwalten von Smart Labels

Verwalten von LDAP-Labels

Suchen nach Informationen und Filtern von Listen

Sie können die Appliance-Datenbanken durchsuchen und Listenseiten filtern, um Informationen zur Appliance zu erhalten.

Wenn die Organisationskomponente auf der Appliance aktiviert ist, können Sie die Datenbank für jede Organisation separat durchsuchen. Sie können nicht die Datenbanken aller Organisationen gleichzeitig durchsuchen. Außerdem ist eine Suche auf Systemebene nicht möglich.

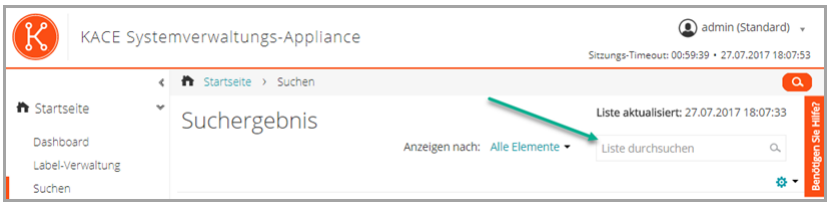
Auf Administratorebene suchen

Sie können in den Datenbanken auf Verwaltungsebene nach Informationen zur Appliance suchen.

Wenn die Organisationskomponente auf der Appliance aktiviert ist, können Sie die Datenbank für jede Organisation separat durchsuchen. Sie können nicht die Datenbanken aller Organisationen gleichzeitig durchsuchen. Außerdem ist eine Suche auf Systemebene nicht möglich.

1. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
2. Führen Sie einen der folgenden Schritte aus:
   - **Klicken Sie oben rechts auf der Seite auf die Schaltfläche *Suchen*, um das Feld *Suchen* anzuzeigen. Geben Sie anschließend mindestens vier Zeichen in das Feld *Globale Suche* ein und drücken Sie Eingabe oder die Eingabetaste. In der folgenden Abbildung sehen Sie das Feld *Suche*:**

   - **Klicken Sie auf Startseite > Suchen. Geben Sie anschließend mindestens vier Zeichen in das Feld *Suchen* über der Liste rechts ein und drücken Sie die Eingabetaste. In der folgenden Abbildung sehen Sie das Feld *Suche*:**



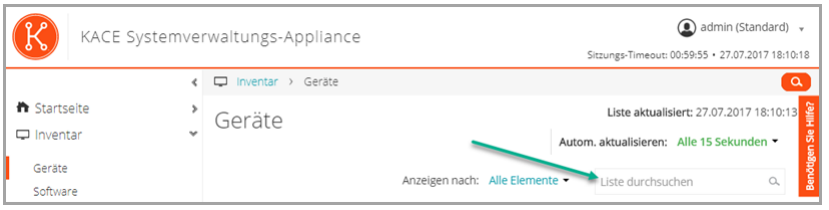
TIPP: Verwenden Sie das Prozentzeichen (%) als Platzhalter. Sie können das Prozentzeichen beispielsweise in einer Suchzeichenfolge verwenden, um alle Elemente zu finden, die den Kriterien vor und nach dem Prozentzeichen entsprechen.

Auf Seitenebene suchen

Mit der Suche auf Seitenebene können Sie auf der aktuellen Seite nach Informationen suchen.

1. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
2. Rufen Sie eine Listenseite auf. Klicken Sie beispielsweise in der linken Navigationsleiste auf **Inventar**. Die Seite *Geräte* wird angezeigt.
3. Geben Sie auf der Listenseite (in diesem Beispiel: *Geräte*) oben rechts auf der Seite in das Feld **Suchen** den Suchtext ein. Drücken Sie die **Eingabetaste**, um die Suche auf Seitenebene zu starten.

   In der folgenden Abbildung sehen Sie das Feld zur *Suche auf Seitenebene*:



> **TIPP:** Verwenden Sie das Prozentzeichen (%) als Platzhalter. Sie können das Prozentzeichen beispielsweise in einer Suchzeichenfolge verwenden, um alle Elemente zu finden, die den Kriterien vor und nach dem Prozentzeichen entsprechen.

Auf Seitenebene mit erweiterten Optionen suchen

Mit der erweiterten Suche auf Seitenebene können Sie auf der jeweils aktuellen Seite mithilfe verschiedener Kombinationen von Kriterien nach Informationen suchen. Die erweiterte Suche auf Seitenebene ist auf den meisten Listenseiten verfügbar, z. B. auf den Seiten *Geräte* und *Software*.

Beispiel: Nach verwalteten Geräten mithilfe der Kriterien der Erweiterten Suche suchen

Dieses Beispiel zeigt, wie Sie mithilfe der erweiterten Suche auf Seitenebene alle Windows Geräte finden können, auf denen nur noch wenig Festplattenkapazität frei ist.

Wenn ein Nutzer mit eingeschränkten Zugriffsrechten eine erweiterte Suche nach Geräten durchführt und seine Benutzerrolle mit einem Smart Label verknüpft ist, enthalten die Ergebnisse nur die Geräte, die mit diesem Smart Label verknüpft sind. Damit weitere Geräte angezeigt werden, können Sie den Umfang des Smart Label nach Bedarf ändern. Weitere Informationen zum Konfigurieren eines Gerätebereichs für eine Benutzerrolle finden Sie unter Benutzerrollen hinzufügen oder bearbeiten. Informationen zu Smart Labels finden Sie unter Verwalten von Smart Labels.

1. Rufen Sie die Liste *Geräte* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Inventar** und anschließend auf **Dashboard**.
2. Klicken Sie rechts oberhalb der Liste **Geräte** auf die Registerkarte *Erweiterte Suche*.

   Der Bereich *Erweiterte Suche* wird angezeigt.

3. Geben Sie die Kriterien an, die erforderlich sind, um Windows Geräte zu finden:

   `Betriebssystem: Name des Betriebssystems | enthält | Windows`

4. Wählen Sie in der Dropdown-Liste "Operator" die Option **UND** aus, klicken Sie zum Hinzufügen einer neuen Zeile auf **Zeile hinzufügen** und geben Sie anschließend die erforderlichen Kriterien für die Suche nach Geräten an, deren Speicherplatz begrenzt ist:

   `Laufwerksinformationen: Datenträger % Kapazität | > | 95`

5. Klicken Sie auf **Suchen**.

Die Liste wird aktualisiert, damit nur die Geräte angezeigt werden, die den festgelegten Kriterien entsprechen.

Smart Labels und Benachrichtigungen mithilfe der Kriterien der Erweiterten Suche hinzufügen

Sie können Smart Labels und Benachrichtigungen mit den im Bereich *Erweiterte Suche* ausgewählten Kriterien hinzufügen.

Wenn ein Nutzer mit eingeschränkten Zugriffsrechten eine erweiterte Suche nach Geräten durchführt und seine Benutzerrolle mit einem Smart Label verknüpft ist, enthalten die Ergebnisse nur die Geräte, die mit diesem Smart Label verknüpft sind. Damit weitere Geräte angezeigt werden, können Sie den Umfang des Smart Label nach Bedarf ändern. Weitere Informationen zum Konfigurieren eines Gerätebereichs für eine Benutzerrolle finden Sie unter Benutzerrollen hinzufügen oder bearbeiten. Informationen zu Smart Labels finden Sie unter Verwalten von Smart Labels.

1. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
2. Rufen Sie eine Listenseite auf. Klicken Sie beispielsweise auf der linken Navigationsleiste auf **Inventar**, um die Seite *Geräte* anzuzeigen.
3. Klicken Sie oberhalb der Liste auf der rechten Seite auf die Registerkarte *Erweiterte Suche* und geben Sie die Suchkriterien ein.

   Siehe Beispiel: Nach verwalteten Geräten mithilfe der Kriterien der Erweiterten Suche suchen.

4. Klicken Sie rechts oberhalb der Liste auf die Registerkarte **Smart Label**.

   Der Bereich *Smart Label* wird angezeigt. Die ausgewählten Suchkriterien bleiben verfügbar.

5. Führen Sie im Menü *Label auswählen* einen der folgenden Schritte aus:

   - **Wählen Sie ein vorhandenes Label aus, um es mit diesem Smart Label zu verknüpfen. Geben Sie in das Feld *Label auswählen* einen Begriff ein, um nach vorhandenen Labels zu suchen.**

HINWEIS: Wenn Sie statt eines Labels eine Labelgruppe auswählen, können Sie das Smart Label nicht auf einen Patching-Zeitplan anwenden. Patch-Zeitpläne können nur Smart Labels verwenden, die auf einem einzelnen Element basieren.

- **Geben Sie einen neuen Namen für das Smart Label im Feld** *Label auswählen* **ein und drücken Sie Enter bzw. die Eingabetaste.**

HINWEIS: Drücken Sie **Enter** bzw. die **Eingabetaste**, nachdem Sie einen neuen Smart Label-Namen eingegeben haben, um den Text aus dem Suchfeld in das Label-Feld zu verschieben.

6. Klicken Sie auf **Erstellen**.

   So werden Smart Labels angewendet

   - Smart Labels werden Geräten automatisch zugewiesen oder von diesen entfernt, sobald sich die Geräte bei der Appliance anmelden und sofern sie bestimmten Kriterien entsprechen.
   - Wenn ein bestimmtes Anwendungs-Smart Label über **Startseite** > **Labels** > **Smart Labels** bearbeitet wird, wird es sofort auf sämtliche Anwendungen angewendet bzw. von diesen entfernt.
   - Smart Labels werden automatisch Anwendungen zugewiesen oder von diesen entfernt, wenn die Elemente auf der Seite *Inventar* > *Software* aktualisiert werden und den angegebenen Kriterien entsprechen.

7. Klicken Sie rechts oberhalb der Liste auf die Registerkarte **Benachrichtigung**.

   Der Bereich *Benachrichtigung* wird angezeigt. Die ausgewählten Suchkriterien bleiben verfügbar.

8. Geben Sie die folgenden Informationen an:

Feld	Beschreibung
Titel	Die Informationen, die in der *Betreff*-Zeile der E-Mail-Benachrichtigung stehen sollen.
Empfänger	Die E-Mail-Adresse oder -Adressen der gewünschten Empfänger. Es müssen vollständige, gültige E-Mail-Adressen verwendet werden. Um E-Mails an mehrere Adressen zu senden, trennen Sie die Adressen durch Kommas oder verwenden E-Mail-Verteiler.
Häufigkeit	Das Intervall, in dem die Appliance die Abfrage ausführt, um die gewählten Kriterien mit Elementen im Inventar zu vergleichen. Werden Kriterien erfüllt, wird eine Benachrichtigung gesendet.

9. **Optional**: Klicken Sie auf **Benachrichtigung testen**, um die Kriterien zu überprüfen.

   Die Liste wird aktualisiert, damit nur die Elemente angezeigt werden, die den festgelegten Kriterien entsprechen. Während des Tests werden keine E-Mail-Nachrichten versendet.

10. Klicken Sie auf **Benachrichtigung erstellen**.

Die Benachrichtigung wird hinzugefügt und auf der Seite *E-Mail-Alarmfunktionen* angezeigt.

Weitere Informationen zum Planen der Benachrichtigungshäufigkeit finden Sie unter Benachrichtigungszeitpläne bearbeiten.

Verwandte Themen

Beispiel: Nach verwalteten Geräten mithilfe der Kriterien der Erweiterten Suche suchen

Smart Labels von der Registerkarte "Erweiterte Suche" laden

Sie können Smart Labels von Listenseiten laden, auf denen die Registerkarte *Erweiterte Suche* verfügbar ist.

Wenn ein Nutzer mit eingeschränkten Zugriffsrechten eine erweiterte Suche nach Geräten durchführt und seine Benutzerrolle mit einem Smart Label verknüpft ist, enthalten die Ergebnisse nur die Geräte, die mit diesem Smart Label verknüpft sind. Damit weitere Geräte angezeigt werden, können Sie den Umfang des Smart Label nach Bedarf ändern. Weitere Informationen zum Konfigurieren eines Gerätebereichs für eine Benutzerrolle finden Sie unter Benutzerrollen hinzufügen oder bearbeiten. Informationen zu Smart Labels finden Sie unter Verwalten von Smart Labels.

1. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
2. Rufen Sie eine Listenseite auf. Klicken Sie beispielsweise auf **Inventar** zum Anzeigen der Liste *Geräte*.
3. Klicken Sie oberhalb der Liste auf der rechten Seite auf die Registerkarte **Erweiterte Suche**, um den Bereich *Erweiterte Suche* anzuzeigen.
4. Wählen Sie oben im Bereich *Erweiterte Suche* in der Dropdown-Liste *Smart Label* das Smart Label aus, das Sie laden wollen.

   Die Dropdown-Liste zeigt Smart Labels, die der Listenseite entsprechen, die Sie momentan anzeigen. Beispielsweise werden die Geräte-Smart Labels in der Dropdown-Liste auf der Seite *Geräte* angezeigt. Außerdem werden Labels nur dann angezeigt, wenn der zugrunde liegende SQL-Code nicht außerhalb des Smart Label Assistenten bearbeitet wurde. Der Grund dafür ist, dass der Assistent keinen benutzerdefinierten SQL-Code anzeigen kann.
5. Klicken Sie auf **Laden**.

Die Kriterien des gewählten Smart Labels werden im Bereich *Erweiterte Suche* angezeigt.

Benutzerdefinierter Ansichten mithilfe von Kriterien für die Erweiterte Suche erstellen

Sie können benutzerdefinierte Ansichten mithilfe von Kriterien für die erweiterte Suche erstellen. In einer benutzerdefinierten Ansicht werden Listenelemente anhand von vordefinierten Kriterien für die Erweiterte Suche angezeigt. Benutzerdefinierte Ansichten sind auf Listenseiten wie *Softwarekatalog*, *Assets* und der Service Desk-Seite *Tickets* verfügbar.

Benutzerdefinierte Ansichten sind benutzerspezifisch. Die Benutzer können nicht auf individuelle Ansichten zugreifen, die andere Benutzer erstellt haben.

1. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in*

Verwaltungskopfzeile anzeigen aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.

2. Rufen Sie eine Seite mit der Option Benutzerdefinierte Ansicht auf, z. B. die Seite *Softwarekatalog* oder die Seite *Assets*.
3. Klicken Sie oben rechts auf der Seite auf die Registerkarte **Erweiterte Suche** und geben Sie die Suchkriterien ein.
4. Klicken Sie oben rechts auf der Seite auf die Registerkarte **Benutzerdefinierte Ansicht**, um den Bereich *Benutzerdefinierte Ansicht* anzuzeigen.
5. Wählen Sie die Kriterien für die benutzerdefinierte Ansicht. Um z. B. eine Ansicht auf der Seite *Softwarekatalog* zu erstellen, bei der alle Windows Geräte mit erfassten Anwendungen in der Kategorie "Infrastrukturanwendungen" angezeigt werden, gehen Sie wie folgt vor:
   a. Geben Sie die erforderlichen Kriterien ein, um Anwendungen zu finden, die als Infrastrukturanwendungen kategorisiert sind:

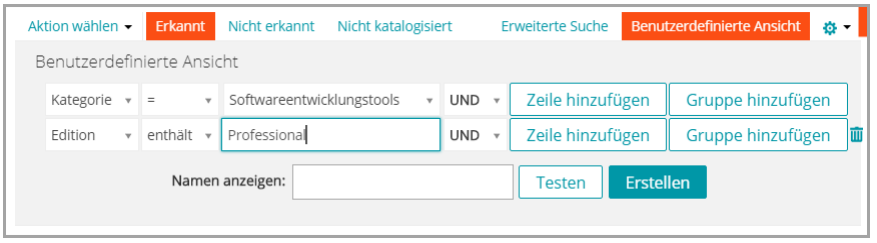
   ```
   Kategorie | = | Infrastrukturanwendungen
   ```

   b. Wählen Sie in der Dropdown-Liste "Operator" **AND** aus und klicken Sie zum Hinzufügen einer neuen Zeile auf **Zeile hinzufügen**.
   c. Geben Sie die erforderlichen Kriterien ein, um Anwendungen anzuzeigen, deren Nutzung erfasst wird:

   ```
   Erfasst | ist | Wahr
   ```

   d. Wählen Sie in der Dropdown-Liste "Operator" **AND** aus und klicken Sie zum Hinzufügen einer neuen Zeile auf **Zeile hinzufügen**.
   e. Geben Sie die Kriterien an, die erforderlich sind, um Windows Geräte zu finden:

   ```
   Plattform | = | Windows
   ```



6. **Optional**: Klicken Sie auf **Testen**, um die Liste zu aktualisieren und Elemente anzuzeigen, die den angegebenen Kriterien entsprechen.
7. Geben Sie im Feld *Ansichtsname* einen Namen für die benutzerdefinierte Ansicht ein und klicken Sie auf **Erstellen**.

Die benutzerdefinierte Ansicht erscheint in der Dropdown-Liste *Anzeigen nach*.

Verwandte Themen

Beispiel: Nach verwalteten Geräten mithilfe der Kriterien der Erweiterten Suche suchen

Zugreifen auf die Produktdokumentation

Die **Administratorkonsole** bietet Zugriff auf den Inhalt der Hilfe und Suchvorgänge in der Dokumentation. Außerdem können Sie nach relevanten Knowledge Base-Artikeln suchen und bei Bedarf mit Produktspezialisten chatten.

1. Melden Sie sich an der Benutzerkonsole, Administratorkonsole oder der Systemkonsole an.
2. Klicken Sie in der oberen rechten Ecke der Administratorkonsole auf **Benötigen Sie Hilfe?**.

Auf der rechten Seite wird ein Hilfefenster mit allgemeinen Informationen über die zugehörige **Administratorkonsole**-Seite angezeigt. Am unteren Rand des Hilfebereichs befinden sich die folgenden Schaltflächen:

- **Appliance Administratorhandbuch**(): Bietet Zugriff auf den Hilfeinhalt der KACE Systemverwaltungs-Appliance.
- **Knowledge-Base** (): Ermöglicht Ihnen, nach Knowledge Base-Artikeln zu suchen, die sich auf die zugehörige **Administratorkonsole**-Seite beziehen.

  HINWEIS: Diese Option ist nur in der **Administratorkonsole** und der Systemkonsole verfügbar. Sie erscheint nicht in der **Benutzerkonsole**.

- **Video Knowledge Base** (): Ermöglicht Ihnen, nach weiteren Schulungsvideos zu suchen, die sich auf die zugehörige **Administratorkonsole**-Seite beziehen. Sie können ein Video im Hilfebereich, in einem kleineren Fenster außerhalb der Seite oder auf der Knowledge Base-Seite des Ziels wiedergeben, auf der das Video gehostet wird.

  HINWEIS: Diese Option ist nur verfügbar, wenn zugehörige Videos im Support-Portal verfügbar sind. Sie wird zudem nur in der **Administratorkonsole** und der Systemkonsole angezeigt. Sie erscheint nicht in der **Benutzerkonsole**.

- **Live-Chat** (): Startet einen Chat mit einem Produktspezialisten für die KACE Systemverwaltungs-Appliance.

  HINWEIS: Diese Option ist nur in der **Administratorkonsole** und der Systemkonsole verfügbar. Sie erscheint nicht in der **Benutzerkonsole**.

- **Ticket öffnen** (): Stellt Links zur Support-Seite (https://support.quest.com/create-service-request) her, auf der Sie eine Serviceanfrage erstellen können.

  HINWEIS: Diese Option ist nur in der **Administratorkonsole** und der Systemkonsole verfügbar. Sie erscheint nicht in der **Benutzerkonsole**.

- **Support** (): Stellt Links zur Seite **Einstellungen > Support** her. Auf dieser Seite sehen Sie Ressourcen zur Fehlerbehebung bei Systemverwaltungsproblemen und zur Kontaktaufnahme mit dem **Quest Support**.

  HINWEIS: Diese Option ist nur in der **Administratorkonsole** und der Systemkonsole verfügbar. Sie erscheint nicht in der **Benutzerkonsole**.

- **KACE GO Mobile App** (): Zeigt ein Dialogfeld mit Links zum Herunterladen der KACE GO Mobile App an. Die App ist für iOS- und Android-Plattformen verfügbar.

  HINWEIS: Diese Option ist verfügbar, wenn die Appliance für die Interaktion mit der K1 GO Mobile App konfiguriert wurde. Sie erscheint nur in der **Administratorkonsole** und der Systemkonsole. Sie erscheint nicht in der **Benutzerkonsole**. Weitere Informationen zum Aktivieren des mobilen Zugriffs finden Sie unter Konfigurieren des Mobilgerätezugriffs.

- **Info** (): Zeigt Informationen zu Ihrer Installation der KACE Systemverwaltungs-Appliance an.

  HINWEIS: Diese Option ist nur in der **Administratorkonsole** und der Systemkonsole verfügbar. Sie erscheint nicht in der **Benutzerkonsole**.

3. Klicken Sie in dem Hilfethema zu der Seite auf einen Link.

   Das ausgewählte Thema wird im Haupt-Hilfesystem angezeigt.

4. Klicken Sie im linken Bereich des Hilfesystems auf die Registerkarte **Suchen**.

   Alle Suchbegriffe werden implizit mit einem Booleschen UND-Operator verknüpft. Wenn Sie z. B. nach **Windows Provisionierung** suchen, werden in der Suche Ergebnisse angezeigt, die beide Wörter enthalten.

TIPP: Zum Anzeigen der Online-Hilfe als PDF-Datei klicken Sie auf der rechten Seite im Haupt-Hilfesystem in der Navigationsleiste ( ) auf die Schaltfläche „Acrobat“.

5. **Nur Administrator- oder Systemkonsole**. Suchen Sie nach Knowledge Base-Artikeln, die sich auf die zugehörigeAdministratorkonsole oder die Seite der Systemkonsole beziehen.
   a. Klicken Sie im unteren Bereich des Navigationsfensters auf .

      Auf der Hilfeseite wird eine Liste relevanter Knowledge Base-Artikel angezeigt.

      HINWEIS: Knowledge Base-Artikel sind gegenwärtig nur auf Englisch verfügbar.

   b. Verwenden Sie die Navigationsschaltflächen, um nach einem bestimmten Artikel zu suchen.
   c. Durchsuchen Sie die aufgelisteten Artikel gegebenenfalls nach einem bestimmten Stichwort.
   d. Wenn Sie den gewünschten Artikel finden, klicken Sie auf den Link im Hilfefenster.

      Der ausgewählte Knowledge Base-Artikel wird unter einer neuen Registerkarte in Ihrem Browser angezeigt.

      WICHTIG: Zum Anzeigen des Artikelinhalts müssen Sie sich mit Ihrem Quest Benutzernamen und Kennwort bei der Quest Support-Website anmelden

6. **Nur Administrator- oder Systemkonsole**. Suchen Sie nach Knowledge Base-Artikeln, die sich auf die zugehörigeAdministratorkonsole oder die Seite der Systemkonsole beziehen.
   a. Klicken Sie im unteren Bereich des Navigationsfensters auf .

      Im Hilfebereich wird eine Liste relevanter Schulungsvideos angezeigt.

      HINWEIS: Um auf die Videos zuzugreifen, müssen Sie sich mit Ihrem Quest Benutzernamen und Kennwort bei der Quest Support-Website anmelden. Schulungsvideos sind gegenwärtig nur auf Englisch verfügbar.

   b. Verwenden Sie die Navigationsschaltflächen, um nach einem bestimmten Video zu suchen.
   c. Klicken Sie zum Abspielen eines Videos auf die Wiedergabe-Schaltfläche.

      Das ausgewählte Video wird im Hilfebereich wiedergegeben.

   d. Fahren Sie mit der Wiedergabe eines Videos im Hilfebereich fort, oder verwenden Sie eine andere Anzeigeoption, z. B. *Bild-in-Bild*, *Vollbild* oder *Popout-Player*, um das Video außerhalb der ausgewählten Seite anzuzeigen. Diese Steuerelemente befinden sich am unteren Rand des Videos.

7. **Nur Administrator- oder Systemkonsole**. Chatten Sie mit einem Produktspezialisten.
   a. Klicken Sie auf .

      Das Dialogfeld *Chat mit Support* wird angezeigt.

   b. Geben Sie Ihren *vollständigen Namen*, Ihre *E-Mail-Adresse* und den *Zweck Ihres Chats* ein und klicken Sie auf **Chat starten**.

      Das Dialogfeld *Chat mit Support* wird aktualisiert und zeigt eine Liste der vorhandenen Knowledge Base-Artikel (KB) an, die Informationen zum angegebenen Thema enthalten können. Die Liste der Themen kann je nach Art der angeforderten Informationen auf mehreren Seiten angezeigt werden.

   c. Prüfen Sie die Liste der KB-Artikel. Verwenden Sie ggf. die Seitennavigationssteuerelemente unten in der Liste. Um einen KB-Artikel zu lesen, klicken Sie auf den Titel in der Liste.
   d. Wenn keiner der aufgeführten KB-Artikel die erforderlichen Informationen enthält, klicken Sie auf **Keine der oben genannten Lösungen hat mein Problem gelöst. Fahren Sie mit dem Chat fort.**

      HINWEIS: Sie können diese Funktion nur verwenden, wenn Produktspezialisten zur Verfügung stehen, die Ihre Fragen beantworten können. Wenn Live-Chat nicht verfügbar ist, wird dies im Dialogfeld angegeben.

Das Dialogfeld *LIVE-CHAT* wird angezeigt. Die Felder *Vollständiger Name*, *E-Mail-Adresse*, *Produkt* und *Zweck Ihres Chats* werden mit den Informationen ausgefüllt, die im Dialogfeld *Chat mit Support* angegeben sind.

e. Klicken Sie auf **Chat starten**.

Das Dialogfeld *LIVE-CHAT* wird aktualisiert.

f. Geben Sie im Dialogfeld *LIVE CHAT* Ihre Frage ein und klicken Sie auf **SENDEN**, um mit einem Produktspezialisten zu chatten.

8. **Nur Administrator- oder Systemkonsole**. Öffnen Sie ein Support-Ticket.

a. Klicken Sie auf .

In einer neuen Registerkarte oder einem neuen Fenster in Ihrem Browser wird die Seite *Serviceanfrage einreichen* (https://support.quest.com/create-service-request) angezeigt.

b. Auf dieser Seite können Sie bei Bedarf ein Service-Ticket öffnen.

9. **Nur Administrator- oder Systemkonsole**. Klicken Sie auf .

Die Seite **Einstellungen > Support** wird angezeigt. Auf dieser Seite sehen Sie Ressourcen zur Fehlerbehebung bei Systemverwaltungsproblemen und zur Kontaktaufnahme mit dem **Quest Support**.

10. **Nur Administrator- oder Systemkonsole, wenn mobiler Zugriff auf der Appliance aktiviert ist.**

HINWEIS: Weitere Informationen zum Aktivieren des mobilen Zugriffs finden Sie unter Konfigurieren des Mobilgerätezugriffs.

a. Klicken Sie auf .

Ein Dialogfeld wird angezeigt, über das Sie KACE GO herunterladen können. Die App ist für iOS- und Android-Plattformen von den jeweiligen App Stores erhältlich.

b. Klicken Sie gegebenenfalls auf den Link für das Betriebssystem Ihres Mobilgeräts, um die App herunterzuladen.

Weitere Informationen zum Herunterladen und Konfigurieren von KACE GO finden Sie unter KACE GO herunterladen und verwenden.

11. **Nur Administrator- oder Systemkonsole**. Überprüfen Sie die Informationen zu Ihrer Installation der KACE Systemverwaltungs-Appliance.

a. Klicken Sie auf .

Ein Dialogfeld mit den Produktinformationen wird angezeigt.

b. Um dieses zu schließen, klicken Sie auf **Schließen**.

12. Zum Schließen des Hilfebereichs klicken Sie auf **Benötigen Sie Hilfe?**.

Melden Sie sich bei der Administratorkonsole an: Erste Anmeldung nach der Erstkonfiguration des Netzwerks

Nachdem Sie die Netzwerkeinstellungen konfiguriert und die Appliance neu gestartet haben, können Sie sich über jeden Computer im LAN (Local Area Network) bei der **Administratorkonsole** der Appliance anmelden.

Bei der ersten Anmeldung nach der Erstkonfiguration des Netzwerks müssen Sie Ihren Appliance-Lizenzschlüssel eingeben und das Kennwort für das Konto vom Typ **admin** festlegen.

HINWEIS: Die Sprache, in der Ihnen die **Administratorkonsole** bei Ihrer ersten Anmeldung angezeigt wird, hängt von Ihren Browsereinstellungen ab. Informationen zum Ändern dieser Einstellung nach dem Anmeldevorgang finden Sie unter Konfigurieren der Gebietsschema-Einstellungen.

1. Öffnen Sie einen Webbrowser und geben Sie die URL der Administratorkonsole an:

   `http://`**appliance_hostname**`/admin`. Zum Beispiel `http://kace_sma/admin`.

2. Geben Sie die folgenden Informationen an:

Option	Beschreibung
Lizenzschlüssel	Geben Sie den Lizenzschlüssel ein, den Sie in der **Begrüßungs**mail von Quest erhalten haben (mit Bindestrichen). Wenn Sie keinen Lizenzschlüssel besitzen, wenden Sie sich an den **Quest Support** unter https://support.quest.com/contact-support.
Kennwort	Geben Sie ein Kennwort für das Standardkonto **admin** ein. Mit diesem Konto melden Sie sich bei der **Administratorkonsole** der Appliance an. Das Standardkonto **admin** ist zu diesem Zeitpunkt das einzige Konto der Appliance. Wenn Sie das Kennwort für dieses Konto vergessen, muss das System möglicherweise auf die Werkseinstellungen zurückgesetzt werden, was einen Datenverlust zur Folge haben kann. **HINWEIS:** Wenn Sie über mehrere KACE Appliances verfügen, empfiehlt Quest, für alle Appliances dasselbe Kennwort für das **Administratorkonto** zu verwenden. Mit einem allgemeinen Kennwort können Sie die Appliances später verknüpfen.
Name der Firma	Geben Sie den Namen Ihrer Firma oder Gruppe ein.
Zeitzone	Wählen Sie die Zeitzone für den Appliance-Standort aus.

3. Klicken Sie auf **Einstellungen übernehmen und neu starten**.

   Die Appliance wird neu gestartet.

4. Aktualisieren Sie nach dem Neustart der Appliance die Browserseite.
5. Akzeptieren Sie die Endbenutzer-Lizenzvereinbarung und melden Sie sich dann mit der Anmelde-ID `admin` und dem Kennwort an, das Sie auf der Seite für die Ersteinrichtung ausgewählt haben.
6. Aktivieren bzw. deaktivieren Sie die Kontrollkästchen neben den Benachrichtigungsfeldern, um E-Mail-Benachrichtigungen für das Administratorkonto ein- bzw. auszuschalten. Sie können diese Einstellungen später nach Bedarf ändern. Siehe E-Mail-Benachrichtigungen des Appliance-Administrators verwalten.

Option	Beschreibung
Quest Sicherheitsbenachrichtigungen aktivieren	Aktivieren Sie Quest, um Sicherheitsbenachrichtigungen an die E-Mail-Adresse des Administrators zu senden. Diese Funktion ist nur für Administratorkonten auf Systemebene verfügbar. Sie steht nicht für Administratorkonten auf Verwaltungsebene oder Benutzerkonten ohne Administratorberechtigungen zur Verfügung.

Option	Beschreibung
Quest Vertriebs- und Marketingbenachrichtigungen aktivieren	Aktivieren Sie Quest, um Vertriebs- und Marketingbenachrichtigungen an die E-Mail-Adresse des Administrators zu senden. Diese Funktion ist nur für Administratorkonten auf Systemebene, aber nicht für Administratorkonten auf Verwaltungsebene oder Benutzerkonten ohne Administratorberechtigungen verfügbar.

Die **Administratorkonsole** wird angezeigt und die Appliance kann verwendet werden.

Erste Schritte

Zur Verwendung der Appliance müssen Sie die Appliance-Einstellungen Ihrer Netzwerkkonfiguration entsprechend konfigurieren.

Darüber hinaus können Sie Labels, die Benutzerauthentifizierung, Replikationsfreigaben, die Verwaltung der Anmeldeinformationen, Assets, die Lizenz-Compliance und die Service Desk-Funktionen gemäß den Anforderungen Ihrer Umgebung einrichten. Wenn die Organisationskomponente auf Ihrer Appliance aktiviert ist, können Sie Organisationen und Organisationseinstellungen nach Bedarf hinzufügen und bearbeiten.

Konfigurieren der Appliance

Im Rahmen der Appliance-Konfiguration werden Netzwerk-, Sicherheits- und Gebietsschema-Einstellungen sowie weitere Einstellungen eingerichtet.

Anforderungen und Spezifikationen

In den technischen Daten der Appliance sind die Kapazität und Anforderungen der Appliance für die Geräteverwaltung beschrieben.

Aktuelle Informationen zur Appliance Hardware, zu den Anforderungen für verwaltete Geräte und zu den Browseranforderungen für den Zugriff auf die **Administratorkonsole** finden Sie in den *technischen Daten* auf der Produktdokumentationsseite: https://support.quest.com/kace-systems-management-appliance/technical-documents.

Einschalten der Appliance und Anmelden bei der Administratorkonsole

Beim ersten Einschalten der Appliance können Sie sich über einen beliebigen Computer in Ihrem LAN bei der **Administratorkonsole** der Appliance anmelden, vorausgesetzt ein DHCP-Server ist verfügbar, um der Appliance eine IP-Adresse zuzuweisen. So können Sie den Setup-Assistenten zum Konfigurieren der anfänglichen Netzwerkeinstellungen verwenden.

- Laden Sie bei Verwendung der virtuellen Appliance die Appliance-Software herunter und richten Sie die Virtualisierungsinfrastruktur ein. Weitere Informationen finden Sie im Einrichtungshandbuch zur virtuellen Appliance Weitere Informationen finden Sie unter https://support.quest.com/kace-systems-management-appliance/release-notes-guides.
- Lesen Sie vor dem Einrichten der Appliance die Sicherheitshinweise im Dokument **Dell PowerEdge R430 – Erste Schritte mit dem System** sowie alle im Lieferumfang der Appliance enthaltenen Sicherheitshinweise. Die Quest Appliance ist eine Plattform mit spezieller Konfiguration. Sie müssen keine internen Komponenten installieren oder entfernen, die Firmware nicht aktualisieren und keine BIOS-Einstellungen ändern. Halten Sie sich beim Einrichten ausschließlich an die Anweisungen in diesem Dokument.
- Geben Sie im A-Datensatz Ihres internen DNS-Servers (Domain Name System) den Hostnamen der Appliance ein. Der A-Datensatz definiert den Hostnamen für den MX-Datensatz. Dadurch können Benutzer

E-Mail-Tickets an den Service Desk senden. Der voreingestellte Hostname der Anwendung ist `k1000`. Sie können ihn jedoch während der Ersteinrichtung ändern.

- Entscheiden Sie, ob Sie ein Split-DNS verwenden möchten. Die Verwendung eines Split-DNS kann nützlich sein, wenn die Verbindung der Appliance mit dem Internet über einen Reverseproxy, durch Hinzufügen zu einem Umkreisnetzwerk oder zu einem überwachten Subnetz hergestellt wird. Durch eine DMZ wird ein LAN (lokales Netzwerk) um eine zusätzliche Sicherheitsebene erweitert.
- (Optional) Rufen Sie eine statische IP-Adresse für die Appliance ab.

Wenn kein DHCP-Server verfügbar ist, können Sie die Netzwerkeinstellungen mithilfe der **Befehlszeilenkonsole** konfigurieren. Siehe Zugriff auf die Befehlszeilenkonsole.

HINWEIS: Weitere Informationen über die Anmeldung beim KACE als Service finden Sie im **KACE als Service Einrichtungshandbuch**. Weitere Informationen finden Sie unter https://support.quest.com/kace-systems-management-appliance/release-notes-guides.

1. Konfigurieren der physischen Appliance:
   a. Installieren Sie die Appliance im Rack und schließen Sie einen Monitor direkt an der Appliance an.
   b. Schließen Sie ein Netzwerkkabel an den entsprechenden Port an:

   c. Schalten Sie die Appliance ein.

      Der **Befehlszeilenkonsole**-Anmeldebildschirm wird auf dem an die Appliance angeschlossenen Monitor angezeigt. Der Anmeldebildschirm zeigt die DHCP-Netzwerkeinstellungen der Appliance.
2. Schalten Sie beim Konfigurieren der virtuellen Appliance den virtuellen Computer ein, um die Appliance zu starten.

   Das erste Einrichten dauert 5 bis 10 Minuten.

   Der **Befehlszeilenkonsole**-Anmeldebildschirm zeigt die DHCP-Netzwerkeinstellungen der Appliance.
3. Öffnen Sie auf einem beliebigen mit Ihrem LAN verbundenen Computer einen Browser und rufen die auf dem Befehlszeilenkonsole-Anmeldebildschirm angezeigte URL auf. Zum Beispiel `http://kace_sma.local/admin`.

   Die Seite *Softwareübertragungsvereinbarung* wird angezeigt.
4. Stimmen Sie der Vereinbarung zu.

   Der Assistent für die *Ersteinrichtung* wird angezeigt.
5. Stellen Sie sicher, dass Sie über die erforderlichen Informationen für die Konfiguration der Appliance verfügen und klicken Sie dann auf **Weiter**.
6. Überprüfen Sie die Informationen auf der Seite *Diagnose-Support-Konsole* und notieren Sie den geheimen Schlüssel und die Offline-Token an einem sicheren Ort.
7. Geben Sie auf der Seite *Lizenzierungs- und Administratoreinstellungen* folgende Informationen an:

Option	Beschreibung
Lizenzschlüssel	Der Lizenzschlüssel, den Sie in der **Begrüßungs**-E-Mail von Quest erhalten haben. (mit Bindestrichen). Wenn Sie keinen Lizenzschlüssel besitzen, wenden Sie sich an den **Quest Support** unter https://support.quest.com/contact-support.
Name der Firma	Der Name Ihrer Firma oder Gruppe.

Option	Beschreibung
E-Mail-Adresse des Administrators	Die E-Mail-Adresse, an die Sie Kommunikation von Quest erhalten möchten.
Kennwort	Das Kennwort für das Standardkonto **admin**. Mit diesem Konto melden Sie sich bei der **Administratorkonsole** der Appliance an. Das Standardkonto **admin** ist zu diesem Zeitpunkt das einzige Konto der Appliance. Wenn Sie das Kennwort für dieses Konto vergessen, muss das System möglicherweise auf die Werkseinstellungen zurückgesetzt werden, was einen Datenverlust zur Folge haben kann. **HINWEIS:** Wenn Sie über mehrere KACE Appliances verfügen, empfiehlt Quest, für alle Appliances dasselbe Kennwort für das **Administratorkonto** zu verwenden. Mit demselben Kennwort für das admin-Konto können Sie die Appliances später verknüpfen. Siehe Verknüpfen von Quest KACE Appliances.
Zweifaktor-Authentifizierung	Wenn Sie mehr Sicherheit für die Benutzer bereitstellen möchten, die sich bei der Appliance anmelden, setzen Sie diese Option auf *Aktiviert*. Diese Funktion fügt einen zusätzlichen Schritt beim Anmeldevorgang hinzu. Sie vertraut auf die Google Authenticator-App, um Verifizierungscodes zu generieren. Die App generiert in regelmäßigen Abständen einen neuen sechsstelligen Code. Wenn diese Option aktiviert ist, werden die Endbenutzer bei jeder Anmeldung aufgefordert, den aktuellen Verifizierungscode einzugeben. **HINWEIS:** Wenn Sie diese Funktion aktivieren, stellen Sie sicher, dass die Uhrzeit des Appliance-Servers und diejenige des Geräts, auf dem Google Authenticator ausgeführt wird, korrekt sind. Der Google Authenticator verlässt sich auf die aktuelle Zeit, um das Token zu erstellen. Wenn die Uhr des Servers nicht mit denen der Geräte synchronisiert wird, auf denen Google Authenticator ausgeführt wird, kann die Tokenvalidierung fehlschlagen, was zu Kontosperrungen führen kann.

8. Befolgen Sie die Anweisungen auf dem Bildschirm, um Ersteinrichtung abzuschließen.

   Sobald die Ersteinrichtung abgeschlossen ist, wird die Appliance neu gestartet und die **Administratorkonsole**-Anmeldeseite wird angezeigt.

   HINWEIS: Wenn Sie die IP-Adresse der Appliance geändert haben, wechseln Sie zu der neuen Adresse, um die Anmeldeseite aufzurufen.

9. Melden Sie sich bei der Administratorkonsole an und verwenden Sie dazu die Anmelde-ID admin und das Kennwort, das Sie bei der Ersteinrichtung festgelegt haben.

Wenn die Zweifaktor-Authentifizierung auf der Seite *Lizenzierungs- und Administratoreinstellungen* aktiviert wurde, wird die Seite *Zweifaktor Authentifizierung konfigurieren* angezeigt.

10. **Nur Zweifaktor-Authentifizierung**. Befolgen Sie die Anweisungen auf der Seite *Zweifaktor-Authentifizierung konfigurieren*, um einen Google Authenticator-Verifizierungscode mit Ihrem Smartphone zu erstellen. Geben Sie in das Feld *Verifizierungscode* den Google Authenticator-Code ein und klicken Sie auf **Konfiguration fertig stellen**. Bei jeder nachfolgenden Anmeldung wird ein neuer Verifizierungscode benötigt.

    Um diesen Schritt zu überspringen, klicken Sie auf **Weiter**. Sie können diesen Schritt nur innerhalb eines zuvor konfigurierten Übergangszeitfensters überspringen. Weitere Informationen hierzu finden Sie unter Sicherheitseinstellungen für die Appliance konfigurieren.

Die **Administratorkonsole** wird angezeigt und die Appliance kann verwendet werden. Die für die Datums- und Uhrzeitinformationen verwendeten Gebietsschemaformate, die bei Ihrer ersten Anmeldung in der **Administratorkonsole** angezeigt werden, sind durch Ihre Browsereinstellungen festgelegt. Zum Ändern der Spracheinstellungen siehe Konfigurieren der Gebietsschema-Einstellungen.

Zugriff auf die Befehlszeilenkonsole

Die **Befehlszeilenkonsole** ist ein Terminalfenster für die Appliance. Über diese Benutzeroberfläche können die Appliance-Einstellungen wie mit der **Administratorkonsole** der Appliance konfiguriert werden. Das ist hilfreich, wenn kein DHCP-Server verfügbar und eine Anmeldung an der **Administratorkonsole** nicht möglich ist.

Die **Befehlszeilenkonsole** wird nicht in Verbindung mit K1 als Service verwendet.

1. Bei Verwendung einer physischen Appliance:
   a. Schließen Sie einen Monitor und eine Tastatur direkt an der Appliance an.
   b. Schließen Sie ein Netzwerkkabel an den entsprechenden Port an:

   c. Schalten Sie die Appliance ein.

      Der **Befehlszeilenkonsole**-Anmeldebildschirm wird auf dem an die Appliance angeschlossenen Monitor angezeigt.

2. Wenn Sie eine virtuelle Appliance-Version haben, schalten Sie den virtuellen Computer ein, um die Appliance zu starten.

   Der **Befehlszeilenkonsole**-Anmeldebildschirm wird angezeigt.

3. Geben Sie an der Eingabeaufforderung Folgendes ein:

   Anmeldename: `konfig`

   Kennwort: `konfig`

4. Wählen Sie die Sprache, die für die Befehlszeilenkonsole verwendet werden soll. Mit den Pfeiltasten können Sie zwischen den Feldern wechseln.
5. Konfigurieren Sie die Netzwerkeinstellungen. Siehe Netzwerkeinstellungen der Appliance ändern.

   TIPP: Mit der Nach-rechts- bzw. der Nach-links-Taste können Sie Optionen in den Feldern auswählen. Mit der Nach-oben- bzw. Nach-unten-Taste können Sie zwischen den Feldern wechseln.

6. Verschieben Sie den Cursor mithilfe der Nach-unten-Taste auf *Speichern* und drücken Sie dann die **Eingabetaste**.

   Die Appliance wird neu gestartet.

Verfolgen von Konfigurationsänderungen

Wenn Verlaufsabonnements zur Aufbewahrung von Informationen konfiguriert wurden, können Sie Details zu den an Einstellungen, Assets und Objekten vorgenommenen Änderungen anzeigen.

Diese Informationen beinhalten auch das Datum der Änderung und den Benutzer, der diese vorgenommen hat. Dies kann bei der Fehlerbehebung nützlich sein.

Verwandte Themen

Informationen zu den Verlaufseinstellungen

Konfigurieren der allgemeinen Einstellungen auf System- und Verwaltungsebene

Wenn die Organisationskomponente auf Ihrer Appliance aktiviert ist, sind die allgemeinen Einstellungen auf Verwaltungs- und Systemebene verfügbar. Wenn die Organisationskomponente auf Ihrer Appliance nicht aktiviert ist, sind alle allgemeinen Einstellungen auf Verwaltungsebene verfügbar.

Wenn die Organisationskomponente für Ihre Appliance aktiviert ist, siehe:

- Allgemeine Appliance-Einstellungen bei aktivierter Organisationskomponente konfigurieren.
- Allgemeine Einstellungen auf Verwaltungs- oder organisationsspezifischer Ebene konfigurieren.

Wenn die Organisationskomponente nicht aktiviert ist, finden Sie weitere Informationen unter:

- Allgemeine Appliance-Einstellungen ohne aktivierte Organisationskomponente konfigurieren.

Allgemeine Appliance-Einstellungen bei aktivierter Organisationskomponente konfigurieren

Wenn die Organisationskomponente auf Ihrer Appliance aktiviert ist, konfigurieren Sie allgemeine Einstellungen auf Systemebene.

Wenn die Organisationskomponente auf Ihrer Appliance nicht aktiviert ist, lesen Sie in Allgemeine Appliance-Einstellungen ohne aktivierte Organisationskomponente konfigurieren weiter.

1. Rufen Sie die Seite *Allgemeine Einstellungen* auf Systemebene auf:
   a. Melden Sie sich bei der Systemadministratorkonsole der Appliance an: `http://`**appliance_hostname**`/system`. Oder wählen Sie in der Dropdown-Liste rechts oben auf der Seite den Eintrag **System** aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Einstellungen** und anschließend auf **Systemsteuerung**.
   c. Klicken Sie in der *Systemsteuerung* auf **Allgemeine Einstellungen**.
2. Geben Sie im oberen Bereich die folgenden Informationen ein:

Option	Beschreibung
Name der Firma	Geben Sie den Namen Ihrer Firma ein.
Standardgebietsschema	Wählen Sie die Sprache aus, die in der **Befehlszeilenkonsole** verwendet werden soll, die das Benutzerkonto `konfig` verwendet.

Option	Beschreibung
Suffix der Firmen-E-Mail-Adresse	Geben Sie die Domäne ein, von der die Benutzer E-Mails senden. Beispiel: quest.com.
E-Mail-Adresse des Appliance-Administrators	Geben Sie die E-Mail-Adresse des Appliance-Administrators ein. An diese Adresse werden systembezogene Meldungen einschließlich kritischer Warnungen gerichtet.
Sitzungs-Timeout	Legen Sie die Zahl der inaktiven Stunden fest, die zugestanden werden, bevor Benutzersitzungen beendet werden und Benutzer sich erneut anmelden müssen. Der Standardwert ist 1. Die **Benutzerkonsole** und die **Administratorkonsole** verfügen über Zähler für den Sitzungs-Timeout, um die Benutzer auf die Frist hinzuweisen. Dabei werden nur Zeiträume ohne Aktivität gezählt. Der Zähler startet neu, sobald der Benutzer eine beliebige Aktion ausführt, die die Konsole zu einer Interaktion mit dem Appliance-Server veranlasst (beispielsweise Aktualisieren eines Fensters, Speichern von Änderungen und Wechseln zwischen Fenstern). Wenn der Zähler den eingestellten Grenzwert erreicht, wird der Benutzer abgemeldet. Nicht gespeicherte Änderungen gehen verloren und die Anmeldeseite wird angezeigt. Der Timeout-Zähler der Sitzung wird in der oberen rechten Ecke jeder Konsole angezeigt.
Mobilgerätezugriff aktivieren	Aktiviert bzw. deaktiviert den Mobilgerätezugriff auf die Appliance. Der Mobilgerätezugriff ermöglicht die Interaktion mit der Appliance mithilfe der KACE GO-App für Smartphones und Tablets mit iOS und Android. Administratoren können mithilfe der App auf Service Desk-, Inventar- und Anwendungsbereitstellungsfunktionen zugreifen. Siehe Konfigurieren des Mobilgerätezugriffs.
Organisationsauswahl bei Anmeldung erforderlich	Zeigt die Dropdown-Liste *Organisation* auf der Anmeldeseite der **Administratorkonsole** unter `http://`**appliance_hostname**`/admin` an, wobei **appliance_hostname** der Hostname Ihrer Appliance ist. Hier können Sie bei der Anmeldung eine Organisation auswählen. Wenn diese Option deaktiviert ist, wird die Dropdown-Liste *Organisation* nicht auf der Anmeldeseite angezeigt und Sie können sich von `http://`**appliance_hostname**`/admin` aus nur bei der Standardorganisation anmelden. Wenn Schneller Wechsel von Organisationen aktiviert ist, können Sie jedoch nach Anmeldung bei der Standardorganisation zwischen Organisationen umschalten.
Organisationsmenü in Verwaltungskopfzeile anzeigen	Zeigt die Dropdown-Liste *Schneller Wechsel* in der oberen rechten Ecke der **Administratorkonsole** neben den Anmeldeinformationen an. Diese Dropdown-Liste ermöglicht die Umgehung

Option	Beschreibung
	der Anmeldeseite beim Umschalten von einer Organisation auf eine andere. Damit sie in der Dropdown-Liste erscheinen, müssen Organisationen dasselbe Kennwort für das **Administratorkonto** besitzen; nur Organisationen, deren **Administratorkennwörter** übereinstimmen, werden in der Liste angezeigt. Änderungen an der Dropdown-Liste werden erst angezeigt, wenn Sie sich abmelden und erneut anmelden.

3. **Optional**. Geben Sie im Abschnitt *Beta-Benachrichtigungen* an, ob Sie am Betatestprogramm teilnehmen möchten.

   Teilnehmer des Betatestprogramms erhalten Benachrichtigungen, wenn eine Betaversion der Appliance verfügbar wird. Diese Benachrichtigungen werden als Warnungen auf dem Dashboard der Startseite angezeigt.

   Diese Benachrichtigungen können sich auf bestimmte Konfigurationen beziehen. Wenn Sie diese Option aktivieren, werden keine automatisierten Upgrades auf Beta-Versionen ausgelöst und die Appliance wird nicht automatisch für das Betatestprogramm registriert. Für die Teilnahme an dem Betatestprogramm ist weiterhin eine Anmeldung erforderlich, und die Details werden in den Benachrichtigungen bereitgestellt.

   Weitere Informationen zum Startseiten-Dashboard finden Sie unter Verwenden der Komponente "Startseite".

   a. Wählen Sie **Beta-Benachrichtigungen von KACE aktivieren** aus.
   b. Wenn Sie möchten, dass diese Benachrichtigungen nur in der Systemverwaltungskonsole angezeigt werden, wählen Sie **Beta-Benachrichtigungen auf System-UI beschränken** aus.

   Wenn diese Option deaktiviert bleibt, werden die Beta-Benachrichtigungen sowohl in der **Administratorkonsole** als auch in der **Systemverwaltungskonsole** angezeigt.

4. Zeigen Sie im Abschnitt *Agent* den Aufgabendurchsatz des KACE Agent an bzw. konfigurieren Sie diesen:

Option	Beschreibung
Letzte Aktualisierung des Aufgabendurchsatzes	Dieser Wert gibt Datum und Uhrzeit der letzten Aktualisierung des Aufgabendurchsatzes der Appliance an.
Aktueller Lastdurchschnitt	Der Wert in diesem Feld steht für die Last auf einer Appliance zu einem bestimmten Zeitpunkt. Damit die Appliance normal läuft, muss der Feldwert zwischen 0,0 und 10,0 liegen.
Aufgabendurchsatz	Der Wert, der steuert, wie geplante Aufgaben, z.B. Inventarerfassung, Skripterstellung und Patch-Aktualisierungen, durch die Appliance ausbalanciert werden. **HINWEIS:** Dieser Wert kann nur erhöht werden, wenn der Wert im Feld „Aktueller Lastdurchschnitt“ nicht über 10,0 liegt und die Zeit für die letzte Aktualisierung des Aufgabendurchsatzes mehr als 15 Minuten beträgt.

5. Ändern Sie im Abschnitt Benutzerkonsole den Text nach Bedarf:

Option	Beschreibung
Titel	Die Überschrift, die auf der Anmeldeseite der **Benutzerkonsole** angezeigt wird.
Begrüßungsmeldung	Ein Begrüßungshinweis oder eine Beschreibung der **Benutzerkonsole**. Dieser Text wird unterhalb des Titels auf der Anmeldeseite der **Benutzerkonsole** angezeigt.

6. Wählen Sie im Abschnitt *Nutzungsrichtlinie* Richtlinieneinstellungen aus:

Option	Beschreibung
Aktiviert	Aktivieren Sie auf der Appliance die Anzeige Ihrer Richtlinie. Legen Sie fest, dass Benutzer die Bedingungen Ihrer Richtlinie akzeptieren müssen, wenn Sie auf die **Administratorkonsole**, **Benutzerkonsole** oder **Befehlszeilenkonsole** zugreifen oder sich über SSH oder FTP anmelden.
Titel	Die Kopfzeile der Richtlinie, die auf der Anmeldeseite der **Benutzerkonsole** angezeigt werden soll.
Meldung	Details der Richtlinie, die unterhalb des *Titels* auf der Anmeldeseite angezeigt werden. Benutzer müssen den Bedingungen der Richtlinie zustimmen, bevor sie sich bei der **Benutzerkonsole** anmelden können.

7. Geben Sie im Abschnitt *Berichterstellung* das Kennwort für das Berichtssystem an:

Option	Beschreibung
Benutzername	(Schreibgeschützt) Der zur Erstellung von Berichten verwendete Benutzername. Der Benutzername für die Berichterstellung ermöglicht Zugriff auf die Datenbank (und damit weitere Berichterstellungstools), jedoch ohne Schreibzugriff für den Benutzer.
Benutzerkennwort	Das Benutzerkennwort für Berichte. Dieses Kennwort wird nur vom Berichterstellungssystem und MySQL™ verwendet.

8. Wählen Sie im Abschnitt *Protokollaufbewahrung* die Anzahl der Tage aus, für die Protokollinformationen gespeichert werden sollen. Protokolleinträge, die älter sind als die ausgewählte Anzahl an Tagen, werden automatisch aus dem Protokoll gelöscht. Siehe Appliance-Protokolle anzeigen.
9. Wählen Sie im Abschnitt *An uns weitergeben* eine der folgenden Datenfreigabeoptionen:

   Zum Validieren der Produktlizenz sammelt Quest einige lizenzbezogene Informationen wie die MAC-Adresse der Appliance, die Version der Appliance-Software, den Lizenzschlüssel und die Zahl der verwalteten Geräte, unabhängig von den in diesem Abschnitt gewählten Datenfreigabeoptionen.

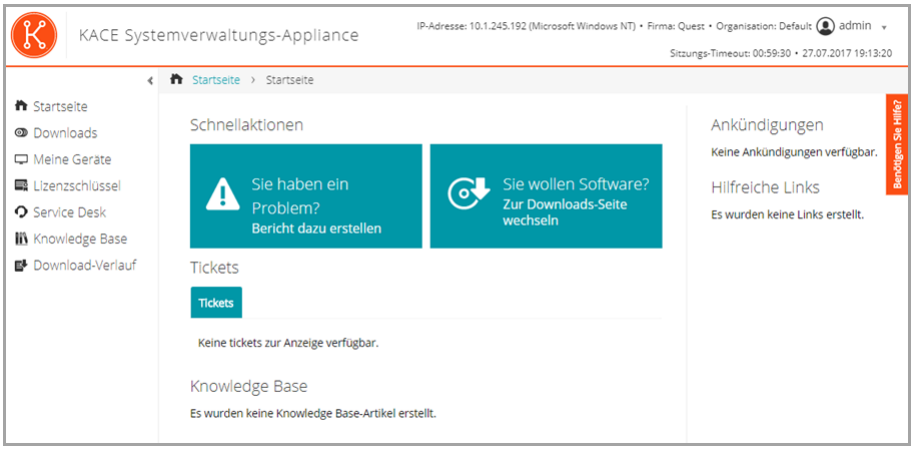
Option	Beschreibung
Zusammenfassung von Nutzungsdaten weitergeben ...	(Empfohlen) Geben Sie Übersichtsinformationen an Quest weiter. Zu diesen Informationen zählen

Option	Beschreibung
	der Betriebszustand der Appliance, die Betriebszeit und der Lastdurchschnitt sowie die Zahl der Geräte, verwalteten Installationen und Anwendungen, die von der Appliance verwaltet werden. Diese Option wird empfohlen, da sie dem **Quest Support** zusätzliche Informationen liefert, falls Sie Unterstützung benötigen. Quest verwendet die weitergegebenen Daten außerdem zur Planung von Produktverbesserungen.
Detaillierte Nutzungsdaten und Absturzberichte weitergeben ...	(Empfohlen) Geben Sie detaillierte Informationen an Quest und anonyme Informationen an ITNinja.com weiter. Zu diesen Informationen zählen Absturzberichte vom Agenten und der Appliance, Statistiken zur Nutzung der Benutzeroberfläche und Inventarinformationen wie beispielsweise Anwendungstitel. Quest nutzt diese Informationen zur Verbesserung des Softwarekatalogs. ITNinja nutzt anonyme Daten zur Ermittlung relevanter Inhalte auf http://www.itninja.com für auf der Appliance **Administratorkonsole** bereitgestellte dynamische Feeds. ITNinja.com ist eine Community-Website, auf der IT-Spezialisten Informationen teilen können und eine Vielzahl von Themen in den Bereichen Systemverwaltung und Systembereitstellung finden. Der ITNinja-Feed ist eine Funktion, über die Tipps zur Softwarebereitstellung und andere kontextbezogene Informationen auf den jeweiligen Seiten in der **Administratorkonsole** der Appliance dynamisch angezeigt werden. Zum Aktivieren des ITNinja-Feeds müssen Sie **Detaillierte Nutzungsdaten weitergeben ...** auswählen. Durch diese Einstellung werden Informationen anonym an ITNinja weitergegeben. Der ITNinja-Feed ist nur verfügbar, wenn **Zusammenfassung von Nutzungsdaten weitergeben ...** ausgewählt ist. Darüber hinaus ist er nur auf Seiten mit Bezug zu Software und Bereitstellung verfügbar, beispielsweise auf den Detailseiten zu Software, verwalteter Installation oder Dateisynchronisierung. Der Feed ist nicht auf der Detailseite zum *Softwarekatalog* verfügbar. Deaktivieren Sie diese Option, um zu verhindern, dass die Appliance Inventardaten an die ITNinja Community weitergibt. Durch das Deaktivieren dieser Option werden allerdings keine Informationen entfernt, die bereits weitergegeben wurden. Weitere Informationen erhalten Sie vom .
Erweiterte Patchdiagnose freigeben	(Empfohlen) Geben Sie detaillierte Patch-Diagnosen mit Quest frei.

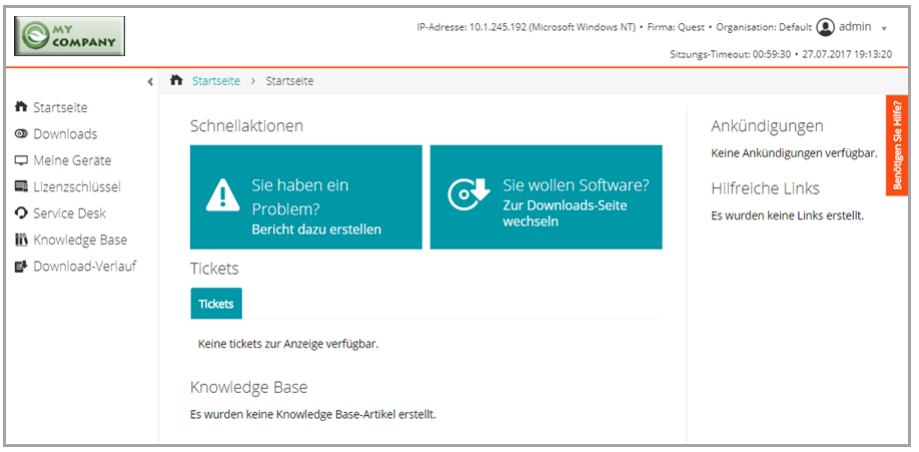
10. Um eine benutzerdefinierte Administratorkonsole, Benutzerkonsole, Berichtslogos und Hintergrundfarben zu verwenden, geben Sie in den Abschnitten *Login Screen Options (Optionen des Anmeldebildschirms)* die folgenden Informationen an.

Option	Beschreibung
Hintergrundfarbe für die Anmeldung an der Systemkonsole **Hintergrundfarbe für die Anmeldung an der Admin-Konsole** **Hintergrundfarbe für die Anmeldung bei der Benutzerkonsole**	Sie können von den folgenden Ebenen auf die Appliance zugreifen: • Die **Administratorkonsole** zeigt organisationsbezogene Funktionen an. • **Systemverwaltungskonsole** bietet Zugriff auf Appliance-bezogene Funktionen. • Die **Benutzerkonsole** stellt Anwendungen für Benutzer auf Self-Service-Basis zur Verfügung. Außerdem ermöglicht sie Benutzern das Einsenden von Service Desk Support-Tickets, mit denen sie Hilfe anfordern oder Fehler melden können. Sie können auf die **Benutzerkonsole** unter `http://<appliance_hostname>/user` zugreifen, wobei `<appliance_hostname>` der Hostname der Appliance ist. Für jede dieser webbasierten Schnittstellen können Sie eine andere Hintergrundfarbe des Anmeldebildschirms festlegen. Alle auf Organisationsebene angegebenen Farben setzen die Einstellungen auf Systemebene außer Kraft. Klicken Sie auf die Farbauswahl und legen Sie damit die Farbe fest, die im Hintergrund des Anmeldebildschirms angezeigt werden soll. Sie können die Farbe mit der Maus auswählen oder die RGB-Werte nach Bedarf angeben. Wenn Sie die Farbauswahl schließen, zeigt das Feld *HTML-Farbcode* auf der rechten Seite den HTML-Code der ausgewählten Farbe an. Um die Auswahl rückgängig zu machen, klicken Sie auf **Zurücksetzen** und beginnen Sie von vorne. **HINWEIS:** Die Farbauswahl wird in Internet Explorer 11 nicht unterstützt.
Systemkonsolenlogo **Adminkonsolenlogo** **Benutzerkonsolenlogo** **Berichtslogo**	Klicken Sie in jedem entsprechenden Abschnitt auf **Datei auswählen**, und geben Sie die Grafikdatei an, die Sie als benutzerdefiniertes Logo in den verfügbaren Weboberflächen und in systemgenerierten Berichten verwenden möchten. Die unterstützten Grafikdateiformate sind `.bmp`, `.gif`, `.jpg` und `.png`. Alle auf Organisationsebene konfigurierten Logos überschreiben die Einstellungen auf Systemebene. Das Standardberichtslogo und ein Beispiel für eine benutzerdefinierte Version sehen Sie in den folgenden Abbildungen.

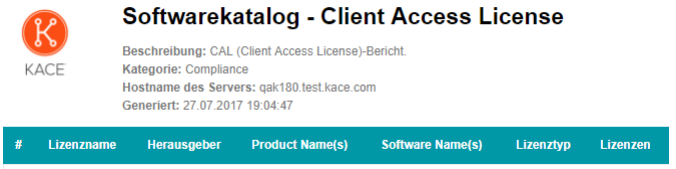
Standardlogo der Benutzerkonsole



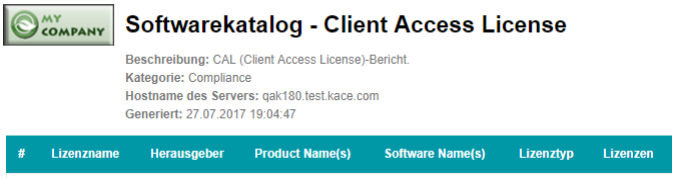
Benutzerdefiniertes Logo der Benutzerkonsole



Standard-Berichtslogo



Benutzerdefiniertes Berichtslogo



11. Wenn Sie Hewlett-Packard (HP) oder Lenovo Geräte verwalten, können Sie ihre Garantieinformationen abrufen. Geben Sie dazu im Abschnitt *Herstellergarantie-API-Schlüssel* die HP und/oder Lenovo API-Schlüssel an, um die Garantiedaten zu erhalten. Lenovo erfordert nur einen Schlüssel, während HP sowohl einen Schlüssel als auch ein Geheimnis benötigt. Diese Werte werden in der Datenbank verschlüsselt gespeichert.

WICHTIG: Um Garantieinformationen zu erhalten, müssen Sie die Garantie-API-Schlüssel des Herstellers konfigurieren. Vollständige Anweisungen finden Sie unter https://go.kace.com/to/k1000-help-warranty.

Wenn diese Option konfiguriert ist, werden die Informationen zur Gerätegarantie auf der Seite *Gerätedetails* in der Gruppe *Inventarinformationen* angezeigt, wenn Sie ein HP oder Lenovo Gerät auswählen. Weitere Informationen hierzu finden Sie unter Elementegruppen und -abschnitte in Gerätedetails.

Option	Beschreibung
Hewlett-Packard	Wählen Sie diese Option, wenn Sie Garantieinformationen für Ihre verwalteten HP Geräte erhalten möchten. Wenn diese Option ausgewählt ist und Sie deaktivieren, werden der HP API-Schlüssel und das Geheimnis aus der Datenbank entfernt.
Schlüssel	Der API-Schlüssel zum Abrufen von Garantieinformationen für verwaltete HP Geräte.
Geheim	Das Geheimnis zum Abrufen von Garantieinformationen für verwaltete HP Geräte.
Lenovo	Wählen Sie diese Option, wenn Sie Garantieinformationen für Ihre verwalteten Lenovo Geräte erhalten möchten. Wenn diese Option ausgewählt ist und Sie deaktivieren, wird der Lenovo Schlüssel aus der Datenbank entfernt.
Schlüssel	Der API-Schlüssel zum Abrufen von Garantieinformationen für verwaltete Lenovo Geräte.

12. Klicken Sie auf **Dienste speichern und neu starten**.

Verwandte Themen

Konfigurieren der Gebietsschema-Einstellungen

Konfigurieren des Mobilgerätezugriffs

Erstellen und Verwalten von Organisationen

Allgemeine Einstellungen auf Verwaltungs- oder organisationsspezifischer Ebene konfigurieren

Wenn die Organisationskomponente auf Ihrer Appliance aktiviert ist, konfigurieren Sie allgemeine Einstellungen auf organisationsspezifischer Ebene auf Verwaltungsebene. Die allgemeinen Einstellungen werden für jede Organisation separat konfiguriert.

Siehe Hinzufügen, Bearbeiten und Löschen von Organisationen.

Wenn die Organisationskomponente auf Ihrer Appliance nicht aktiviert ist, lesen Sie in Allgemeine Appliance-Einstellungen ohne aktivierte Organisationskomponente konfigurieren weiter.

1. Rufen Sie die Seite *Allgemeine Einstellungen* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen*

aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.

b. Klicken Sie in der linken Navigationsleiste auf **Einstellungen** und anschließend auf **Allgemeine Einstellungen**.

2. Geben Sie im Bereich *Allgemeine Optionen* die folgenden Informationen ein bzw. zeigen Sie sie an:

Option	Beschreibung
Zuletzt aktualisiert und **Name der Organisation**	(Schreibgeschützt) Das Datum, an dem die Information geändert wurde, und der Name der Organisation. Sie können den Wert *Name der Organisation* auf Systemebene bearbeiten. Siehe Organisationen hinzufügen oder bearbeiten.
Name der Firma	Geben Sie den Namen Ihrer Firma ein.
E-Mail-Adresse des Administrators	Geben Sie die E-Mail-Adresse des Appliance-Administrators ein. An diese Adresse werden systembezogene Meldungen einschließlich kritischer Warnungen gerichtet.
Suffix der Firmen-E-Mail-Adresse	Geben Sie die Domäne ein, von der die Benutzer E-Mails senden. Beispiel: beispiel.com.

3. Optional: Geben Sie im Abschnitt *Gebietsschema-Einstellungen* die Gebietsschema-Einstellungen an. Siehe Konfigurieren der Gebietsschema-Einstellungen.

Option	Beschreibung
Organisationsgebietsschema	Wählen Sie das Gebietsschema aus, das für die **Administratorkonsole** und die **Benutzerkonsole** der ausgewählten Organisation verwendet werden soll. Wenn Sie mehrere Organisationen haben, können Sie unterschiedliche Gebietsschemata für die unterschiedlichen Organisationen auswählen. Siehe: • Hinzufügen, Bearbeiten und Löschen von Organisationen • Konfigurieren der Gebietsschema-Einstellungen

4. Optional: Wählen Sie im Abschnitt *Samba Freigabeeinstellungen* die Dateifreigabeoptionen und klicken Sie auf **Samba Einstellungen speichern**. Sind die Dateifreigaben deaktiviert, müssen Sie sie auf Systemebene aktivieren, damit Sie sie auch für die Organisation aktivieren können. Siehe Sicherheitseinstellungen für die Appliance konfigurieren.

Option	Beschreibung
Dateifreigabe aktivieren	Verwenden Sie die Client-Freigabe der Appliance, um Dateien zu speichern (beispielsweise zur Anwendungsinstallation auf verwalteten Geräten). Die Client-Freigabe der Appliance verfügt über einen integrierten Windows Dateiserver, der vom Bereitstellungsdienst verwendet werden kann, um die Verteilung des Samba Clients in Ihrem Netzwerk zu unterstützen. Quest empfiehlt, diesen Dateiserver nur zu aktivieren, wenn Sie

Option	Beschreibung
	Anwendungsinstallationen auf verwalteten Geräten ausführen.
Dateifreigabe - Kennwort für 'admin'-Benutzer	Geben Sie das Kennwort ein, um mit dem Administratorkonto auf das Dateifreigabeverzeichnis zuzugreifen.

5. Geben Sie im Abschnitt *Einstellungen der Client-IP-Adresse ignorieren* die zu ignorierenden IP-Adressen ein. Trennen Sie die einzelnen Adressen durch ein Komma. Das Ignorieren von IP-Adressen ist sinnvoll, wenn mehrere Geräte dieselbe IP-Adresse melden könnten, beispielsweise eine Proxy-Adresse.
6. Wählen Sie im Abschnitt *Warnkonfigurationen zur Lizenznutzung* den Prozentsatz aus, der bei der Nutzung von Softwarelizenzen für den Warnungsschwellenwert und den kritischen Schwellenwert verwendet werden soll. Wenn Sie Software-Lizenz-Assets konfiguriert haben, werden Schwellenwertinformationen in den lizenzbezogenen Widgets auf dem *Dashboard* angezeigt.
7. Wählen Sie im Abschnitt *Datenaufbewahrung* die Optionen für die Datenaufbewahrung in der Datenbank der Appliance aus.

Option	Beschreibung
Daten zur Gerätebetriebszeit aufbewahren	Die Anzahl der Monate, für die Informationen zur Gerätebetriebszeit in der Datenbank der Appliance gespeichert werden. Die Gerätebetriebszeit liefert Informationen zur Anzahl der Stunden pro Tag, die verwaltete Geräte in Betrieb sind. Sie können diese Daten für eine bestimmte Anzahl an Monaten, **Unbegrenzt** oder nie (**Deaktiviert**) speichern.
Erfassungsdaten beibehalten	Die Anzahl der Monate, für die Erfassungsdaten in der Datenbank der Appliance gespeichert werden. Erfassungsdaten sind Informationen darüber, wie Anwendungen auf den von Ihnen verwalteten Windows und Mac Geräten installiert und verwendet werden. Erfassungsdaten, die älter als die ausgewählte Anzahl von Monaten sind, werden am ersten Tag jedes Monats gelöscht. Siehe Informationen zu Erfassungsinformationen.
Nicht katalogisierte Daten im Softwarekatalog beibehalten	Gibt an, ob Informationen über nicht katalogisierte Anwendungen in der Datenbank der Appliance gespeichert werden sollen. Nicht katalogisierte Anwendungen sind ausführbare Dateien, die zwar im Appliance-Inventar, aber nicht im Softwarekatalog enthalten sind. Standardmäßig speichert die Appliance Informationen über diese Anwendungen. Für Organisationen mit einer großen Anzahl verwalteter Geräte kann durch die Speicherung dieser Daten die Größe der Datenbank jedoch erheblich anwachsen. Durch die Zunahme der Datenbankgröße können die Ladezeit der Seiten in der **Administratorkonsole** und der Zeitbedarf für die Durchführung der Datenbanksicherungen ansteigen. Aktivieren Sie dieses Kontrollkästchen, um Daten für nicht katalogisierte Software in der Appliance-Datenbank zu speichern. Deaktivieren Sie das

Option	Beschreibung
	Kontrollkästchen, um die Datenaufbewahrung zu deaktivieren. Wenn die Datenaufbewahrung für nicht katalogisierte Software deaktiviert ist: • Die Agenten auf verwalteten Geräten laden weiterhin die vollständigen Inventarinformationen hoch und für Rohdaten mit Anwendungsbezug werden Fingerprints erzeugt. Wenn die Datenfreigabe aktiviert ist, werden die Daten außerdem in den Quest KACE Softwarekatalog hochgeladen. Siehe Konfigurieren der Datenfreigabeeinstellungen. • Die Appliance speichert weiterhin Informationen mit Bezug zu katalogisierten Anwendungen und lokal katalogisierten Anwendungen in der Organisationsdatenbank. • Informationen mit Bezug zu nicht katalogisierten Anwendungen werden nicht in der Organisationsdatenbank gespeichert und die Liste in der **Administratorkonsole** ist leer. • Berichte zu katalogisierten Anwendungen funktionieren weiter wie erwartet. Berichte mit Bezug zu nicht katalogisierten Anwendungen enthalten jedoch nur Anwendungen, die in katalogisierten Softwaretiteln enthalten sind.

8. Geben Sie im Abschnitt *Asset-Archiv* die Anzahl der Tage an, wie lange Sie die zur Archivierung markierten Assets behalten wollen, bevor Sie diese archivieren. Der Standardwert beträgt 3 Tage.
9. Geben Sie im Bereich *Benutzerarchiv* nach Bedarf an, ob Sie die Benutzerarchivierung aktivieren möchten.
   a. Um Benutzerkonten archivieren zu können, aktivieren Sie das Kontrollkästchen **Benutzerarchivierung aktivieren**.

   HINWEIS: Wenn die Benutzerarchivierung aktiviert ist, können Benutzerkonten nur gelöscht werden, wenn sie als archiviert gekennzeichnet sind.

   b. Geben Sie im Feld *Archivierungs-Tag* eine Bezeichnung ein, die sie mit dem Status archivierter Benutzer verknüpfen möchten. Beispielsweise `Archiviert` oder `Inaktiv`.
   c. Geben Sie an, ob Sie Service Desk-Ticket- und Asset-Zuordnungen zu archivierten Benutzern beibehalten möchten. Stellen Sie jedes der Felder *Ticket-Zuordnungen* und *Asset-Zuordnungen* auf eine der folgenden Optionen ein:

   - **Benutzer beibehalten**: Wählen Sie diese Option, wenn Sie dem archivierten Benutzer weiterhin Tickets oder Assets zuordnen möchten. Wenn Sie diese Option auswählen, wird das konfigurierte *Archivierungs-Tag* neben dem Namen des archivierten Benutzers angezeigt, um darauf hinzuweisen, dass der Benutzer nicht mehr aktiv ist.
   - **Benutzer entfernen**: Wählen Sie diese Option, wenn Sie alle Ticket- oder Asset-Zuordnungen zu archivierten Benutzern entfernen möchten.

   Weitere Informationen zur Archivierung von Benutzerkonten finden Sie unter Benutzerkonten archivieren.
10. Geben Sie im Abschnitt *Gerätezuordnung* an, wie Sie Benutzer den Geräten zuordnen möchten: **Einmalige Synchronisierung**, **Fortlaufenden Synchronisierung** oder **Deaktiviert**.
11. Klicken Sie im Abschnitt *Geräteaktionen* auf **Neue Aktion hinzufügen** und wählen Sie die zu aktivierenden skriptbasierten Aktionen aus.

Geräteaktionen sind skriptbasierte Aktionen, die auf verwalteten Geräten ausgeführt werden können. Es stehen bereits mehrere programmierte Aktionen zur Verfügung. Wenn Sie eine eigene Aktion hinzufügen möchten, wählen Sie im Menü **Aktion** die Option *Benutzerdefinierte Aktion* aus und geben Sie den Befehl im Textfeld *Befehlszeile* ein.

Die folgenden Variablen sind für Geräteaktionen verfügbar:

KACE_HOST_IP

KACE_HOST_NAME

KACE_CUSTOM_INVENTORY_*

Wenn Geräteaktionen ausgeführt werden, ersetzt die Appliance Variablen durch ihre entsprechenden Werte.

Ersetzen Sie bei KACE_CUSTOM_INVENTORY_ * das Sternchen (*) durch den Namen einer Softwareanwendung einer Regel für benutzerdefinierte Inventarisierung. Wenn die Geräteaktion ausgeführt wird, wird der Name durch den Wert der Regel für benutzerdefinierte Inventarisierung für das Gerät ersetzt. Geben Sie den Namen der Softwareanwendung in Großbuchstaben ein. Zulässig sind folgende Zeichen: [A-Z0-9.-].“

HINWEIS: Für die meisten Aktionen in der Dropdown-Liste *Aktion* müssen Sie zusätzliche Anwendungen installieren, damit sie ordnungsgemäß funktionieren. Wenn Sie beispielsweise DameWare nutzen möchten, müssen Sie sowohl auf Ihrem Gerät als auch auf dem, auf das Sie zugreifen möchten, TightVNC installieren.

Diese Funktion wird nur auf Windows-Geräten unterstützt. Auf dem Windows-Gerät, auf dem die Geräteaktion ausgeführt wird, muss der KACE Agent ab Version 9.0 installiert und verbunden sein.

Wenn Sie das Gerät über den Agenten initiieren, muss die ausführbare Datei für die Aktion hier platziert werden: `%PATH%`. Der Agent ist 32-Bit, also verwenden Sie auf 64-Bit-Windows-Geräten `%windir%/System32` als Alias für das Verzeichnis `%windir%/Wow64`. Wenn Sie ein Programm ausführen müssen, das sich im Verzeichnis `%windir%/System32` auf einem 64-Bit-Windows-System befindet, müssen Sie das virtuelle Verzeichnis `%windir%/SysNative` verwenden. Sie können entweder `%windir%/SysNative` zu Ihrer Umgebungsvariable `%PATH%` hinzufügen oder einen vollqualifizierten Pfad angeben, indem Sie bei der Definition Ihrer Geräteaktion `%windir%/SysNative` Ihrer ausführbaren Datei voranstellen.

12. Wählen Sie im Abschnitt *Patch-Zeitplan* Abschnitt, wenn Sie deaktivieren möchten, dass Administratoren Patches auf alle Geräte anwenden, das Kontrollkästchen **Alle Geräte ausblenden** aus.

    HINWEIS: Sie können diese Einstellung nur wählen, wenn Sie keine Patch-Zeitplan eingerichtet haben, die gegen alle Geräte laufen. Andernfalls wird eine Warnung angezeigt.

13. Geben Sie im Abschnitt *Zulässige Bulk-Aktionen* an, ob Bulk-Aktionen für KACE Cloud Mobile Device Manager (MDM) und virtuelle VMware-Maschinen aktiviert werden sollen. Wenn Bulk-Aktionen aktiviert sind, werden die zugehörigen Befehle für KACE Cloud MDM und virtuelle VMware-Maschinen über das Menü **Aktion auswählen** auf der Seite *Geräteliste* verfügbar.

Option	Beschreibung
Bulk-Aktionen für KACE Cloud MDM aktivieren	Aktivieren Sie dieses Kontrollkästchen, um Befehle für mehrere KACE Cloud MDM-Geräte auf der Seite *Geräteliste* zu aktivieren.
Bulk-Aktionen für virtuelle Maschinen aktivieren	Aktivieren Sie dieses Kontrollkästchen, um Befehle für mehrere VMware- oder Hyper-V-VMs auf der Seite *Geräteliste* zu aktivieren.

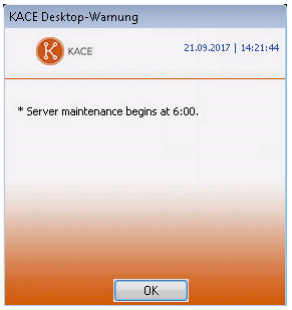
Option	Beschreibung
Bulk-Aktionen für Chrome-Betriebssystem aktivieren	Aktivieren Sie dieses Kontrollkästchen, um Befehle für mehrere Geräte mit Chrome-Betriebssystem auf der Seite *Geräteliste* zu aktivieren.

14. Um eine benutzerdefinierte Administratorkonsole, Benutzerkonsole, Berichte, Warnungslogos und Hintergrundfarben des KACE Agent zu verwenden, geben Sie in den Abschnitten *Login Screen Options (Optionen des Anmeldebildschirms)* die folgenden Informationen an.

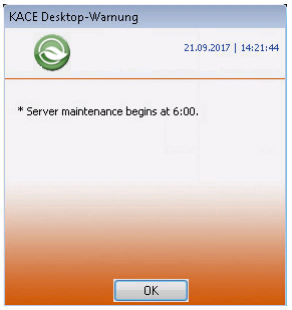
Option	Beschreibung
Admin Console Login Background Color (Hintergrundfarbe für die Anmeldung an der Admin-Konsole) **User Console Login Background Color (Hintergrundfarbe für die Anmeldung an der Benutzerkonsole)**	Sie können von den folgenden Ebenen auf die Appliance zugreifen: • Die **Administratorkonsole** zeigt organisationsbezogene Funktionen an. • **Systemverwaltungskonsole** bietet Zugriff auf Appliance-bezogene Funktionen. • Die **Benutzerkonsole** stellt Anwendungen für Benutzer auf Self-Service-Basis zur Verfügung. Außerdem ermöglicht sie Benutzern das Einsenden von Service Desk Support-Tickets, mit denen sie Hilfe anfordern oder Fehler melden können. Sie können auf die **Benutzerkonsole** unter `http://<appliance_hostname>/user` zugreifen, wobei `<appliance_hostname>` der Hostname der Appliance ist. Wenn Sie eine Organisation in der **Administratorkonsole** auswählen, können Sie eine andere Hintergrundfarbe für die Anmeldebildschirme der **Administratorkonsole** und **Benutzerkonsole** festlegen. Alle auf Organisationsebene angegebenen Farben setzen die Einstellungen auf Systemebene außer Kraft. Informationen zum Konfigurieren der Einstellungen auf Systemebene finden Sie unter Allgemeine Appliance-Einstellungen bei aktivierter Organisationskomponente konfigurieren. Klicken Sie auf die Farbauswahl und legen Sie damit die Farbe fest, die im Hintergrund des Anmeldebildschirms angezeigt werden soll. Sie können die Farbe mit der Maus auswählen oder die RGB-Werte nach Bedarf angeben. Wenn Sie die Farbauswahl schließen, zeigt das Feld *HTML-Farbcode* auf der rechten Seite den HTML-Code der ausgewählten Farbe an. Um die Auswahl rückgängig zu machen, klicken Sie auf **Zurücksetzen** und beginnen Sie von vorne. **HINWEIS:** Die Farbauswahl wird in Internet Explorer 11 nicht unterstützt.
Adminkonsolenlogo **Benutzerkonsolenlogo** **Berichtslogo**	Klicken Sie in jedem entsprechenden Abschnitt auf **Datei auswählen**, und geben Sie die Grafikdatei an, die als benutzerdefiniertes Logo in der **Administratorkonsole**, **Benutzerkonsole**,

Option	Beschreibung
Logo der Agenten-Warnmeldung	in systemgenerierten Berichten und in KACE Agent Warnungen verwendet werden soll, die auf verwalteten Geräten angezeigt werden. Die unterstützten Grafikdateiformate sind `.bmp`, `.gif`, `.jpg` und `.png`. Für KACE Agent Warnungen werden nur `.bmp`-Dateien unterstützen. Alle auf Organisationsebene konfigurierten Logos überschreiben die Einstellungen auf Systemebene. Die folgenden Abbildungen zeigen standardmäßige KACE Agent Warnungen und benutzerdefinierte Beispielversionen. Beispiele für Standard- und benutzerdefinierte Logos in der **Administratorkonsole**, **Benutzerkonsole** und in Berichten auf Systemebene finden Sie unter Allgemeine Appliance-Einstellungen bei aktivierter Organisationskomponente konfigurieren.

Standardlogo der Warnmeldung



Benutzerdefiniertes Logo der Warnmeldung



15. Klicken Sie auf **Dienste speichern und neu starten**.
16. Wenn Sie mehrere Organisationen haben, wiederholen Sie die oben aufgeführten Schritte für jede Organisation.

Allgemeine Appliance-Einstellungen ohne aktivierte Organisationskomponente konfigurieren

Wenn die Organisationskomponente auf Ihrer Appliance nicht aktiviert ist, sind alle allgemeinen Appliance-Einstellungen auf Verwaltungsebene verfügbar.

Wenn die Organisationskomponente auf Ihrer Appliance aktiviert ist, finden Sie weitere Informationen unter Allgemeine Einstellungen auf Verwaltungs- oder organisationsspezifischer Ebene konfigurieren.

1. Rufen Sie die Seite *Allgemeine Einstellungen* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`.
   b. Klicken Sie in der linken Navigationsleiste auf **Einstellungen** und anschließend auf **Allgemeine Einstellungen**.
2. Geben Sie im Bereich *Allgemeine Optionen* die folgenden Informationen ein:

Option	Beschreibung
Zuletzt aktualisiert	Schreibgeschützt: Das Datum, an dem die Information geändert wurde, und der Name der Organisation.
Name der Firma	Geben Sie den Namen Ihrer Firma ein.
E-Mail-Adresse des Administrators	Geben Sie die E-Mail-Adresse des Appliance-Administrators ein. An diese Adresse werden systembezogene Meldungen einschließlich kritischer Warnungen gerichtet.
Suffix der Firmen-E-Mail-Adresse	Geben Sie die Domäne ein, von der die Benutzer E-Mails senden. Beispiel: beispiel.com.
Mobilgerätezugriff aktivieren	Aktiviert bzw. deaktiviert den Mobilgerätezugriff auf die Appliance. Der Mobilgerätezugriff ermöglicht die Interaktion mit der Appliance mithilfe der KACE GO-App für Smartphones und Tablets mit iOS und Android. Administratoren können mithilfe der App auf Service Desk-, Inventar- und Anwendungsbereitstellungsfunktionen zugreifen. Siehe Konfigurieren des Mobilgerätezugriffs.
Sitzungs-Timeout	Legen Sie die Zahl der inaktiven Stunden fest, die zugestanden werden, bevor Benutzersitzungen beendet werden und Benutzer sich erneut anmelden müssen. Der Standardwert ist 1. Die **Benutzerkonsole** und die **Administratorkonsole** verfügen über Zähler für den Sitzungs-Timeout, um die Benutzer auf die Frist hinzuweisen. Dabei werden nur Zeiträume ohne Aktivität gezählt. Der Zähler startet neu, sobald der Benutzer eine beliebige Aktion ausführt, die die Konsole zu einer Interaktion mit dem Appliance-Server veranlasst (beispielsweise Aktualisieren eines Fensters, Speichern von Änderungen und Wechseln zwischen Fenstern). Wenn der Zähler den eingestellten Grenzwert erreicht, wird der Benutzer abgemeldet. Nicht gespeicherte Änderungen gehen verloren und die Anmeldeseite wird angezeigt. Der Timeout-Zähler der Sitzung wird in der oberen rechten Ecke jeder Konsole angezeigt.

3. Geben Sie im Abschnitt *Dateigrößenfilter für Client Drop* eine Dateigröße an.

Optionen	Beschreibung
Dateigrößenfilter für Client Drop	Ein Dateigrößenfilter für den Client-Drop-Speicherort der Organisation. Der Client-Drop-Speicherort ist ein Speicherbereich (Samba-Freigabe) für die Organisation auf der Appliance. Dieser Speicherbereich dient zum Hochladen großer Dateien, z. B. von Installationsprogrammen für Anwendungen und Appliance-Sicherungsdateien, auf die Appliance. Das Hochladen von Dateien auf den Client-Drop-Speicherort ist eine Alternative zum Hochladen von Dateien über die **Administratorkonsole** mit dem Standard-HTTP-Mechanismus, bei dem es bei großen Dateien zu Browser-Timeouts kommen kann. Der Filter *Client-Drop-Größe* bestimmt, ob auf den Client-Drop-Speicherort der Organisation hochgeladene Dateien in der Liste *Client-Drop-Datei hochladen und verknüpfen* auf der Seite *Softwaredetail* angezeigt werden. Wenn der Filter „Client-Drop-Größe“ z. B. auf 1 GB eingestellt ist, werden in der Liste *Client-Drop-Datei hochladen und verknüpfen* Dateien angezeigt, die 1 GB oder größer sind. Dateien, die kleiner als 1 GB sind, werden in der Liste nicht angezeigt. Anwendungsdateien werden vom Client-Drop-Speicherort der Organisation zu dem entsprechenden Bereich verschoben, wenn die Datei auf der Seite *Softwaredetail* ausgewählt und gespeichert wird. Am Client-Drop-Speicherort abgelegte Appliance-Sicherungsdateien werden automatisch als Appliance-Sicherungsdateien erkannt und innerhalb von fünf Minuten auf der Seite *Sicherungseinstellungen* für die Auswahl verfügbar. Siehe Dateien kopieren und auf dem Client-Drop-Speicherort der Appliance ablegen.

4. Geben Sie im Abschnitt Benutzerkonsole Anpassungen für den Benutzerkonsole-Text ein:

Option	Beschreibung
Titel	Die Überschrift, die auf der Anmeldeseite der **Benutzerkonsole** angezeigt wird. Die **Benutzerkonsole** ist die webbasierte Oberfläche, die Benutzern Anwendungen auf Self-Service-Basis zur Verfügung stellt. Außerdem ermöglicht sie Benutzern das Einsenden von Service Desk Support-Tickets, mit denen sie Hilfe anfordern oder Fehler melden können. Sie können auf die **Benutzerkonsole** unter `http://<appliance_hostname>/user` zugreifen, wobei `<appliance_hostname>` der Hostname der Appliance ist.
Begrüßungsmeldung	Ein Begrüßungshinweis oder eine Beschreibung der **Benutzerkonsole**. Dieser Text wird unterhalb des

Option	Beschreibung
	Titels auf der Anmeldeseite der **Benutzerkonsole** angezeigt.

5. Wählen Sie im Abschnitt *Nutzungsrichtlinie* Richtlinieneinstellungen aus:

Option	Beschreibung
Aktiviert	Aktivieren Sie auf der Appliance die Anzeige Ihrer Richtlinie. Legen Sie fest, dass Benutzer die Bedingungen Ihrer Richtlinie akzeptieren müssen, wenn Sie auf die **Administratorkonsole**, **Benutzerkonsole** oder **Befehlszeilenkonsole** zugreifen oder sich über SSH oder FTP anmelden.
Titel	Die Kopfzeile der Richtlinie, die auf der Anmeldeseite der **Benutzerkonsole** angezeigt werden soll.
Meldung	Details der Richtlinie, die unterhalb des *Titels* auf der Anmeldeseite angezeigt werden. Benutzer müssen den Bedingungen der Richtlinie zustimmen, bevor sie sich bei der **Benutzerkonsole** anmelden können.

6. Wählen Sie im Abschnitt *Protokollaufbewahrung* die Anzahl der Tage aus, für die Protokollinformationen gespeichert werden sollen. Protokolleinträge, die älter sind als die ausgewählte Anzahl an Tagen, werden automatisch aus dem Protokoll gelöscht. Siehe Zum Anzeigen von Microsoft Exchange Server-Fehlern auf Appliance-Protokolle zugreifen.
7. Geben Sie im Abschnitt *An uns weitergeben* Datenfreigabeoptionen an.

> **HINWEIS:** Zum Validieren der Produktlizenz sammelt Quest einige lizenzbezogene Informationen wie die MAC-Adresse der Appliance, die Version der Appliance-Software, den Lizenzschlüssel und die Zahl der verwalteten Geräte, unabhängig von den in diesem Abschnitt gewählten Datenfreigabeoptionen.

Option	Beschreibung
Zusammenfassung von Nutzungsdaten weitergeben ...	(Empfohlen) Geben Sie Übersichtsinformationen an Quest weiter. Zu diesen Informationen zählen der Betriebszustand der Appliance, die Betriebszeit und der Lastdurchschnitt sowie die Zahl der Geräte, verwalteten Installationen und Anwendungen, die von der Appliance verwaltet werden. Diese Option wird empfohlen, da sie dem **Quest Support** zusätzliche Informationen liefert, falls Sie Unterstützung benötigen. Quest verwendet die weitergegebenen Daten außerdem zur Planung von Produktverbesserungen.
Detaillierte Nutzungsdaten und Absturzberichte weitergeben ...	(Empfohlen) Geben Sie detaillierte Informationen an Quest und anonyme Informationen an ITNinja.com weiter. Zu diesen Informationen zählen Absturzberichte vom Agenten und der Appliance, Statistiken zur Nutzung der Benutzeroberfläche und Inventarinformationen wie beispielsweise Anwendungstitel. Quest nutzt diese Informationen zur Verbesserung des Softwarekatalogs. ITNinja nutzt anonyme Daten zur Ermittlung relevanter

Option	Beschreibung
	Inhalte auf http://www.itninja.com für auf der Appliance **Administratorkonsole** bereitgestellte dynamische Feeds. ITNinja.com ist eine Community-Website, auf der IT-Spezialisten Informationen teilen können und eine Vielzahl von Themen in den Bereichen Systemverwaltung und Systembereitstellung finden. Der ITNinja-Feed ist eine Funktion, über die Tipps zur Softwarebereitstellung und andere kontextbezogene Informationen auf den jeweiligen Seiten in der **Administratorkonsole** der Appliance dynamisch angezeigt werden. Zum Aktivieren des ITNinja-Feeds müssen Sie **Detaillierte Nutzungsdaten weitergeben ...** auswählen. Durch diese Einstellung werden Informationen anonym an ITNinja weitergegeben. Der ITNinja-Feed ist nur verfügbar, wenn **Zusammenfassung von Nutzungsdaten weitergeben ...** ausgewählt ist. Darüber hinaus ist er nur auf Seiten zu Software oder Bereitstellung verfügbar, beispielsweise auf den Detailseiten zu Software, verwalteter Installation oder Dateisynchronisierung. Der Feed ist nicht auf der Detailseite zum *Softwarekatalog* verfügbar. Deaktivieren Sie diese Option, um zu verhindern, dass die Appliance Inventardaten an die ITNinja Community weitergibt. Durch das Deaktivieren dieser Option werden allerdings keine Informationen entfernt, die bereits weitergegeben wurden. Weitere Informationen erhalten Sie vom .
Erweiterte Patchdiagnose freigeben	(Empfohlen) Geben Sie detaillierte Patch-Diagnosen mit Quest frei.

8. Geben Sie im Abschnitt *Gebietsschema-Einstellungen* die Gebietsschema-Einstellungen an. Durch diese Einstellungen werden die Formate für die in der Administratorkonsole angezeigten Datums- und Uhrzeitinformationen festgelegt.

Option	Beschreibung
Organisationsgebietsschema	Das für die **Administratorkonsole** und **Benutzerkonsole** der Organisation zu verwendende Gebietsschema.
Befehlszeilenkonsole Gebietsschema	Das Gebietsschema, das in der **Befehlszeilenkonsole** verwendet werden soll, die das Benutzerkonto `konfig` verwendet.

9. Geben Sie im Abschnitt *Einstellungen der Client-IP-Adresse ignorieren* die zu ignorierenden IP-Adressen ein. Trennen Sie die einzelnen Adressen durch ein Komma. Das Ignorieren von IP-Adressen ist sinnvoll, wenn mehrere Geräte dieselbe IP-Adresse melden könnten, beispielsweise eine Proxy-Adresse.
10. Wählen Sie im Abschnitt *Warnkonfigurationen zur Lizenznutzung* den Prozentsatz aus, der bei der Nutzung von Softwarelizenzen für den Warnungsschwellenwert und den kritischen Schwellenwert verwendet werden

soll. Wenn Sie Software-Lizenz-Assets konfiguriert haben, werden Schwellenwertinformationen in den lizenzbezogenen Widgets auf dem *Dashboard* angezeigt.

11. Geben Sie im Abschnitt *Benutzerkennwort für Berichterstellung aktualisieren* das Kennwort des für die Ausführung von Berichten zur Organisation erforderlichen Kontos an. Weder der *Datenbankname* noch der *Benutzername für den Bericht* kann geändert werden.
12. Wählen Sie im Abschnitt *Datenaufbewahrung* die Optionen für die Datenaufbewahrung in der Appliance aus. Sie können diese Daten für eine bestimmte Anzahl an Monaten, **Unbegrenzt** oder nie (**Deaktiviert**) speichern.

Option	Beschreibung
Daten zur Gerätebetriebszeit aufbewahren	Die Menge der zu speichernden Betriebszeitdaten für Geräte. Die Daten zur Gerätebetriebszeit liefern Informationen zu der Zahl der Stunden pro Tag, die Ihre verwalteten Geräte laufen. Sie können diese Daten für eine bestimmte Anzahl an Monaten, **Unbegrenzt** oder nie (**Deaktiviert**) speichern.
Erfassungsdaten beibehalten	Die Anzahl der Monate, für die Erfassungsdaten in der Datenbank der Appliance gespeichert werden. Erfassungsdaten sind Informationen darüber, wie Anwendungen auf den von Ihnen verwalteten Windows und Mac Geräten installiert und verwendet werden. Erfassungsdaten, die älter als die ausgewählte Anzahl von Monaten sind, werden am ersten Tag jedes Monats gelöscht. Siehe Informationen zu Erfassungsinformationen.
Nicht katalogisierte Daten im Softwarekatalog beibehalten	Gibt an, ob Informationen über nicht katalogisierte Anwendungen in der Datenbank der Appliance gespeichert werden sollen. Nicht katalogisierte Anwendungen sind ausführbare Dateien, die zwar im Appliance-Inventar, aber nicht im Softwarekatalog enthalten sind. Standardmäßig speichert die Appliance Informationen über diese Anwendungen. Für Organisationen mit einer großen Anzahl verwalteter Geräte kann durch die Speicherung dieser Daten die Größe der Datenbank jedoch erheblich anwachsen. Dadurch können die Ladezeit der Seiten in der **Administratorkonsole** und der Zeitbedarf für die Durchführung der Datenbanksicherungen ansteigen. Aktivieren Sie dieses Kontrollkästchen, um Daten für nicht katalogisierte Software in der Appliance-Datenbank zu speichern. Deaktivieren Sie das Kontrollkästchen, um die Datenaufbewahrung zu deaktivieren. Wenn die Datenaufbewahrung für nicht katalogisierte Software deaktiviert ist: • Die Agenten auf verwalteten Geräten laden weiterhin die vollständigen Inventarinformationen hoch und für Rohdaten mit Anwendungsbezug werden Fingerprints erzeugt. Wenn die Datenfreigabe aktiviert ist, werden die Daten außerdem in den Quest

Option	Beschreibung
	KACE Softwarekatalog hochgeladen. Siehe Konfigurieren der Datenfreigabeeinstellungen. • Die Appliance speichert weiterhin Informationen mit Bezug zu katalogisierten Anwendungen und lokal katalogisierten Anwendungen in der Organisationsdatenbank. • Informationen mit Bezug zu nicht katalogisierten Anwendungen werden nicht in der Organisationsdatenbank gespeichert und die Liste in der **Administratorkonsole** ist leer. • Berichte zu katalogisierten Anwendungen funktionieren weiter wie erwartet. Berichte mit Bezug zu nicht katalogisierten Anwendungen enthalten jedoch nur Anwendungen, die in katalogisierten Softwaretiteln enthalten sind.

13. Klicken Sie im Abschnitt *Geräteaktionen* auf **Neue Aktion hinzufügen** und wählen Sie die zu aktivierenden skriptbasierten Aktionen aus.

    Geräteaktionen sind skriptbasierte Aktionen, die auf verwalteten Geräten ausgeführt werden können. Es stehen bereits mehrere programmierte Aktionen zur Verfügung. Wenn Sie eine eigene Aktion hinzufügen möchten, wählen Sie im Menü **Aktion** die Option *Benutzerdefinierte Aktion* aus und geben Sie den Befehl im Textfeld *Befehlszeile* ein.

    Die folgenden Variablen sind für Geräteaktionen verfügbar:

    KACE_HOST_IP

    KACE_HOST_NAME

    KACE_CUSTOM_INVENTORY_*

    Wenn Geräteaktionen ausgeführt werden, ersetzt die Appliance Variablen durch ihre entsprechenden Werte.

    Ersetzen Sie bei KACE_CUSTOM_INVENTORY_ * das Sternchen (*) durch den Namen einer Softwareanwendung einer Regel für benutzerdefinierte Inventarisierung. Wenn die Geräteaktion ausgeführt wird, wird der Name durch den Wert der Regel für benutzerdefinierte Inventarisierung für das Gerät ersetzt. Geben Sie den Namen der Softwareanwendung in Großbuchstaben ein. Zulässig sind folgende Zeichen: [A-Z0-9.-].“

    HINWEIS: Für die meisten Aktionen in der Dropdown-Liste *Aktion* müssen Sie zusätzliche Anwendungen installieren, damit sie ordnungsgemäß funktionieren. Wenn Sie beispielsweise DameWare nutzen möchten, müssen Sie sowohl auf Ihrem Gerät als auch auf dem, auf das Sie zugreifen möchten, TightVNC installieren.

    Diese Funktion wird nur auf Windows-Geräten unterstützt. Auf dem Windows-Gerät, auf dem die Geräteaktion ausgeführt wird, muss der KACE Agent ab Version 9.0 installiert und verbunden sein.

    Wenn Sie das Gerät über den Agenten initiieren, muss die ausführbare Datei für die Aktion hier platziert werden: `%PATH%`. Der Agent ist 32-Bit, also verwenden Sie auf 64-Bit-Windows-Geräten `%windir%/System32` als Alias für das Verzeichnis `%windir%/Wow64`. Wenn Sie ein Programm ausführen müssen, das sich im Verzeichnis `%windir%/System32` auf einem 64-Bit-Windows-System befindet, müssen Sie das virtuelle Verzeichnis `%windir%/SysNative` verwenden. Sie können entweder `%windir%/SysNative` zu Ihrer Umgebungsvariable `%PATH%` hinzufügen oder einen vollqualifizierten Pfad angeben,

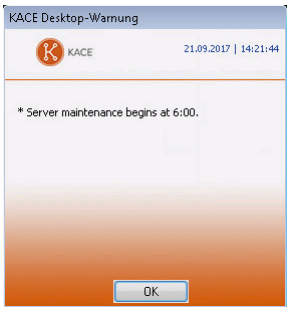
indem Sie bei der Definition Ihrer Geräteaktion `%windir%/SysNative` Ihrer ausführbaren Datei voranstellen.

14. Um eine benutzerdefinierte Administratorkonsole, Benutzerkonsole, Berichte, Warnungslogos und Hintergrundfarben des KACE Agent zu verwenden, geben Sie in den Abschnitten *Login Screen Options (Optionen des Anmeldebildschirms)* die folgenden Informationen an.

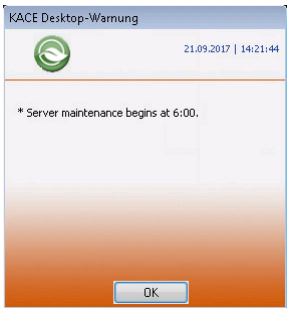
Option	Beschreibung
Admin Console Login Background Color (Hintergrundfarbe für die Anmeldung an der Admin-Konsole) **User Console Login Background Color (Hintergrundfarbe für die Anmeldung an der Benutzerkonsole)**	Sie können von den folgenden Ebenen auf die Appliance zugreifen: • Die **Administratorkonsole** zeigt organisationsbezogene Funktionen an. • **Systemverwaltungskonsole** bietet Zugriff auf Appliance-bezogene Funktionen. • Die **Benutzerkonsole** stellt Anwendungen für Benutzer auf Self-Service-Basis zur Verfügung. Außerdem ermöglicht sie Benutzern das Einsenden von Service Desk Support-Tickets, mit denen sie Hilfe anfordern oder Fehler melden können. Sie können auf die **Benutzerkonsole** unter `http://<appliance_hostname>/user` zugreifen, wobei `<appliance_hostname>` der Hostname der Appliance ist. Wenn Sie eine Organisation in der **Administratorkonsole** auswählen, können Sie eine andere Hintergrundfarbe für die Anmeldebildschirme der **Administratorkonsole** und **Benutzerkonsole** festlegen. Alle auf Organisationsebene angegebenen Farben setzen die Einstellungen auf Systemebene außer Kraft. Informationen zum Konfigurieren der Einstellungen auf Systemebene finden Sie unter Allgemeine Appliance-Einstellungen bei aktivierter Organisationskomponente konfigurieren. Klicken Sie auf die Farbauswahl und legen Sie damit die Farbe fest, die im Hintergrund des Anmeldebildschirms angezeigt werden soll. Sie können die Farbe mit der Maus auswählen oder die RGB-Werte nach Bedarf angeben. Wenn Sie die Farbauswahl schließen, zeigt das Feld *HTML-Farbcode* auf der rechten Seite den HTML-Code der ausgewählten Farbe an. Um die Auswahl rückgängig zu machen, klicken Sie auf **Zurücksetzen** und beginnen Sie von vorne. **HINWEIS:** Die Farbauswahl wird in Internet Explorer 11 nicht unterstützt.
Adminkonsolenlogo **Benutzerkonsolenlogo** **Berichtslogo** **Logo der Agenten-Warnmeldung**	Klicken Sie in jedem entsprechenden Abschnitt auf **Datei auswählen**, und geben Sie die Grafikdatei an, die als benutzerdefiniertes Logo in der **Administratorkonsole**, **Benutzerkonsole**, in systemgenerierten Berichten und in KACE Agent Warnungen verwendet werden soll, die auf verwalteten Geräten angezeigt werden.

Option	Beschreibung
	Die unterstützten Grafikdateiformate sind `.bmp`, `.gif`, `.jpg` und `.png`. Für KACE Agent Warnungen werden nur `.bmp`-Dateien unterstützen. Alle auf Organisationsebene konfigurierten Logos überschreiben die Einstellungen auf Systemebene. Die folgenden Abbildungen zeigen standardmäßige KACE Agent Warnungen und benutzerdefinierte Beispielversionen. Beispiele für Standard- und benutzerdefinierte Logos in der **Administratorkonsole**, **Benutzerkonsole** und in Berichten auf Systemebene finden Sie unter Allgemeine Appliance-Einstellungen bei aktivierter Organisationskomponente konfigurieren.

Standardlogo der Warnmeldung



Benutzerdefiniertes Logo der Warnmeldung



15. Wenn Sie Hewlett-Packard (HP) oder Lenovo Geräte verwalten, können Sie ihre Garantieinformationen abrufen. Geben Sie dazu im Abschnitt *Herstellergarantie-API-Schlüssel* die HP und/oder Lenovo API-Schlüssel an, um die Garantiedaten zu erhalten. Lenovo erfordert nur einen Schlüssel, während HP sowohl einen Schlüssel als auch ein Geheimnis benötigt. Diese Werte werden in der Datenbank verschlüsselt gespeichert.

    WICHTIG: Um Garantieinformationen zu erhalten, müssen Sie die Garantie-API-Schlüssel des Herstellers konfigurieren. Vollständige Anweisungen finden Sie unter https://go.kace.com/to/k1000-help-warranty.

    Wenn diese Option konfiguriert ist, werden die Informationen zur Gerätegarantie auf der Seite *Gerätedetails* in der Gruppe *Inventarinformationen* angezeigt, wenn Sie ein HP oder Lenovo Gerät auswählen. Weitere Informationen hierzu finden Sie unter Elementegruppen und -abschnitte in Gerätedetails.

Option	Beschreibung
Hewlett-Packard	Wählen Sie diese Option, wenn Sie Garantieinformationen für Ihre verwalteten HP Geräte erhalten möchten. Wenn diese Option ausgewählt ist und Sie deaktivieren, werden der HP API-Schlüssel und das Geheimnis aus der Datenbank entfernt.
Schlüssel	Der API-Schlüssel zum Abrufen von Garantieinformationen für verwaltete HP Geräte.
Geheim	Das Geheimnis zum Abrufen von Garantieinformationen für verwaltete HP Geräte.
Lenovo	Wählen Sie diese Option, wenn Sie Garantieinformationen für Ihre verwalteten Lenovo Geräte erhalten möchten. Wenn diese Option ausgewählt ist und Sie deaktivieren, wird der Lenovo Schlüssel aus der Datenbank entfernt.
Schlüssel	Der API-Schlüssel zum Abrufen von Garantieinformationen für verwaltete Lenovo Geräte.

16. Klicken Sie auf **Dienste speichern und neu starten**.

    Die Appliance wird neu gestartet.

Konfigurieren der Datum- und Uhrzeiteinstellungen der Appliance

Konfigurieren Sie die Datums- und Uhrzeiteinstellungen der Appliance im Abschnitt "Einstellungen" der **Administratorkonsole**. Wenn die Organisationskomponente auf Ihrer Appliance aktiviert ist, sind Datum- und Uhrzeiteinstellungen auf Systemebene verfügbar.

Es ist wichtig, die Datum- und Uhrzeiteinstellungen der Appliance exakt einzustellen, da viele Berechnungen auf diesen Einstellungen basieren.

1. Navigieren Sie zur *Systemsteuerung* der Appliance:
   - **Wenn die Organisationskomponente nicht für die Appliance aktiviert ist, melden Sie sich bei der Administratorkonsole an: `https://appliance_hostname/admin`, und wählen Sie dann Einstellungen > Systemsteuerung aus.**
   - **Wenn die Organisationskomponente für die Appliance aktiviert ist, melden Sie sich bei der Systemverwaltungskonsole der Appliance an: `https://appliance_hostname/system`. Oder wählen Sie in der Dropdown-Liste rechts oben auf der Seite den Eintrag System aus, und klicken Sie dann auf Einstellungen > Systemsteuerung.**
2. Klicken Sie auf **Datum- und Uhrzeiteinstellungen**.

   Die Seite *Datum- und Uhrzeiteinstellungen* wird angezeigt.
3. Legen Sie die folgenden Einstellungen fest:

Option	Beschreibung
Zeitzone	Wählen Sie eine Zeitzone aus der Dropdown-Liste aus.

Option	Beschreibung
Uhrzeiteinstellung	Wählen Sie eine Option aus: • **Network Time Protocol (NTP) konfigurieren**. Verwenden Sie einen Internetzeitserver. Wenn Sie diese Option gewählt haben, geben Sie die Web-Adresse des Servers in das Feld *Server* ein. • **Datum und Uhrzeit manuell konfigurieren**. Stellen Sie die Uhrzeit der Appliance manuell ein. Wählen Sie eine Uhrzeit und ein Datum in der Dropdown-Liste aus. Die Dropdown-Liste *Stunde* ist im 24-Stunden-Format.
Server	Verwendet einen Internetzeitserver, um die Uhrzeit der Appliance festzulegen. Geben Sie die Webadresse des Zeitservers in das Textfeld ein. Beispiel: time.example.com.

4. Klicken Sie auf **Speichern und neu starten**.

   Der Webserver wird neu gestartet und die Einstellungen werden übernommen.

   HINWEIS: Aktive Verbindungen können durch den Neustart unterbrochen werden. Beim Speichern der Änderungen wird die Seite automatisch nach 15 Sekunden aktualisiert. Nach dem Neustart des Appliance-Webservers werden das aktualisierte Datum und die aktualisierte Uhrzeit unten rechts in der**Administratorkonsole** angezeigt.

Zweifaktor-Authentifizierung für alle Benutzer aktivieren

Die Zwei-Faktor-Authentifizierung (2FA) bietet mehr Sicherheit für Benutzer, die sich im Gerät anmelden, indem sie einen zusätzlichen Schritt für den Anmeldevorgang hinzufügt. Sie vertraut auf die Google Authenticator-App, um Verifizierungscodes zu generieren. Die App generiert in regelmäßigen Abständen einen neuen sechsstelligen Code. Wenn diese Option aktiviert ist, werden die Endbenutzer bei jeder Anmeldung aufgefordert, den aktuellen Verifizierungscode einzugeben.

Um die Google Authenticator-App herunterzuladen, besuchen Sie eine der folgenden Websites:

- **Android-Geräte**: https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2
- **iOS-Geräte:** https://itunes.apple.com/ca/app/google-authenticator/id388497605?mt=8

Sie können den 2FA-Zugriff auf die **Administratorkonsole** und **Benutzerkonsole** für alle Benutzer in der ausgewählten Organisation auf der Seite *Zweifaktor-Authentifizierung* in der **Administratorkonsole** aktivieren, wie unten beschrieben. Alternativ können Sie den 2FA-Zugriff auf die **Administratorkonsole** und **Benutzerkonsole** über das **Systemverwaltungskonsole** aktivieren oder deaktivieren. Weitere Informationen hierzu finden Sie unter Zweifaktor-Authentifizierung für Organisationen konfigurieren.

1. Rufen Sie die Seite *Zweifaktor-Authentifizierung* auf der Verwaltungsebene auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.

b. Klicken Sie in der linken Navigationsleiste auf **Einstellungen** und anschließend auf **Zweifaktor-Authentifizierung**.

2. Um 2FA für alle Benutzer in der Administratorkonsole zu aktivieren, wählen Sie unter *Zweifaktor-Authentifizierung für Admin-Portal* die Option **Für alle Benutzer erforderlich**.

   Diese Option überschreibt 2FA-Einstellungen auf der Seite *Benutzerdetails*. Wenn 2FA für alle Benutzer auf dieser Seite aktiviert ist, kann sie für Benutzer, die mit der ausgewählten Organisation verknüpft sind (falls zutreffend), auf der Seite *Benutzerdetails* nicht für einzelne Benutzer deaktiviert werden.

3. Um 2FA für alle Benutzer in der Benutzerkonsole zu aktivieren, wählen Sie unter *Zweifaktor-Authentifizierung für Benutzer-Portal* die Option **Für alle Benutzer erforderlich**.

Überprüfen von Port-Einstellungen, NTP-Dienst und Website-Zugriff

Die Porteinstellungen, der NTP-Dienst und der Websitezugriff müssen ordnungsgemäß konfiguriert sein, damit Funktionen wie etwa Agent-Kommunikation, Softwarekatalogaktualisierungen und Patch-Downloads genutzt werden können.

Porteinstellungen überprüfen

Appliance-Ports müssen ordnungsgemäß konfiguriert sein, um die Geräteverwaltung und den Datenbank- oder Dateizugriff zu ermöglichen.

- Stellen Sie sicher, dass die jeweiligen Appliance-Ports nicht durch Firewall-Einstellungen blockiert werden:

Port	Verwendung	Richtung
20 und 21	(Optional und nicht empfohlen) Wird für den Zugriff auf Sicherungsdateien auf der Appliance über FTP von außerhalb der Firewall verwendet.	Eingehend zur Appliance
22	(Empfohlen) Wird zum Erstellen eines SSH-Tunnels an "quest.com" verwendet.	Ausgehend von der Appliance
25	(Optional) Wird vom SMTP-Server der Appliance für E-Mails (Nicht-SSL) verwendet. Wird nur benötigt, falls Sie SMTP-E-Mail konfigurieren. Siehe Konfigurieren von SMTP-E-Mail-Servern.	Ausgehend von der Appliance
80	(Erforderlich. Es sei denn, SSL ist aktiviert.) Wird für den standardmäßigen HTTP-Zugriff (Web) auf die **Administratorkonsole** und **Benutzerkonsole** verwendet.	Eingehend zur Appliance
110	(Optional) Wird für POP3-E-Mail (Nicht-SSL) verwendet	Eingehend zur Appliance

Port	Verwendung	Richtung
161	(Optional) Dient zur SNMP-Überwachung. Siehe Erkennen von Geräten im Netzwerk.	Ausgehend von der Appliance
443	(Erforderlich) Verwendet für SSL-Zugriff und -Kommunikation (Agenten-Messaging-Protokoll). Geräte verwenden diesen Port, wenn sie sich unter Verwendung von HTTPS bei der Appliance anmelden. Die Appliance überwacht diesen Port auf Kommunikation von Geräten, auf denen die KACE Agent-Software installiert ist.	Eingehend zur Appliance
587	(Optional) Wird vom SMTP-Server der Appliance für sichere E-Mail (SSL aktiviert) verwendet. Wird nur benötigt, falls Sie sichere SMTP-E-Mail konfigurieren. Siehe Konfigurieren von SMTP-E-Mail-Servern.	Ausgehend von der Appliance
995	(Optional) Wird für POP3-E-Mail (SSL aktiviert) verwendet.	Eingehend zur Appliance
3306	(Optional) Verwendet für den Zugriff auf die Appliance-Datenbank mithilfe externer Tools. Dieser Port wird beispielsweise verwendet, um mithilfe von Microsoft Access® oder Excel® Berichte für die Appliance-Datenbank zu erstellen.	Eingehend zur Appliance

- Stellen Sie sicher, dass die Appliance auf die jeweiligen Geräte-Ports zugreifen kann:

Port	Verwendung
7	(Optional) Dient der Appliance für UDP-Datenverkehr im Netzwerk, der für Wake on LAN verwendet wird Siehe Verwenden von Wake on LAN.
139	(Optional) Wird während der Provisionierung durch den KACE Agent auf Windows-Geräten verwendet.
161	(Optional) Dient zur SNMP-Überwachung. Dieser Port sollte offen und an SNMP gebunden sein. Siehe Erkennen von Geräten im Netzwerk.

Port	Verwendung
445	(Optional) Verwendet während der Provisionierung durch den KACE Agent. Siehe Provisionierung des KACE Agent.

- Wenn Sie einen LDAP-Server für die Authentifizierung verwenden möchten, stellen Sie sicher, dass die Appliance auf die jeweiligen Ports zugreifen kann:

Port	Verwendung
389	(Optional) Verwendet für den LDAP-Zugriff
636	(Optional) Verwendet für den sicheren LDAP-Zugriff

Status des NTP-Dienstes überprüfen

Um Patches über HTTPS herunterladen zu können, muss der NTP-Dienst (Network Time Protocol) auf der Appliance ausgeführt werden. Der NTP-Dienst ist erforderlich, weil das sichere Protokoll aktuelle Datumsstempel der Appliance verwendet, um die Gültigkeit des Zertifikats sicherzustellen.

Falls der NTP-Service nicht ausgeführt wird, könnte das Herunterladen der Patches fehlschlagen, was ein Hinweis auf ungültige Zertifikate sein könnte.

Erforderliche Websites für die Appliance verfügbar machen

Für Patch-Downloads, den Zugriff auf Produktinformationen und die Interaktion mit **Quest Support** müssen die Einstellungen für Firewall, DNS-Server und Proxy-Server zulassen, dass die Appliance über Port 80 und Port 443 auf Domänen zugreift.

- Stellen Sie sicher, dass die Administratorkonsole der Appliance Links zu den folgenden Websites enthält:

Website	Beschreibung
https://twitter.com/quest	Twitter®
https://www.facebook.com/questsoftware	Facebook®
http://linkedin.com/	LinkedIn®
http://my.kace.com/inKpadsubscriptioncenter	Quest KACE Inkpad
https://www.quest.com/community/b/en/p/endpoint-management	Quest KACE Blog
https://kace.uservoice.com/forums/82699-k1000	Quest KACE Uservoice

Konfigurieren von Netzwerk- und Sicherheitseinstellungen

Zu den Appliance-Netzwerkeinstellungen zählen der Hostname, der Name des Webservers, die IP-Adresse sowie weitere Informationen, die für den Zugriff auf die Appliance über das Netzwerk erforderlich sind.

Netzwerkeinstellungen der Appliance ändern

Im Anschluss an die Erstkonfiguration können Sie die Netzwerkeinstellungen der Appliance jederzeit ändern, um sie an die Anforderungen Ihrer Umgebung anzupassen.

Für die virtuelle und die physische Version der Appliance erfolgt die Erstkonfiguration der Netzwerkeinstellungen während der ersten Anmeldung bei der Administratorkonsole oder Befehlszeilenkonsole. Siehe Netzwerkeinstellungen der Appliance ändern.

Bei K1 als Dienst ist die Appliance mit einer statischen IP-Adresse, einer Subnetzmaske und einem Standard-Gateway vorkonfiguriert. Weitere Informationen zur Konfiguration finden Sie im **KACE SMA als Service Einrichtungshandbuch**. Weitere Informationen finden Sie unter https://support.quest.com/k1000-as-a-service/release-notes-guides.

Um die meisten Netzwerkeinstellungen zu ändern, ist ein Neustart der Appliance erforderlich. Der Neustart dauert insgesamt ein bis zwei Minuten – vorausgesetzt, die Änderungen ergeben eine gültige Konfiguration.

TIPP: Das Testen eines externen SMTP-Servers erfordert keinen Neustart der Appliance. Sie können die SMTP-Konfiguration testen, bevor Sie Ihre Änderungen speichern.

1. Navigieren Sie zur *Systemsteuerung* der Appliance:
   - **Wenn die Organisationskomponente nicht für die Appliance aktiviert ist, melden Sie sich bei der Administratorkonsole an: `https://appliance_hostname/admin`, und wählen Sie dann Einstellungen > Systemsteuerung aus.**
   - **Wenn die Organisationskomponente für die Appliance aktiviert ist, melden Sie sich bei der Systemverwaltungskonsole der Appliance an: `https://appliance_hostname/system`. Oder wählen Sie in der Dropdown-Liste rechts oben auf der Seite den Eintrag System aus, und klicken Sie dann auf Einstellungen > Systemsteuerung.**
2. Klicken Sie auf **Netzwerkeinstellungen**, um die Seite *Netzwerkeinstellungen* anzuzeigen.
3. Geben Sie auf der Seite *Netzwerkeinstellungen* im Abschnitt *Appliance-Netzwerkkonfiguration* die folgenden Informationen an:

Option	Beschreibung
DNS-Hostname	Geben Sie den Hostnamen der Appliance ein. Der Standardname lautet k1000.
Name des Webservers	Geben Sie den vollständigen Domainnamen der Appliance ein. Hierbei handelt es sich um den mit der **Domain** verknüpften **Hostnamen**. Beispiel: k1000.beispiel.com. Geräte stellen über diesen Namen eine Verbindung mit der Appliance her. Quest mpfiehlt, dass Sie dem DNS-Server einen statischen IP-Adresseintrag für die Appliance hinzufügen. Wenn Sie ein SSL-Zertifikat verwenden, muss der Hostname vollständig und gültig sein und demjenigen auf dem Zertifikat entsprechen.

Option	Beschreibung
Servernamen automatisch generieren	Aktivieren Sie dieses Kontrollkästchen, damit das System den Namen des Appliance-Webservers im folgenden Format generiert: `Hostname.Domäne`. Beispiel: `k1000.beispiel.com`. Deaktivieren Sie dieses Kontrollkästchen, wenn Sie einen benutzerdefinierten Webservernamen eingeben möchten.

4. Geben Sie im Bereich *IPv4-Konfiguration* die folgenden Informationen ein:

Option	Beschreibung
Netzwerk mit DHCP konfigurieren	Wählen Sie diese Option, wenn Sie DHCP (Dynamic Host Configuration Protocol) verwenden möchten, um die IPv4-Adresse und andere Informationen zur Netzwerkkonfiguration für die Appliance automatisch zu beziehen.
Netzwerk manuell konfigurieren	Wählen Sie diese Option, wenn Sie IPv4-Adresse, Domäne, Subnetzmaske, Standard-Gateway und DNS-Einstellungen für die Appliance manuell eingeben möchten: • **IP-Adresse**: Geben Sie die statische IP-Adresse der Appliance ein. VORSICHT: **Wenn die IP-Adresse falsch ist, können Sie nicht über die Webbenutzeroberflächen (Administratorkonsole und Benutzerkonsole) auf die Appliance zugreifen. Öffnen Sie in diesem Fall die Befehlszeilenkonsole der Appliance und verwenden Sie die `konfig`-Anmeldung, um die richtige IP-Adresse einzugeben.** • **Domäne**: Geben Sie die Domain ein, in der sich die Appliance befindet. Beispiel: `beispiel.com`. • **Subnetzmaske**: Geben Sie die Subnetzmaske (Netzwerksegment) der Appliance ein. Der Standardwert lautet `255.255.255.0`. • **Standard-Gateway**: Geben Sie das Netzwerk-Gateway für die Appliance ein. • **Primärer DNS-Server**: Geben Sie die IP-Adresse des primären DNS-Servers ein, den die Appliance zur Auflösung von Hostnamen verwendet. • **Sekundärer DNS-Server**: (Optional) Geben Sie die IP-Adresse des sekundären DNS-Servers ein, den die Appliance zur Auflösung von Hostnamen verwendet.

5. Geben Sie im Bereich *IPv6-Konfiguration* die folgenden Informationen ein:

Option	Beschreibung
Netzwerk mit SLAAC konfigurieren	Wählen Sie diese Option aus, wenn Sie SLAAC (Stateless Address Autoconfiguration – zustandslose Adressenautokonfiguration) verwenden möchten, die im Rahmen von IPv6 verfügbar ist, um die Netzwerkeinstellungen der Appliance zu konfigurieren. Mit SLAAC können Geräte ihre eigenen IPv6-Adressen basierend auf dem Präfix auswählen, das von der verbundenen Schnittstelle mitgeteilt wird.
Netzwerk manuell konfigurieren	Wählen Sie diese Option aus, wenn Sie die IPv6-Adresse, die Präfixlänge und das Standard-Gateway für die Appliance manuell angeben möchten: • **IPv6-Adresse**: Geben Sie die statische IP-Adresse der Appliance ein. VORSICHT: **Wenn die IP-Adresse falsch ist, können Sie nicht über die Webbenutzeroberflächen (Administratorkonsole und Benutzerkonsole) auf die Appliance zugreifen. Öffnen Sie in diesem Fall die Befehlszeilenkonsole der Appliance und verwenden Sie die `konfig`-Anmeldung, um die richtige IP-Adresse einzugeben.** • **Präfixlänge**: Geben Sie die Anzahl der Bits in das IPv6-Adressenpräfix ein. Ein IPv6-Präfix besteht üblicherweise aus 64 Bits. • **Standard-Gateway**: Geben Sie das Netzwerk-Gateway für die Appliance ein.
Deaktivieren Sie IPv6.	Wählen Sie diese Option, wenn Sie die IPv6-Adresse für die Appliance deaktivieren möchten. Dies ist die Standardeinstellung.

6. **Optional**: Aktivieren Sie zum Einrichten des Proxy-Servers im Abschnitt *Proxy-Konfiguration* die Option **Proxy-Server aktivieren** und geben Sie die Proxy-Servereinstellungen an:

Option	Beschreibung
Typ	Geben Sie HTTP oder SOCKS5 als Proxy-Typ ein.
Server	Geben Sie den Namen des Proxy-Servers ein.
Port	Geben Sie den Port des Proxy-Servers ein. Der Standardport ist 8080.
Standard-Proxy-Authentifizierung aktivieren	Aktivieren Sie das Kontrollkästchen, um die lokalen Anmeldedaten für den Zugriff auf den Proxy-Server zu verwenden.

Option	Beschreibung
Anmeldung	Geben Sie den Benutzernamen für den Zugriff auf den Proxy-Server ein.
„Kennwort“ und „Kennwort bestätigen“	Geben Sie das Kennwort für den Zugriff auf den Proxy-Server ein.

HINWEIS: Die Appliance unterstützt Proxy-Server mit bereichsbasierter Standardauthentifizierung, für die Benutzernamen und Kennwörter erforderlich sind. Verwendet Ihr Proxy-Server eine andere Authentifizierungsmethode, fügen Sie die IP-Adresse der Appliance zur Ausnahmeliste des Servers hinzu.

7. Um einen externen SMTP-Server zu verwenden, wählen Sie **SMTP-Server aktivieren** im Abschnitt *E-Mail-Konfiguration* und geben dann die SMTP-Server-Optionen an:

Option	Beschreibung
Server	Geben Sie den Hostnamen oder die IP-Adresse eines externen SMTP-Servers an, beispielsweise **smtp.gmail.com**. Externe SMTP-Server müssen die anonyme (nicht authentifizierte) Übermittlung ausgehender E-Mails unterstützen. Vergewissern Sie sich, dass es Ihre Netzwerkrichtlinien der Appliance gestatten, den SMTP-Server direkt zu kontaktieren. Der E-Mail-Server muss zudem für die Weiterleitung von E-Mails von der Appliance ohne Authentifizierung konfiguriert sein. Wenn Sie eine IP-Adresse angeben, setzen Sie sie in eckige Klammern. Beispiel: `[10.10.10.10]`.
Port	Geben Sie die für den externen SMTP-Server zu verwendende Port-Nummer ein. Für Standard-SMTP verwenden Sie Port 25. Für sicheres SMTP verwenden Sie Port 587.
Anmeldung	Geben Sie den Benutzernamen für ein Konto ein, das Zugriff auf den externen SMTP-Server hat, beispielsweise **Ihr_Kontoname**@gmail.com.
„Kennwort“ und „Kennwort bestätigen“	Geben Sie das Kennwort für das angegebene Serverkonto ein.

8. Testen Sie die SMTP-Konfiguration.
   a. Klicken Sie auf **Verbindungstest**.
   b. Geben Sie im nun angezeigten Dialogfeld *Verbindungstest SMTP* die E-Mail-Adresse ein, an die Sie eine Test-E-Mail mit dem neu konfigurierten SMTP-Server senden möchten, und klicken Sie dann auf **Test-E-Mail senden**.

      Das Dialogfeld *Verbindungstest SMTP* wird aktualisiert und zeigt die Testergebnisse der E-Mail-Operation an. Wenn der Test fehlschlägt, überprüfen Sie Ihre Konfiguration und probieren es erneut.
9. Klicken Sie auf **Speichern**.

   Die Appliance wird neu gestartet. Der Neustart dauert insgesamt ein bis zwei Minuten – vorausgesetzt, die Änderungen ergeben eine gültige Konfiguration.
10. Wenn Sie die IP-Adresse der Appliance geändert haben, wechseln Sie zur neuen Adresse, um die Anmeldeseite der Administratorkonsole anzuzeigen.

Lokale Routing-Tabellen konfigurieren

Konfigurieren Sie lokale Routing-Tabellen, damit die Appliance den Datenverkehr über mehrere Gateways in einem Netzwerk leiten kann.

Lokale Routing-Tabellen sind nützlich, wenn sich die physische Appliance und verwaltete Geräte nicht am selben Standort befinden. Falls sich die Appliance beispielsweise in Texas befindet, die verwalteten Geräte jedoch in Kalifornien stehen, versorgt die Appliance Geräte über das Subnetz in Texas. Mit einer lokalen Routing-Tabelle kann die Appliance auf das Netzwerk in Kalifornien verwiesen werden, sodass sie die Geräte in Kalifornien sowie die Geräte in Texas hostet.

1. Navigieren Sie zur *Systemsteuerung* der Appliance:
   - **Wenn die Organisationskomponente nicht für die Appliance aktiviert ist, melden Sie sich bei der Administratorkonsole an: `https://appliance_hostname/admin`, und wählen Sie dann Einstellungen > Systemsteuerung aus.**
   - **Wenn die Organisationskomponente für die Appliance aktiviert ist, melden Sie sich bei der Systemverwaltungskonsole der Appliance an: `https://appliance_hostname/system`. Oder wählen Sie in der Dropdown-Liste rechts oben auf der Seite den Eintrag System aus, und klicken Sie dann auf Einstellungen > Systemsteuerung.**
2. Klicken Sie auf **Lokale Routing-Tabelle**, um die Seite *Einstellungen für lokale Routing-Tabelle* anzuzeigen.
3. Klicken Sie auf die Schaltfläche **Hinzufügen**, um einen Eintrag hinzuzufügen: +.
4. Legen Sie die folgenden Einstellungen fest:

Option	Beschreibung
Name	Geben Sie einen Namen für die Route ein.
Ziel	Geben Sie die IP-Adresse oder das Netzwerk für das Ziel ein, mit dem die Appliance kommunizieren soll.
Subnetzmaske oder CIDR	Geben Sie die Subnetzmaske des festgelegten Netzwerks ein. Beispiel: `24, 255.255.240.0.` Diese wird auf den Host angewendet.
Gateway	Geben Sie die IP-Adresse des Routers ein, der den Datenverkehr zwischen der Appliance und dem Zielnetzwerk weiterleitet.

5. Klicken Sie am Ende der Zeile auf **Speichern**, um den Eintrag zu speichern.
6. Klicken Sie unten auf der Seite auf **Speichern und neu starten**, um alle Änderungen zu speichern.

   Eine Warnung wird mit dem Hinweis angezeigt, dass der Apache™ Dienst neu gestartet werden muss.
7. Klicken Sie auf **OK**, um fortzufahren.

Lokale Webservereinstellungen konfigurieren und Zugriff auf Hosts zulassen

Sie können lokale Webservereinstellungen konfigurieren, um eine Positivliste von Hosts festzulegen, die berechtigt sind, auf die Seiten der **Administratorkonsole**, **Systemverwaltungskonsole**, und **Benutzerkonsole** zuzugreifen. Nachdem Sie eine Positivliste erstellt haben, ist der Zugriff auf die Hosts auf der Positivliste beschränkt.

HINWEIS: Wenn eine IP-Adresse oder ein Domänenname zur *'Allow'-Liste* hinzugefügt wurde, hat nur diese IP-Adresse oder Domäne Zugriff. Alle anderen werden gesperrt.

1. Navigieren Sie zur *Systemsteuerung* der Appliance:
   - **Wenn die Organisationskomponente nicht für die Appliance aktiviert ist, melden Sie sich bei der Administratorkonsole an: `https://appliance_hostname/admin`, und wählen Sie dann Einstellungen > Systemsteuerung aus.**
   - **Wenn die Organisationskomponente für die Appliance aktiviert ist, melden Sie sich bei der Systemverwaltungskonsole der Appliance an: `https://appliance_hostname/system`. Oder wählen Sie in der Dropdown-Liste rechts oben auf der Seite den Eintrag System aus, und klicken Sie dann auf Einstellungen > Systemsteuerung.**
2. Klicken Sie auf **Zugriffssteuerungsliste**, um die Seite *Details zur Zugriffssteuerungsliste* anzuzeigen.
3. Legen Sie die folgenden Optionen fest:

Option	Beschreibung
Keine Zugriffseinschränkungen	Wählen Sie diese Option, um Zugriff von einer beliebigen Webadresse zuzulassen.
Zugriff wie unten angegeben einschränken	Wählen Sie diese Option, um den Zugriff auf Webadressen in der 'Allow'-Liste zu beschränken. Um den Zugriff auf IP-Adressen im Subnetz der Appliance zusätzlich zu den angegebenen Zielen zu aktivieren, wählen Sie **Alle IP-Adressen im gleichen Subnetz wie die Appliance zulassen**.

4. Klicken Sie im Abschnitt *'Allow'-Liste* auf die Schaltfläche **Hinzufügen**, um einen Eintrag hinzuzufügen: +.
5. Legen Sie die folgenden Optionen fest.

Option	Beschreibung
Ziel	Legen Sie das Ziel fest: • **adminui**: Dies ist die Verwaltungsebene der **Administratorkonsole**. Eine Liste mit zulässigen IP-Adressen und/oder Hostnamen, die sich bei `http://`**appliance_hostname**`/admin` anmelden können. • **userui**: Dies ist die **Benutzerkonsole**. Eine Liste mit zulässigen IP-Adressen und/oder Hostnamen, die sich bei `http://`**appliance_hostname**`/user` anmelden können. • **systemui**: Dies ist die **Systemverwaltungskonsole** (nur verfügbar, wenn die Organisationskomponente auf der Appliance aktiviert ist). Eine Liste mit zulässigen IP-Adressen und/oder Hostnamen, die sich bei `http://`**appliance_hostname**`/system` anmelden können. • **api**: Dies ist die Appliance-API. Eine Liste der zulässigen IP-Adressen und/oder Hostnamen, die über ihre API, einschließlich der KACE GO-App, auf die Appliance zugreifen können.

Option	Beschreibung
IP-Adresse/Domänenname	Geben Sie die zulässige Adresse ein. Kann einen der folgenden Werte besitzen: • Domänen- oder untergeordneten Domänennamen (vollständig oder einen Teil) • Eine IP-Adresse (vollständig oder einen Teil)
Subnetzmaske/CIDR	(Optional) Geben Sie eine zulässige Subnetzmaske/CIDR (Classless Inter-Domain Routing) ein. Dies ermöglicht eine genauere Subnetzsteuerung.

6. Klicken Sie am Ende der Zeile auf **Speichern**, um den Eintrag zu speichern.
7. Klicken Sie unten auf der Seite auf **Speichern**, um die Änderungen zu speichern.

   Eine Warnung wird mit dem Hinweis angezeigt, dass der Apache-Dienst neu gestartet werden muss.
8. Klicken Sie auf **OK**, um fortzufahren.

HINWEIS: Wenn eine IP-Adresse oder ein Domänenname zur *'Allow'-Liste* hinzugefügt wurde, kann nur diese IP-Adresse oder Domäne auf die Seite zugreifen. Alle anderen werden gesperrt.

Sicherheitseinstellungen für die Appliance konfigurieren

Sie müssen die Appliance-Sicherheitseinstellungen für die Aktivierung einiger Funktionen wie Samba Freigabe, SSL, SNMP, SSH, Datenbankzugriff und FTP-Zugriff konfigurieren.

Zum Aktivieren von SSL benötigen Sie die richtige Datei für den privaten SSL-Schlüssel sowie ein signiertes SSL-Zertifikat. Wenn Ihr privater Schlüssel über ein Kennwort verfügt, kann kein automatischer Neustart der Appliance ausgeführt werden. Wenn bei Ihnen dieses Problem auftritt, wenden Sie sich an den **Quest Support** unter https://support.quest.com/contact-support.

- Beim Speichern der Sicherheitseinstellungen wird die Appliance neu gestartet.
- Unter Umständen stellt der Firefox®-Browser die **Administratorkonsole**-Anmeldeseite nicht korrekt dar, nachdem Sie den Zugriff auf Port 443 gestattet und die Appliance neu gestartet haben. Löschen Sie in diesem Fall den Firefox Browser-Cache und die Cookies und versuchen Sie es erneut.

1. Navigieren Sie zur *Systemsteuerung* der Appliance:
   - **Wenn die Organisationskomponente nicht für die Appliance aktiviert ist, melden Sie sich bei der Administratorkonsole an: `https://appliance_hostname/admin`, und wählen Sie dann Einstellungen > Systemsteuerung aus.**
   - **Wenn die Organisationskomponente für die Appliance aktiviert ist, melden Sie sich bei der Systemverwaltungskonsole der Appliance an: `https://appliance_hostname/system`. Oder wählen Sie in der Dropdown-Liste rechts oben auf der Seite den Eintrag System aus, und klicken Sie dann auf Einstellungen > Systemsteuerung.**
2. Klicken Sie auf **Sicherheitseinstellungen**, um die Seite *Sicherheitseinstellungen* anzuzeigen.
3. Geben Sie im oberen Abschnitt folgende Einstellungen an:

Option	Beschreibung
Aktivieren von SSH	Gestattet der Appliance SSH-Anmeldungen. Wenn SSH aktiviert ist, wird SSH-verschlüsselte Kommunikation über Port 22 zugelassen.
Webserver-Komprimierung aktivieren	Ermöglicht es der Appliance, Webseiten zu komprimieren. Durch diese Komprimierung

Option	Beschreibung
	werden die Seiten der **Administratorkonsole** und **Benutzerkonsole** im Browser schneller geladen.
SNMP Lesen-Zugriff aktivieren	Unidirektional (schreibgeschützten) SNMP-Zugriff auf verwaltete Geräten im Netzwerk aktivieren.
SNMP-Community-Zeichenfolge	Die SNMP-Communityzeichenfolge, die schreibgeschützten SNMP-Zugriff erlaubt. Der Standardwert ist public.
SNMP-Trap-Überwachung aktivieren	Aktivieren Sie SNMP (Simple Network Management Protocol), ein Protokoll zum Überwachen von verwalteten Geräten in einem Netzwerk. SNMP wird von Dell Open Manage und vielen Produkten von Drittanbietern unterstützt. Falls Sie keine SNMP-Traps von Netzwerkgeräten erhalten möchten, empfiehlt es sich, diese Option zu deaktivieren. Wenn Sie diese Funktion auf dem Gerät aktivieren und die zugehörigen Geräte ebenfalls für die Überwachung aktiviert sind, kann das Gerät SNMP-Traps von den überwachten Netzwerkgeräten wie Drucker, Projektoren und Routern empfangen. Diese Funktion gilt nur für Netzwerkgeräte, die über SNMP-verwaltete Geräte verwaltet werden, wie z. B. agentenlose Geräte mit SNMP-Verbindungen. Informationen zur Aktivierung der Geräteüberwachung finden Sie unter Aktivieren der Überwachung für ein oder mehrere Geräte. SNMP-Traps sind Meldungen, die von Netzwerkgeräte initiiert und an den Trap-Empfänger auf dem Gerät gesendet werden. Zum Beispiel kann ein Router eine Meldung senden, wenn seine Stromversorgung ausfällt. Oder ein Drucker leitet eine Meldung weiter, wenn das Druckerpapier fehlt. Das Gerät erhält diese Traps und generiert Warnungen bei bestimmten Geräten die vordefinierten Grenzwerte erreicht werden. • **SNMP-Version 1 oder 2**: Diese Version erfordert nur eine gültige Communityzeichenfolge. Eine Communityzeichenfolge ist erforderlich ist, damit das Gerät SNMP Trap-Meldungen von überwachten Netzwerkgeräten empfängt. Die Appliance unterstützt mehrere Sicherheitszeichenfolgen. Soll eine Communityzeichenfolge hinzufügt werden, öffnen Sie die Registerkarte **v1/v2**, klicken auf +, geben die Communityzeichenfolge ein und klicken auf **Speichern**. • **SNMP-Version 3**: Diese Version implementiert erweiterte Sicherheit und Funktionen für die Remote-Konfiguration und erfordert einen gültigen Benutzernamen und Verschlüsselungsinformationen. Um einen

Option	Beschreibung
	Sicherheitsnamen hinzuzufügen öffnen Sie die Registerkarte **v3** , klicken auf + und geben folgende Informationen an: ◦ **Sicherheitsname**: Der Account-Name des benutzerbasierten Sicherheitsmodell (USM), das den SNMP-Trap sendet. ◦ **Engine-ID**: Die ID der SNMP-Anwendungs-Engine, die die SNMP-Trap sendet. ◦ **Authentifizierungskennwort**: Das mit dem Sicherheitsnamen verknüpfte Kennwort. ◦ **Authentifizierungsprotokoll**: Das zur Authentifizierung des Benutzers verwendete Protokoll: MD5 oder SHA. ◦ **Datenschutzkennwort**: Der Verschlüsselungsschlüssel für das Datenpaket. ◦ **Datenschutzprotokoll**: Das Verschlüsselungsprotokoll: AES oder DES. ◦ **Sicherheitsstufe**: Zeigt die Sicherheitsstufe an: ▪ **authPriv**: Die Identität des Absenders wird überprüft und die Informationen sind verschlüsselt. ▪ **authNoPriv**: Die Identität des Absenders wird überprüft, aber die Informationen sind nicht verschlüsselt. ▪ **noAuthNoPriv**: Die Identität des Absenders wird nicht überprüft und die Informationen sind nicht verschlüsselt.
MIB-Dateien	Hochladen herstellerspezifische MIB-Dateien (Management Information Base). Eine MIB-Datei ermöglicht dem Trap-Empfänger auf der Appliance SNMP-Traps in lesbare Meldungen zu übersetzen. Diese Dateien sind optional. • Um eine MIB-Datei auf der Seite *Sicherheitseinstellungen* unter *MIB-Dateien* hochzuladen, klicken Sie im Bereich *MIB hochladen* auf **Durchsuchen** und wählen eine MIB-Datei aus. • Eine MIB-Datei muss gewisse Standards erfüllen. Das Gerät überprüft jede MIB-Datei, die Sie hochladen. Wenn Sie eine ungültige MIB-Datei hochladen, wird eine Fehlermeldung oben auf der Seite

Option	Beschreibung
	Sicherheitseinstellungen angezeigt. Wenn Sie den Inhalt der MIB-Datei validieren möchten, aktivieren Sie das Kontrollkästchen **MIB-Validierung überspringen**.
'Sicherungsdateien sichern' aktivieren	Erfordert für den Zugriff auf Appliance-Sicherungsdateien, die durch die Eingabe einer URL in einem Browser verfügbar sind, Authentifizierung durch Benutzername und Kennwort. Deaktivieren Sie diese Option, wenn der Zugriff auf Sicherungsdateien über eine URL ohne Authentifizierung mittels Benutzername und Kennwort ermöglicht werden soll. Dies ist zweckmäßig für externe Prozesse, die den Zugriff benötigen. Siehe Informationen zu Appliance-Sicherungen.
Sicherung über FTP aktivieren	Ermöglicht den Zugriff auf Datenbanksicherungsdateien über einen schreibgeschützten FTP-Server. Auf diese Weise können Sie für den Zugriff auf Sicherungsdateien einen Prozess auf einem anderen Server erstellen. Wenn Sie diesen Zugriff nicht benötigen, deaktivieren Sie diese Option.
Schreibschutz für FTP aufheben	Aktivieren Sie das Hochladen von Sicherungsdateien per FTP. Dies ist zweckmäßig für Sicherungsdateien, die zu groß für die HTTP-Standardmechanismen sind und zu Browser-Timeouts führen.
Neues FTP-Benutzerkennwort	Verlangt ein Kennwort für den FTP-Zugriff auf die Sicherungsdateien.
mDNS aktivieren	Ermöglicht der Appliance die Reaktion auf Multicast Domain Name System(mDNS)- und DNS Service Discovery (DNS-SD)-Anfragen. Diese Option erleichtert Benutzern und Administratoren das Aufrufen der **Administratorkonsole** und **Benutzerkonsole**. Wenn die Appliance nicht auf derartige Anfragen reagieren soll, deaktivieren Sie diese Option.
Zugriff auf Munin aktivieren	Aktivieren Sie die Appliance, um die Servernutzung und die Kennzahlen über einen bestimmten Zeitraum anzuzeigen. **HINWEIS:** Dies ermöglicht uneingeschränkten, nicht authentifizierten Zugriff auf `/munin`.
Datenbankzugriff aktivieren	Ermöglicht Benutzern das Ausführen von Berichten für die Appliance-Datenbank unter Verwendung externer Tools wie Microsoft Access oder Excel über Port 3306. Wenn Sie die Datenbank nicht auf diese

Option	Beschreibung
	Weise zugänglich machen müssen, deaktivieren Sie diese Option. **HINWEIS:** Auf die Appliance-Datenbank kann von jedem ODBC-kompatiblen Drittanbieter-Tool aus zugegriffen werden, wenn Sie den (32-Bit) MySQL ODBC-Treiber installiert haben. Aktivieren Sie dieses Kontrollkästchen, wenn Sie diese Funktion verwenden möchten. Außerdem müssen Sie eine Datenquelle für Ihren MySQL ODBC-Treiber konfigurieren und die Appliance-Verbindungsinformationen angeben. Weitere Informationen finden Sie in der Dokumentation zum MySQL ODBC-Treiber.
Sicheren Datenbankzugriff (SSL) aktivieren	Ermöglicht den SSL-Zugriff auf die Datenbank und den Zugriff auf weitere SSL-Optionen.
Remote-Syslog aktivieren	Aktivieren Sie die Appliance, um begrenzte Serverprotokolldaten an einen Remote-`Syslog`-Server zu senden. **HINWEIS:** Auf diese Weise gesendete Protokolldaten sind unverschlüsselt und verwenden UDP (User Datagram Protocol). Bevor Sie diese Option auswählen, lesen Sie die Richtlinien Ihres Unternehmens zu Sicherheit und Netzwerksättigung.
Remote-Syslog-Server	Geben Sie die den FQDN (Fully Qualified Domain Name) oder die IP-Adresse und die Portnummer des Remote-`Syslog`-Servers an. IPv4- und IPv6-Adressen werden unterstützt. Wenn Sie keine Portnummer angeben, verwendet die Appliance 514 (UDP), die Standardportnummer für `Syslog`-Datenverkehr.

4. Konfigurieren Sie im Abschnitt *Zwei-Faktor-Authentifizierung* die Zwei-Faktor-Authentifizierung (2FA). 2FA bietet mehr Sicherheit für Benutzer, die sich im Gerät anmelden, indem sie einen zusätzlichen Schritt für den Anmeldevorgang hinzufügt. Sie vertraut auf die Google Authenticator-App, um Verifizierungscodes zu generieren. Die App generiert in regelmäßigen Abständen einen neuen sechsstelligen Code. Wenn diese Option aktiviert ist, werden die Endbenutzer bei jeder Anmeldung aufgefordert, den aktuellen Verifizierungscode einzugeben.

   HINWEIS: Wenn Sie diese Funktion aktivieren, stellen Sie sicher, dass die Uhrzeit des Appliance-Servers und diejenige des Geräts, auf dem Google Authenticator ausgeführt wird, korrekt sind. Der Google Authenticator verlässt sich auf die aktuelle Zeit, um das Token zu erstellen. Wenn die Uhr des Servers nicht mit denen der Geräte synchronisiert wird, auf denen Google Authenticator ausgeführt wird, kann die Tokenvalidierung fehlschlagen, was zu Kontosperrungen führen kann.

   a. Legen Sie die folgenden Optionen fest. Sie werden in der Reihenfolge ihrer Priorität aufgeführt, wenn Sie sie von oben nach unten aktivieren. Zum Beispiel können Sie 2FA für

das Benutzerkonsole nur dann aktivieren, wenn Sie zuvor 2FA für den Administratorkonsole konfiguriert haben.

- **Zweistufige Authentifizierung für das Systemportal aktivieren**: Markieren Sie dieses Kontrollkästchen, wenn Sie 2FA für das **Systemverwaltungskonsole** verwenden möchten. Um 2FA für alle Benutzer zu aktivieren, wählen Sie **Für alle Benutzer erforderlich**.

  HINWEIS: Diese Option ist nur für Appliances mit mehreren Organisationen verfügbar.

- **Zweistufige Authentifizierung für das Administratorportal aktivieren**: Diese Option wird nur angezeigt, wenn Sie 2FA für den **Systemverwaltungskonsole** aktiviert haben, oder wenn Ihr Gerät nur eine Organisation hat. Markieren Sie dieses Kontrollkästchen, wenn Sie 2FA für das **Administratorkonsole** verwenden möchten. Als Nächstes geben Sie die Benutzer an, für die bei der Anmeldung eine 2FA-Authentifizierung erforderlich ist. Wählen Sie dazu eine der folgenden Optionen aus:
  - **Für alle Benutzer erforderlich**: **Nur Geräte mit einer einzigen Organisation**. Um 2FA für alle Benutzer zu aktivieren, wählen Sie diese Option.
  - **Definiert nach Organisation**: **Nur Appliances mit mehreren Organisationen**. Wenden Sie nach Bedarf die gleiche 2FA-Konfiguration auf alle Benutzer in jeder Organisation im **Administratorkonsole** an.
  - **Für alle Benutzer erforderlich**: **Nur Appliances mit mehreren Organisationen**. 2FA für alle Benutzer in **Administratorkonsole** aktivieren.
  - **Nicht erforderlich**: **Nur Appliances mit mehreren Organisationen**. 2FA für alle Benutzer in **Administratorkonsole** deaktivieren.
- **Zweistufige Authentifizierung für das Benutzerportal aktivieren**: Diese Option wird nur angezeigt, wenn Sie 2FA für den **Administratorkonsole**aktiviert haben. Markieren Sie dieses Kontrollkästchen, wenn Sie 2FA für das **Benutzerkonsole** verwenden möchten. Als Nächstes geben Sie die Benutzer an, für die bei der Anmeldung eine 2FA-Authentifizierung erforderlich ist. Wählen Sie dazu eine der folgenden Optionen aus:
  - **Definiert nach Organisation**: Wenden Sie nach Bedarf die gleiche 2FA-Konfiguration auf alle Benutzer in jeder Organisation im **Benutzerkonsole** an.
  - **Für alle Benutzer erforderlich**: 2FA für alle Benutzer in **Benutzerkonsole** aktivieren.
  - **Nicht erforderlich**: 2FA für alle Benutzer in **Benutzerkonsole** deaktivieren.

b. Geben Sie unter **Übergangsfenster** den Zeitraum an, in dem Benutzer, die 2FA benötigen, den 2FA-Konfigurationsschritt umgehen können.

Wenn beispielsweise ein Benutzer sein Telefon zu Hause vergisst und daher keinen neuen Code generieren kann, kann er während des hier angegebenen Zeitraums weiterhin auf das Portal zugreifen.

5. Verwenden Sie die Einstellungen im Bereich *Brute Force Prevention (Schutz vor Brute-Force-Angriffen)*, um mehrere aufeinander folgende Angriffe mit falschen Anmeldeinformationen auf die Appliance zu verhindern. Sie können die Anzahl der fehlgeschlagenen Authentifizierungsversuche innerhalb eines bestimmten Zeitraums konfigurieren, nach dem die Appliance jegliche Anmeldungen für diesen Benutzer verhindert.

   Die Standardeinstellung ist drei Versuche während eines Zeitraums von fünf Minuten. Sie können diese Werte nach Bedarf ändern.

   Wenn die Appliance die Anmeldung eines Benutzerkontos deaktiviert, sind andere Benutzer nicht betroffen und können sich unter Angabe gültiger Anmeldeinformationen bei der Appliance anmelden.

6. **Optional**: Klicken Sie im Abschnitt *Appliance-Verschlüsselungsschlüssel* auf **Schlüssel generieren**, um einen neuen Verschlüsselungsschlüssel zu generieren. Mithilfe dieses Schlüssels kann der Quest Support unter Verwendung eines Tethers auf Ihre Appliance zugreifen und Probleme beheben. Ein neuer Schlüssel muss erst erstellt werden, wenn der aktuelle Schlüssel Ihrer Meinung nach manipuliert wurde. Siehe Tether zum Support von Quest KACE aktivieren.

Der Zeitstempel zeigt die Uhrzeit der Schlüsselerstellung.

7. Geben Sie im Abschnitt *Einmaliges Anmelden* Authentifizierungseinstellungen an:

Option	Beschreibung
Deaktiviert	Damit wird verhindert, dass die Appliance die einmalige Anmeldung verwendet. Dank der einmaligen Anmeldung können Benutzer, die sich bei der Domäne angemeldet haben, auf die**Administratorkonsole** und die**Benutzerkonsole** der Appliance zugreifen, ohne die Anmeldeinformationen erneut auf der Anmeldeseite der Appliance eingeben zu müssen.
Active Directory	Verwendet Active Directory für die Authentifizierung. Active Directory authentifiziert Benutzer im Netzwerk mithilfe der Domäne. Siehe Verwenden von Active Directory für die einmalige Anmeldung.

8. Geben Sie im Abschnitt **Samba** folgende Einstellungen an:

Option	Beschreibung
Für Appliances mit aktivierter Organisationskomponente: **Dateifreigaben in Organisation aktivieren** Für Appliances ohne aktivierte Organisationskomponente: **Dateifreigabe aktivieren**	Verwenden Sie die Client-Freigabe der Appliance, um Dateien zu speichern (beispielsweise zur Anwendungsinstallation auf verwalteten Geräten). Die Client-Freigabe der Appliance verfügt über einen integrierten Windows Dateiserver, der vom Bereitstellungsdienst verwendet werden kann, um die Verteilung des Samba Clients in Ihrem Netzwerk zu unterstützen. Quest empfiehlt, diesen Dateiserver nur zu aktivieren, wenn Sie Anwendungsinstallationen auf verwalteten Geräten ausführen. **HINWEIS:** Wenn die Organisationskomponente in Ihrer Appliance aktiviert ist, können Sie weitere Dateifreigabeoptionen für jede Organisation auswählen. Siehe Dateifreigabe auf Systemebene aktivieren.
Samba-Minimalprotokoll,**Samba-Maximalprotokoll**	Wählen Sie nach Bedarf das minimale und maximale Samba-Protokoll aus. Die folgenden Optionen sind in jeder der Einstellungen verfügbar: • **SMB2**: Erneute Implementierung des SMB-Protokolls. Wird von Windows Vista und neueren Versionen von Windows verwendet. SMB2 verfügt über Unterprotokolle.

Option	Beschreibung
	Standardmäßig wird bei SMB2 die Variante SMB2_10 ausgewählt. • **SMB2_02**: Die früheste SMB2-Version. • **SMB2_10**: Windows 7 SMB2. • **SMB2_22**: Frühe Version von Windows 8 SMB2. • **SMB2_24**: Windows 8 Beta SMB2. • **SMB3**: Erneute Implementierung des SMB2-Protokolls. Wird von Windows 8 verwendet. SMB3 verfügt über Unterprotokolle. Standardmäßig verwendet SMB3 die Variante SMB3_11. • **SMB3_00**: Windows 8 SMB3 (ähnlich SMB2_24). • **SMB3_02**: Windows 8,1 SMB3. • **SMB3_10**: Frühe Windows 10 Technical Preview-Version. • **SMB3_11**: Windows 10 Technical Preview-Version.
Anmeldung erforderlich	Aktiviert die Anmeldung für das Samba-Protokoll.
NTLMv2 zur Authentifizierung von Dateifreigaben der Appliance erforderlich	Aktivieren Sie die NTLMv2-Authentifizierung für die Appliance-Dateifreigaben. Wenn diese Option aktiviert ist, müssen verwaltete Geräte, die eine Verbindung mit den Appliance-Dateifreigaben herstellen, NTLMv2 unterstützen und sich bei der Appliance mithilfe von NTLMv2 authentifizieren. Obwohl NTLMv2 sicherer ist als NTLM und LANMAN, sind Konfigurationen ohne NTLMv2 häufiger und diese Option ist in der Regel deaktiviert. Wenn Sie diese Option aktivieren, werden **lanman auth** und **ntlm auth** auf dem Samba Server deaktiviert. NTLMv2 Level 1 – 4 werden unterstützt. Falls Sie NTLM v2 Level 5 benötigen, sollten Sie in Erwägung ziehen, den KACE Agenten manuell bereitzustellen. Siehe Manuelle Bereitstellung des KACE Agent.
NTLMv2 für Offboard-Dateifreigaben erforderlich	Erzwingt, dass einige Funktionen der Appliance, die durch den Samba-Client unterstützt werden (z. B. die Agenten-Provisionierung), mithilfe von NTLMv2 bei den Offboard-Netzwerkdateifreigaben authentifiziert werden müssen. Obwohl NTLMv2 sicherer ist als NTLM und LANMAN, sind Konfigurationen ohne NTLMv2 häufiger und diese Option ist in der Regel deaktiviert. Wenn Sie diese Option aktivieren, wird die Option **client ntlmv2 auth** für Samba Client-Funktionen aktiviert.

9. **Optional**: Geben Sie im Abschnitt *SSL* die SSL-Einstellungen an:

WICHTIG: Die Aktivierung von SSL funktioniert für verwaltete Geräte nur in eine Richtung automatisch. Wenn Sie SSL deaktivieren, müssen die Geräte manuell neu konfiguriert werden.

Option	Beschreibung
Zugriff auf Port 80 aktivieren	Ermöglicht den Zugriff auf die Appliance über Port 80. Wenn Sie den Zugriff auf Port 80 deaktivieren, wenden Sie sich an den **Quest Support**, um die Agenten-Bereitstellungsskripte für den Umgang mit SSL anzupassen.
Aktivieren von SSL	Ermöglicht verwalteten Geräten, sich mithilfe von SSL (HTTPS) mit der Appliance zu verbinden. Aktivieren Sie diese Einstellungen nur, nachdem Sie die Appliance in Ihrem LAN ordnungsgemäß im Nicht-SSL-Modus bereitgestellt haben. Um SSL zu aktivieren, müssen Sie ein SSL-Zertifikat gemäß der Beschreibung in Schritt 10 laden.

10. Führen Sie zum Laden eines SSL-Zertifikats eine der folgenden Aktionen aus:
    - **Klicken Sie auf SSL-Zertifikatformular, um Zertifikatanfragen zu generieren oder selbstsignierte Zertifikate zu laden. Siehe SSL-Zertifikate generieren.**
    - **Wenn Sie über ein SSL-Zertifikat und einen privaten Schlüssel verfügen, klicken Sie in den Feldern** *Datei für privaten SSL-Schlüssel* **oder** *Datei für SSL-Zertifikat* **auf Durchsuchen oder Datei auswählen. Die Dateien müssen ähnlich wie bei von Apache Webservern genutzten Dateien im Format Privacy Enhance Mail (PEM) vorliegen.**
    - **Wählen Sie SSL-Zwischenzertifikat aktivieren aus, um SSL-Zwischenzertifikate zu aktivieren und hochzuladen. Dabei handelt es sich um signierte Zertifikate, die von Zertifikatanbietern als Vollmachten für Stammzertifikate bereitgestellt werden. SSL-Zwischenzertifikate müssen im PEM-Format vorliegen.**
    - **Wenn Ihr Zertifikat im PKCS-12-Format vorliegt, klicken Sie im Feld** *PKCS-12-Datei* **auf Durchsuchen oder Datei auswählen, um es auszuwählen. Geben Sie dann im Feld** *Kennwort für die PKCS-12-Datei* **das Kennwort für die Datei ein.**
11. Wählen Sie im Abschnitt *Sichere Anhänge für Service Desk*, ob Sie die Sicherheitseinstellungen für an Service Desk Tickets angehängte Dateien hinzufügen wollen:
    - Wählen Sie das Kontrollkästchen aus, um die Sicherheitseinstellungen für an Tickets angehängte Dateien zu aktivieren. Wenn Sie diese Option wählen, können Benutzer nur innerhalb der **Administratorkonsole** oder **Benutzerkonsole** der Appliance auf an Tickets angehängte Dateien zugreifen.
    - Deaktivieren Sie das Kontrollkästchen, wenn Benutzer auch außerhalb der **Administratorkonsole** oder **Benutzerkonsole** durch Klicken auf Links auf Ticket-Dateianhänge zugreifen dürfen.
12. Klicken Sie auf **Dienste speichern und neu starten**, um die Änderungen zu übernehmen und die Appliance neu zu starten.

HINWEIS: Unter Umständen stellt der Browser Firefox die **Administratorkonsole**-Anmeldeseite nicht korrekt dar, nachdem Sie den Zugriff auf Port 443 gestattet und die Appliance neu gestartet haben. Löschen Sie in diesem Fall den Firefox Browser-Cache und die Cookies und versuchen Sie es erneut.

Active Directory als Methode für das einmalige Anmelden konfigurieren

Die einmalige Active Directory Anmeldung ermöglicht Benutzern, die sich bei der Domain angemeldet haben, auf die **Administratorkonsole** und die **Benutzerkonsole** der Appliance zuzugreifen, ohne die Anmeldeinformationen bei jeder Anmeldung erneut eingeben zu müssen.

Vergewissern Sie sich vor der Verbindung der Appliance mit einem Active Directory-Server folgender Punkte:

- Netzwerk- und DNS-Einstellungen sind so konfiguriert, dass die Appliance auf den Active Directory-Server zugreifen kann. Siehe Netzwerkeinstellungen der Appliance ändern.
- Die Zeiteinstellungen des Active Directory-Servers stimmen mit den Zeiteinstellungen der Appliance überein. Weitere Informationen zur Einstellung der Zeit auf der Appliance finden Sie unter Konfigurieren der Datum- und Uhrzeiteinstellungen der Appliance.

1. Navigieren Sie zur *Systemsteuerung* der Appliance:
   - **Wenn die Organisationskomponente nicht für die Appliance aktiviert ist, melden Sie sich bei der Administratorkonsole an: `https://appliance_hostname/admin`, und wählen Sie dann Einstellungen > Systemsteuerung aus.**
   - **Wenn die Organisationskomponente für die Appliance aktiviert ist, melden Sie sich bei der Systemverwaltungskonsole der Appliance an: `https://appliance_hostname/system`. Oder wählen Sie in der Dropdown-Liste rechts oben auf der Seite den Eintrag System aus, und klicken Sie dann auf Einstellungen > Systemsteuerung.**
2. Wählen Sie im Abschnitt *Einmalige Anmeldung* der Seite *Sicherheitseinstellungen* die Option **Active Directory** aus und geben Sie die folgenden Informationen an:

Option	Beschreibung
Domain	Der Hostname der Domain Ihres Active Directory® Servers, z.B. beispiel.com.
Benutzername	Der Benutzername des Administratorkontos auf dem Active Directory-Server. Beispiel: benutzername@beispiel.com.
Kennwort	Das Kennwort des Administratorkontos auf dem Active Directory-Server.
Computerobjektcontainer	Der Name des Computerobjektcontainers des Administratorkontos auf dem Active Directory-Server.
Computerobjektname	Der Name des Computerobjektcontainers des Administratorkontos auf dem Active Directory-Server.
Servicekontocontainer	Der Name des Servicekontocontainers des Administratorkontos auf dem Active Directory-Server.

3. Klicken Sie auf **Beitreten**.

Die Appliance führt die folgenden Tests aus (Leseberechtigung erforderlich), um festzustellen, ob die Domäne korrekt für den Beitritt der Appliance konfiguriert ist:

- Prüfung auf unterstützte Betriebssysteme und korrekte Betriebssystem-Patches
- Prüfung auf ausreichenden Speicherplatz zur Installation von QAS
- Prüfung, dass der Hostname des Systems nicht 'localhost' ist
- Prüfung, ob der Namensdienst für die Verwendung von DNS konfiguriert ist
- Prüfung, ob die Namensdiensteinträge in resolv.conf richtig formatiert sind und ob der Host aufgelöst werden kann
- Prüfung auf einen Namensserver, der über die entsprechenden DNS SRV-Datensätze für Active Directory verfügt
- Erkennung eines beschreibbaren Domänencontrollers mit offenem UDP-Port 389
- Erkennung der Active Directory-Site, falls verfügbar
- Prüfung, ob TCP-Port 464 für Kerberos kpasswd geöffnet ist
- Prüfung, ob UDP-Port 88 und TCP-Port 88 für Kerberos-Datenverkehr geöffnet sind
- Prüfung, ob TCP-Port 389 für LDAP geöffnet ist
- Prüfung auf einen globalen Katalogserver und ob TCP-Port 3268 für die Kommunikation mit globalen Katalogservern geöffnet ist
- Prüfung auf einen gültigen Zeitversatz über Active Directory
- Prüfung auf die QAS-Anwendungskonfiguration in Active Directory
- Prüfung, ob TCP-Port 445 für Microsoft CIFS-Datenverkehr geöffnet ist

Diese Tests erfordern keinen Schreibzugriff. Auch für einzelne Verzeichnisse werden keine Schreibberechtigungen benötigt. Zudem werden bei diesen Tests keine Benutzernamen und Kennwörter überprüft. Wenn die Anmeldeinformationen nicht korrekt sind, kann die Appliance selbst bei erfolgreich verlaufenen Tests möglicherweise nicht der Domäne beitreten.

Eine Meldung mit den Ergebnissen des Tests wird angezeigt. Klicken Sie zum Anzeigen von Fehlern auf **Protokolle** und wählen Sie aus der Dropdown-Liste *Protokoll* das Protokoll **Serverfehler** aus.

4. **Optional**: Damit der Server Fehler ignoriert und der Domäne beitritt, wählen Sie **Beitritt erzwingen** aus.
5. Klicken Sie auf **Dienste speichern und neu starten**.

Wenn Benutzer an Geräten angemeldet sind, die zur Active Directory Domain hinzugefügt wurden, können Sie auf die **Benutzerkonsole** der Appliance zugreifen, ohne die Anmeldeinformationen erneut eingeben zu müssen. Wenn Benutzer an Geräten angemeldet sind, die nicht zur Active Directory-Domäne hinzugefügt wurden, wird das Anmeldefenster angezeigt, mit dem sich die Benutzer mit einem lokalen Appliance-Benutzerkonto anmelden können. Siehe Benutzerkonten auf Systemebene hinzufügen oder bearbeiten.

HINWEIS: Zur Verwendung der einmaligen Anmeldung mit den Browsern Microsoft Edge und Firefox müssen die Benutzer ihre Browsereinstellungen für die richtige Authentifizierung konfigurieren. Siehe Browsereinstellungen für die einmalige Anmeldung konfigurieren.

SSL-Zertifikate generieren

Sie können in der **Administratorkonsole** ein selbst signiertes SSL-Zertifikat oder eine Zertifikatsignierungsanforderung für Zertifikate von Drittanbietern erstellen.

1. Navigieren Sie zur *Systemsteuerung* der Appliance:
   - **Wenn die Organisationskomponente nicht für die Appliance aktiviert ist, melden Sie sich bei der Administratorkonsole an: `https://appliance_hostname/admin`, und wählen Sie dann Einstellungen > Systemsteuerung aus.**
   - **Wenn die Organisationskomponente für die Appliance aktiviert ist, melden Sie sich bei der Systemverwaltungskonsole der Appliance an: `https://appliance_hostname/system`. Oder wählen Sie in der Dropdown-Liste rechts oben auf der Seite den Eintrag System aus, und klicken Sie dann auf Einstellungen > Systemsteuerung.**
2. Klicken Sie auf **Sicherheitseinstellungen**, um die Seite *Sicherheitseinstellungen* anzuzeigen.
3. Klicken Sie im Abschnitt *SSL* auf **Aktivieren von SSL**.

   Es werden weitere SSL-Optionen angezeigt.
4. Klicken Sie auf **SSL-Zertifikatformular**, um die Seite *SSL-Zertifikatformular* anzuzeigen.

   HINWEIS: Wurde zuvor eine Signierungsanfrage generiert, wird diese auf der Seite angezeigt. Für eine neue Anfrage müssen Sie die Informationen im Abschnitt *Konfigurieren* aktualisieren und dann auf **Speichern** klicken, bevor Sie auf **Selbstsigniertes Zertifikat erstellen** klicken.
5. Geben Sie im Bereich *Konfigurieren* die folgenden Informationen ein:

Option	Beschreibung
Name der Firma	Der Name Ihres Unternehmens
Name der Organisation	Der Name Ihrer Organisationseinheit oder Unternehmensgruppe
Allgemeiner Name	Der allgemeine Name der Appliance, für die Sie das SSL-Zertifikat erstellen
E-Mail	Ihre E-Mail-Adresse.
Name der Stadt	Der Name Ihres Ortes
Name für Bundesland/Kanton	Der Name Ihres Bundeslands oder Kantons
Ländername	Der Name Ihres Landes

6. Klicken Sie auf **Speichern**.

   Wird das *SSL-Zertifikatformular* damit zum ersten Mal gespeichert, wird der Abschnitt *Zertifikat-Signierungsanfrage* angezeigt. Wurde das Formular zuvor gespeichert, wird der Abschnitt *Zertifikat-Signierungsanfrage* aktualisiert.
7. Führen Sie einen der folgenden Schritte aus:
   - **So erstellen Sie ein Zertifikat mithilfe eines externen Zertifikatanbieters:**
     1. Kopieren Sie den gesamten Text im Abschnitt *Zertifikat-Signierungsanfrage*, einschließlich der Zeilen `"-----BEGIN CERTIFICATE REQUEST-----"` und `"-----END CERTIFICATE REQUEST-----"` sowie des gesamten Texts zwischen diesen Zeilen. Senden Sie diesen Text an den externen Zertifikatanbieter oder die Person, die für Ihre Firma Webserverzertifikate bereitstellt.

2. Wenn Sie ein Zertifikat von dem externen Zertifikatanbieter erhalten haben, kehren Sie zur Seite *Sicherheitseinstellungen* zurück und laden Sie das Zertifikat hoch. Siehe Sicherheitseinstellungen für die Appliance konfigurieren.

- **So generieren Sie ein selbstsigniertes Zertifikat:**

1. Klicken Sie zum Generieren auf **Selbstsigniertes Zertifikat erstellen**. Das Zertifikat können Sie sich im Abschnitt *Zertifikat-Signierungsanfrage* ansehen.
2. Klicken Sie auf **Selbstsigniertes Zertifikat bereitstellen** und dann auf **Ja**.
3. Klicken Sie auf der Seite *Sicherheitseinstellungen* auf **Dienste speichern und neu starten**.

Selbstsignierte Zertifikate werden in **PEM**-Dateien konvertiert und `kbox.pem` genannt. Die Dateien werden in Datenordnern des KACE Agent gespeichert.

HINWEIS: Ihr privater Schlüssel wird im Feld *Privater Schlüssel* angezeigt. Er wird in der Appliance bereitgestellt, sobald Sie ein gültiges Zertifikat bereitgestellt haben. Senden Sie den privaten Schlüssel nicht an eine andere Person. Er wird hier nur angezeigt, damit Sie das Zertifikat ggf. auf einem anderen Webserver bereitstellen können.

HINWEIS: Aus Sicherheitsgründen werden das Zertifikat und der private Schlüssel für SSL nicht wie die anderen Appliance-Daten täglich gesichert. Bewahren Sie diese beiden Dateien gut auf.

Konfigurieren der Agenten-Einstellungen

Agenten-Einstellungen legen die vom KACE Agenten verwendeten Port- und Sicherheitseinstellungen fest. Diese Einstellungen gelten speziell für die Agenten-Infrastruktur und wirken sich nicht auf andere Konfigurationseinstellungen oder Laufzeitvorgänge der Appliance aus.

HINWEIS: Wenn Sie die Agenten-Einstellungen ändern, wird die Kommunikation zwischen der Appliance und den Agenten vorübergehend unterbrochen, gehen Sie daher vorsichtig vor. Weitere Informationen erhalten Sie vom **Quest Support** unter https://support.quest.com/contact-support.

Informationen zu Konea

Konea ist eine Komponente, die die Kommunikation zwischen dem KACE Agenten, der auf vom Agenten verwalteten Geräten installiert ist, und der Appliance ermöglicht.

Konea ermöglicht optimierte Echtzeitkommunikation für Systemverwaltungsvorgänge.

Agenten-Einstellungen konfigurieren

Sie können KACE Agent-Einstellungen auf der Appliance konfigurieren. Es handelt sich dabei um Einstellungen auf Systemebene. Wenn die Organisationskomponente auf der Appliance aktiviert ist, gelten die Agenten-Einstellungen für alle Organisationen.

1. Navigieren Sie zur *Systemsteuerung* der Appliance:
   - **Wenn die Organisationskomponente nicht für die Appliance aktiviert ist, melden Sie sich bei der Administratorkonsole an: `https://appliance_hostname/admin`, und wählen Sie dann Einstellungen > Systemsteuerung aus.**
   - **Wenn die Organisationskomponente für die Appliance aktiviert ist, melden Sie sich bei der Systemverwaltungskonsole der Appliance an: `https://appliance_hostname/system`. Oder wählen Sie in der Dropdown-Liste rechts oben auf der Seite den Eintrag System aus, und klicken Sie dann auf Einstellungen > Systemsteuerung.**
2. Klicken Sie auf **Agenten-Einstellungen**, um die Seite *Agenten-Einstellungen* aufzurufen.
3. Legen Sie die folgenden Einstellungen fest:

Option	Beschreibung
Allow legacy agents (pre-11.0) (Ältere Agenten zulassen (vor Version 11.0))	Diese Option wird nur angezeigt, wenn ein vorhandenes Gerät auf Version 11.0 aktualisiert wurde. Lassen Sie diese Option nur aktiviert, wenn Sie ältere Agenten ohne eine sichere Verbindung weiterhin verwenden möchten, was jedoch die Gesamtsicherheit der Appliance verringert. Quest empfiehlt, alle älteren Agenten auf die neueste Version zu aktualisieren. Wenn Sie diese Option deaktivieren, werden alle Agenten vor Version 11.0 deaktiviert, sodass sie dauerhaft keine Verbindung zur Appliance herstellen können, bis eine sichere Verbindung konfiguriert wurde. Wenn diese Option deaktiviert ist, kann sie nicht mehr aktiviert werden. Weitere Informationen zum Konfigurieren von Agenten für die Verwendung einer sicheren Verbindung finden Sie unter Registrieren des KACE Agent bei der Appliance.

HINWEIS: Die folgenden Einstellungen sind für KACE Agenten Version 11.0 oder höher nicht erforderlich, da die gesamte Kommunikation über den Konea-Tunnel übertragen wird. Weitere Informationen zu Konea finden Sie unter Informationen zu Konea.

SSL für Dateiübertragungen erforderlich	Konfigurieren Sie den KACE Agent für die Verwendung von sicheren Verbindungen. SSL-Verbindungen (Secure Sockets Layer) ermöglichen es dem Agenten, einen verschlüsselten Link zu erstellen, um sicherzustellen, dass alle vom und an den Agenten übergebenen Daten privat und integral bleiben. **WICHTIG: Nach Ändern dieser Einstellung müssen Sie den Agenten manuell mit dem Befehl AMPTools Neustart neu starten, um sicherzustellen, dass diese Änderungen auf dem Client-Computer wiedergespiegelt werden.**
SSL-Zertifikate überprüfen	Überprüfen Sie SSL-Zertifikate vor Aufbau einer Verbindung. Ein SSL-Zertifikat enthält einen öffentlichen Schlüssel, der zur Verschlüsselung verwendet wird und Informationen über seine Eigentümer-ID. **WICHTIG: Nach Ändern dieser Einstellung müssen Sie den Agenten manuell mit dem Befehl AMPTools Neustart neu starten, um sicherzustellen, dass diese Änderungen auf dem Client-Computer wiedergespiegelt werden.**
CA-Zertifikat-Paketdatei	In einigen Umgebungen werden während der Kommunikation zwischen Agent und Server benutzerdefinierte cURL (Client-URL)-CA (Zertifizierungsstelle)-Zertifikate verwendet. Auf diese Weise können SSL-Zertifikate überprüft werden, die von einer Zertifizierungsstelle signiert

Option	Beschreibung
	wurden, auf die im Standard-Agentenpaket nicht verwiesen wird. • Klicken Sie zum Hochladen Ihres benutzerdefinierten cURL-CA-Pakets auf **Datei auswählen**. Die Zertifikatbündeldatei muss im `.PEM`-Format vorliegen. Die Appliance überprüft den Dateiinhalt. Wenn die Datei gültig ist, ersetzt sie das vorhandene oder das Standardbündel (`cacert.pem`), sofern zutreffend. Falls die Datei ungültig ist, wird eine Fehlermeldung angezeigt. • Um zum Standardzertifikat zurückzukehren, klicken Sie auf **Auf Standard zurücksetzen**. **HINWEIS:** Diese Option ist nur nach dem Hochladen eines gültigen benutzerdefinierten CA-Pakets verfügbar.

4. Klicken Sie auf **Dienste speichern und neu starten**, um die Einstellungen zu speichern und den Messaging-Protokoll-Prozessor neu zu starten.

Verwandte Themen

Sicherheitseinstellungen für die Appliance konfigurieren

Fehlerbehebung bei Problemen mit der Appliance

Optional: Konfigurieren Sie die Agenten-Kommunikationseinstellungen, die festlegen, wie häufig Agenten mit der Appliance kommunizieren. Siehe Kommunikation des Agenten verwalten.

Konfigurieren der Einstellungen für Sitzungs-Timeout und automatische Aktualisierung

Das Sitzungs-Timeout ist eine Einstellung auf Systemebene, die den Zeitraum der Inaktivität angibt, nach dem Benutzer automatisch von der **Administratorkonsole** oder **Benutzerkonsole** abgemeldet werden. Einstellungen zur automatischen Aktualisierung betreffen Einstellungen auf Benutzerebene, die festlegen, wie häufig die Seiten der Konsole aktualisiert werden.

Sitzungs-Timeouts festlegen

Sie können Sitzungs-Timeouts entsprechend Ihrer Sicherheitsanforderungen konfigurieren.

1. Navigieren Sie zur *Systemsteuerung* der Appliance:
   - **Wenn die Organisationskomponente nicht für die Appliance aktiviert ist, melden Sie sich bei der Administratorkonsole an: `https://appliance_hostname/admin`, und wählen Sie dann Einstellungen > Systemsteuerung aus.**
   - **Wenn die Organisationskomponente für die Appliance aktiviert ist, melden Sie sich bei der Systemverwaltungskonsole der Appliance an: `https://appliance_hostname/system`. Oder wählen Sie in der Dropdown-Liste rechts oben auf der Seite den Eintrag System aus, und klicken Sie dann auf Einstellungen > Systemsteuerung.**
2. Klicken Sie auf **Allgemeine Einstellungen**, um die Seite *Allgemeine Einstellungen* aufzurufen.
3. Konfigurieren Sie das Sitzungs-Timeout im oberen Abschnitt:

Optionen	Beschreibung
Sitzungs-Timeout	Legen Sie die Zahl der inaktiven Stunden fest, die zugestanden werden, bevor Benutzersitzungen beendet werden und Benutzer sich erneut anmelden müssen. Der Standardwert ist 1. Die **Benutzerkonsole** und die **Administratorkonsole** verfügen über Zähler für den Sitzungs-Timeout, um die Benutzer auf die Frist hinzuweisen. Dabei werden nur Zeiträume ohne Aktivität gezählt. Der Zähler startet neu, sobald der Benutzer eine beliebige Aktion ausführt, die die Konsole zu einer Interaktion mit dem Appliance-Server veranlasst (beispielsweise Aktualisieren eines Fensters, Speichern von Änderungen und Wechseln zwischen Fenstern). Wenn der Zähler den eingestellten Grenzwert erreicht, wird der Benutzer abgemeldet. Nicht gespeicherte Änderungen gehen verloren und die Anmeldeseite wird angezeigt. Der Timeout-Zähler der Sitzung wird in der oberen rechten Ecke jeder Konsole angezeigt.

4. Klicken Sie auf **Dienste speichern und neu starten**.

Automatische Aktualisierung festlegen

Sie können die automatische Aktualisierung so festlegen, dass stets die neuesten Ergebnisse auf Listenseiten angezeigt werden. Sie können die automatische Aktualisierung aber auch deaktivieren, sodass die Seiten nur dann aktualisiert werden, wenn sie im Browser neu geladen werden.

Eine Aktualisierungshäufigkeit von maximal 30 Sekunden ist hilfreich für Seiten mit Statusanzeige, wie etwa die Seite *Provisionierungsergebnisse* und die Seite *Geräte*. Für andere Seiten, wie beispielsweise die Seite *Softwarekatalog*, ist eine längere Aktualisierungshäufigkeit oder eine Deaktivierung der automatischen Aktualisierung möglicherweise sinnvoller, da die Aktualisierung dieser Seiten länger dauert.

Die automatische Aktualisierung betrifft seiten- und benutzerspezifische Einstellungen. Die Einstellungen für Seiten und Benutzerkonten sind jeweils separat.

1. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
2. Gehen Sie zu der Seite, deren Informationen aktualisiert werden sollen, beispielsweise **Inventar > Geräte**.

   Die Seite *Geräte* wird angezeigt.
3. Wählen Sie über der Liste rechts aus der Dropdown-Liste **Automatisch aktualisieren** die Häufigkeit aus.

   Die Liste wird je nach ausgewählter Häufigkeit aktualisiert.
4. Klicken Sie auf die Schaltfläche **Aktualisieren** in der oberen rechten Ecke der Seite, um die Seite sofort zu aktualisieren.
5. **Optional**: Wählen Sie über der Liste rechts aus der Dropdown-Liste **Automatisch aktualisieren** die Option **AUS** aus, um die automatische Aktualisierung zu deaktivieren.

   Die automatische Aktualisierung ist deaktiviert. Die Informationen auf der Seite werden nicht mehr automatisch aktualisiert.

Konfigurieren der Gebietsschema-Einstellungen

Gebietsschema-Einstellungen bestimmen die Sprache, die für Text in der Befehlszeilenkonsole, Administratorkonsole und Benutzerkonsole verwendet wird. Gebietsschema-Einstellungen bestimmen die Formate, die für die Anzeige von Datums- und Zeitinformationen in der **Administratorkonsole** und **Benutzerkonsole** verwendet werden. Alle Texte der Benutzeroberflächen werden unabhängig von den Gebietsschema-Einstellungen in englischer Sprache angezeigt.

Die Gebietsschemaeinstellungen sind durch Ihre Lizenzvereinbarung verfügbar. Siehe Version, Modell und Lizenzinformationen der Appliance anzeigen.

So werden Gebietsschema-Einstellungen angewendet:

Gebietsschema-Einstellungen werden in einer bestimmten Reihenfolge angewendet.

Wenn Sie das Gebietsschema für Text der **Befehlszeilenkonsole**, **Administratorkonsole** und **Benutzerkonsole** auswählen, verwendet die Appliance die folgende Priorität:

1. **Benutzer**: Wenn das Benutzer-Gebietsschema festgelegt ist, wird dieses verwendet.
2. **Organisation**: Wenn das Benutzer-Gebietsschema nicht festgelegt ist, wird die Organisationseinstellung verwendet (diese Option ist nur dann verfügbar, wenn auf der Appliance die Organisationskomponente aktiviert ist).
3. **Browser**: Wenn weder das Benutzer-Gebietsschema noch das Organisations-Gebietsschema festgelegt ist, werden die Browser-Einstellungen verwendet.
4. **System** (**Befehlszeilenkonsole**): Wenn weder das Benutzer-, noch das Organisations-, noch das Browser-Gebietsschema festgelegt ist, werden die System-Einstellungen verwendet.
5. **Standard**: Wenn keine der obigen Optionen festgelegt ist, wird das Standard-Gebietsschema (Englisch) verwendet.

Gebietsschema-Einstellungen für die Administratorkonsole und die Befehlszeilenkonsole konfigurieren

Sie können die Gebietsschema-Einstellungen für die **Administratorkonsole** auf Systemebene konfigurieren. Damit wird auch das Gebietsschema für die **Befehlszeilenkonsole** festgelegt, für die der Zugriff über das Benutzerkonto `konfig` erfolgt.

Durch die Gebietsschema-Einstellungen werden die Formate für die in der Administratorkonsole angezeigten Datums- und Uhrzeitinformationen festgelegt. Alle Texte der Benutzeroberfläche werden unabhängig von den Gebietsschema-Einstellungen in englischer Sprache angezeigt. Durch die Gebietsschema-Einstellungen werden auch die Datums- und Uhrzeitformate festgelegt, die für an den Service Desk gesendete E-Mails verwendet werden.

1. Navigieren Sie zur *Systemsteuerung* der Appliance:
   - **Wenn die Organisationskomponente nicht für die Appliance aktiviert ist, melden Sie sich bei der Administratorkonsole an: `https://appliance_hostname/admin`, und wählen Sie dann Einstellungen > Systemsteuerung aus.**
   - **Wenn die Organisationskomponente für die Appliance aktiviert ist, melden Sie sich bei der Systemverwaltungskonsole der Appliance an: `https://appliance_hostname/system`. Oder**

wählen Sie in der Dropdown-Liste rechts oben auf der Seite den Eintrag System aus, und klicken Sie dann auf Einstellungen > Systemsteuerung.

2. Klicken Sie auf **Allgemeine Einstellungen**, um die Seite *Allgemeine Einstellungen* aufzurufen.
3. Wenn die Organisationskomponente auf Ihrer Appliance aktiviert ist, gehen Sie wie folgt vor:
   a. Wählen Sie ein Gebietsschema in der Dropdown-Liste *Standardgebietsschema* im oberen Abschnitt aus.
   b. Klicken Sie unten auf der Seite auf **Dienste speichern und neu starten**.
4. Wenn die Organisationskomponente auf Ihrer Appliance nicht aktiviert ist, gehen Sie wie folgt vor:
   a. Wählen Sie im Abschnitt *Gebietsschema-Einstellungen* in der Dropdown-Liste *Organisationsgebietsschema* ein Gebietsschema aus.
   b. Wählen Sie im Abschnitt *Gebietsschema-Einstellungen* in der Dropdown-Liste der Befehlszeilenkonsole ein Gebietsschema aus.
   c. Klicken Sie auf **Dienste speichern und neu starten**.

Das ausgewählte Gebietsschema wird für die **Administratorkonsole** und **Befehlszeilenkonsole** verwendet.

Konfigurieren von Gebietsschema-Einstellungen für die Benutzerkonsole

Die Appliance unterstützt mehrere Gebietsschemata. Die **Administratorkonsole**, **Systemverwaltungskonsole** und Online-Hilfe können neben Englisch auf Deutsch, Französisch, Japanisch, Portugiesisch (Brasilien) und Spanisch angezeigt werden.

Zusätzlich zu diesen Sprachen, können Sie die **Benutzerkonsole** bei Bedarf auch in nicht unterstützte Gebietsschemata übersetzen, wie etwa Afrikaans (Südafrika). Wenn Sie die **Benutzerkonsole** in eine nicht unterstützte Sprache übersetzen, erscheint der Inhalt der Hilfe weiterhin auf Englisch. Andere Elemente der Appliance wie etwa die **Administratorkonsole**, **Systemverwaltungskonsole** und die zugehörige Online-Hilfe, werden jedoch in der ausgewählten Sprache angezeigt.

Standardmäßig bestimmt das Gebietsschema des Browsers die Sprache, in der die **Benutzerkonsole** angezeigt wird. Wenn die **Benutzerkonsole** in andere Sprachen übersetzt wird und korrekt konfiguriert ist (wie unten beschrieben), können alle Benutzer, deren Browser dieses Gebietsschema verwenden, die **Benutzerkonsole** in der übersetzten Sprache anzeigen.

1. Navigieren Sie zur *Systemsteuerung* der Appliance:
   - **Wenn die Organisationskomponente nicht für die Appliance aktiviert ist, melden Sie sich bei der Administratorkonsole an: `https://appliance_hostname/admin`, und wählen Sie dann Einstellungen > Systemsteuerung aus.**
   - **Wenn die Organisationskomponente für die Appliance aktiviert ist, melden Sie sich bei der Systemverwaltungskonsole der Appliance an: `https://appliance_hostname/system`. Oder wählen Sie in der Dropdown-Liste rechts oben auf der Seite den Eintrag System aus, und klicken Sie dann auf Einstellungen > Systemsteuerung.**
2. Klicken Sie auf **Lokalisierung**, um die Seite *Lokalisierungseinstellungen der Benutzerkonsole* anzuzeigen.
3. Exportieren Sie die mit dem Gebietsschema, von dem Sie eine Gettext Portable Object (PO)-Datei übersetzen wollen, verknüpften Textfolgen zusammen mit einer Portable Object Template (POT) zur Übersetzung. Weitere Informationen zu Gettext PO-Dateien finden Sie unter https://www.gnu.org/software/gettext/manual/html_node/PO-Files.html.
   a. Klicken Sie auf der Seite *Lokalisierungseinstellungen der Benutzerkonsole* unter *Gettext PO (Portable Object)-Datei exportieren* auf **Gebietsschema exportieren** und wählen Sie das Gebietsschema aus, von dem Sie übersetzen wollen. Die Liste, die daraufhin angezeigt wird, schließt alle unterstützten sowie alle weiteren Sprachen ein, in die Sie die Benutzerkonsole bereits übersetzt hatten.
   b. Klicken Sie auf **Exportieren**.

Wenige Momente später steht eine ZIP-Datei mit dem folgenden Inhalt zum Download bereit:

- Eine PO (Portable Object)-Datei enthält alle Textzeichenfolgen der **Benutzerkonsole**, die in ihrem ausgewählten Gebietsschema existieren.
- Eine POT (Portable Object Template)-Datei enthält eine Vorlagendatei, die zum Generieren der leeren PO-Datei anhand der GetText-Utilities verwendet wird (optional).

4. Übersetzen Sie die Textzeichenfolgen der Benutzerkonsole nach Bedarf, und erstellen Sie eine PO-Datei.
5. Importieren Sie die übersetzten Zeichenfolgen der Benutzerkonsole.

   Sie können einen PO-Dateieditor zum Übersetzen der Textfolgen in der PO-Datei verwenden. Weitere Informationen finden Sie unter:

   - **GNU gettext utilities documentation**: https://www.gnu.org/software/gettext/manual/html_node/index.html
   - **GNU Web Translators Manual**: https://www.gnu.org/software/trans-coord/manual/web-trans/html_node/index.html#SEC_Contents https://www.gnu.org/software/gettext/manual/html_node/PO-Files.html
   - **PO File Format**: https://www.gnu.org/software/trans-coord/manual/web-trans/html_node/PO-Editors.html
   - **Additional information about editing PO (portable object) files with editor suggestions**: https://www.gnu.org/software/trans-coord/manual/web-trans/html_node/PO-Editors.html

     a. Klicken Sie unter *Gettext PO (Portable Object)-Datei importieren* auf **Gebietsschema importieren** und wählen Sie das Gebietsschema aus, das Sie mit der importierten PO-Datei verknüpfen möchten. Dies ist das Gebietsschema, in das die Benutzerkonsole während der Übersetzung der importierten PO-Datei übersetzt wird, wenn das Gebietsschema des Browsers übereinstimmt.
     b. Klicken Sie unter *Übersetzte PO (Portable Object)-Datei* auf **Datei auswählen** und navigieren Sie zur übersetzten PO-Datei.
     c. Klicken Sie auf **Importieren**.
6. Falls Sie irgendwelche zuvor importieren Gebietsschemata löschen wollen, klicken Sie unter *Ein hochgeladenes Gebietsschema löschen* auf *Gebietsschema löschen* und wählen Sie das zu löschende Gebietsschema aus. Klicken Sie auf **Löschen**.

Gebietsschema-Einstellungen für Organisationen konfigurieren

Wenn die Organisationskomponente auf der Appliance aktiviert ist, können Sie für jede Organisation separate Gebietsschema-Einstellungen auswählen.

Durch die Gebietsschema-Einstellungen werden die Formate für die in der Administratorkonsole und Benutzerkonsole angezeigten Datums- und Uhrzeitinformationen festgelegt. Alle Texte der Benutzeroberflächen werden unabhängig von den Gebietsschema-Einstellungen in englischer Sprache angezeigt. Durch die Gebietsschema-Einstellungen werden auch die Datums- und Uhrzeitformate festgelegt, die für an den Service Desk gesendete E-Mails verwendet werden.

1. Rufen Sie die Seite *Allgemeine Einstellungen* auf:

   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Einstellungen** und anschließend auf **Allgemeine Einstellungen**.
2. Wenn die Organisationskomponente auf Ihrer Appliance aktiviert ist, gehen Sie wie folgt vor:

   a. Wählen Sie im Abschnitt *Gebietsschema-Einstellungen* in der Dropdown-Liste *Organisationsgebietsschema* ein Gebietsschema aus.
   b. Klicken Sie unten auf der Seite auf **Dienste speichern und neu starten**.
   c. Wenn Sie mehrere Organisationen haben, wiederholen Sie die oben aufgeführten Schritte für jede Organisation.
3. Wenn die Organisationskomponente auf Ihrer Appliance nicht aktiviert ist, gehen Sie wie folgt vor:
   a. Wählen Sie im Abschnitt *Gebietsschema-Einstellungen* in der Dropdown-Liste *Organisationsgebietsschema* ein Gebietsschema aus.
   b. Wählen Sie im Abschnitt *Gebietsschema-Einstellungen* in der Dropdown-Liste der Befehlszeilenkonsole ein Gebietsschema aus.
   c. Klicken Sie auf **Dienste speichern und neu starten**.

Das ausgewählte Gebietsschema wird übernommen. Benutzer der Organisation, die sich an der **Administratorkonsole** und **Benutzerkonsole** anmelden, sehen die Formate für dieses Gebietsschema, wenn in den Browser-Einstellungen die Anzeige des Gebietsschemas festgelegt ist. Die Gebietsschema-Einstellungen von Benutzern haben jedoch Vorrang vor Gebietsschema-Einstellungen von Organisationen.

Gebietsschema-Einstellungen für Benutzer konfigurieren

Sie können Gebietsschema-Einstellungen für jeden Benutzer konfigurieren. Die Gebietsschema-Einstellungen für Benutzer haben Vorrang vor den Organisationseinstellungen sowie den Gebietsschema-Einstellungen auf Systemebene.

Durch die Gebietsschema-Einstellungen werden die Formate für die in der **Administratorkonsole** und **Benutzerkonsole** angezeigten Datums- und Uhrzeitinformationen festgelegt. Alle Texte der Benutzeroberflächen werden unabhängig von den Gebietsschema-Einstellungen in englischer Sprache angezeigt.

1. Rufen Sie die Seite *Benutzerdetails* auf.
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie auf der linken Navigationsleiste auf **Einstellungen** und anschließend auf **Benutzer**.
   c. Klicken Sie auf den Namen eines Benutzers.
2. Wählen Sie aus der Dropdown-Liste *Gebietsschema* ein Gebietsschema aus.
3. Klicken Sie auf **Speichern**.

Das ausgewählte Gebietsschema wird verwendet, wenn sich der Benutzer bei der **Administratorkonsole** oder **Benutzerkonsole** anmeldet. Voraussetzung dafür ist, dass das Gebietsschema auch in den Browser-Einstellungen festgelegt ist. Diese Gebietsschema-Einstellungen haben Vorrang vor den Gebietsschema-Einstellungen der Organisation des Benutzers.

Konfigurieren des Standard-Designs

Bei einer Standardinstallation wird die Administrationskonsole für jeden neuen Benutzer standardmäßig im Design „Hell“ angezeigt. Zwei weitere Designs sind verfügbar: „Dunkel“ und „Hybrid“. Sie können das Standard-Design für die Appliance ändern. Wenn das Design der Appliance für Ihre Verwendung nicht geeignet ist, können Sie ganz einfach ein anderes Design für Ihr Profil auswählen.

Wenn beispielsweise das Design „Hell“ standardmäßig für die Appliance auf der Systemebene eingestellt ist und Sie das Design „Dunkel“ mit ihrem Benutzerprofil verknüpfen, wird bei jeder Anmeldung das Design „Dunkel“ angewendet.

Ändern des Standard-Designs für die Appliance

In einer Standardinstallation ist das Gerät so konfiguriert, dass das Design „Hell“ verwendet wird. Je nach Bedarf können Sie ein anderes Design als Standardgerätedesign auswählen.

1. Navigieren Sie zur *Systemsteuerung* der Appliance:
   - **Wenn die Organisationskomponente nicht für die Appliance aktiviert ist, melden Sie sich bei der Administratorkonsole an: `https://appliance_hostname/admin`, und wählen Sie dann Einstellungen > Systemsteuerung aus.**
   - **Wenn die Organisationskomponente für die Appliance aktiviert ist, melden Sie sich bei der Systemverwaltungskonsole der Appliance an: `https://appliance_hostname/system`. Oder wählen Sie in der Dropdown-Liste rechts oben auf der Seite den Eintrag System aus, und klicken Sie dann auf Einstellungen > Systemsteuerung.**
2. Klicken Sie auf **Allgemeine Einstellungen**, um die Seite *Allgemeine Einstellungen* aufzurufen.
3. Klicken Sie auf der Seite *Allgemeine Einstellungen*, die angezeigt wird, unter *Designs* auf **Standardmäßiges Appliance-Design** und wählen Sie eine der folgenden Optionen: **Hell**, **Hybrid** oder **Dunkel**.

   Wenn Sie das Design **Hell** oder **Hybrid** als Standard-Design für die Appliance auswählen, wird die Anmeldeseite mit einem weißen Hintergrund angezeigt. Ein dunkler Hintergrund wird verwendet, wenn das Design **Dunkel** als standardmäßiges Design für die Appliance ausgewählt wird. Die Farbe des Anmeldebildschirms spiegelt immer das Design der konfigurierten Appliance wider, nicht das mit Ihrem Benutzerkonto verknüpfte Design. Wenn Sie beispielsweise das Design „Dunkel“ in der **Administratorkonsole** auswählen, wird dieses Design mit Ihrem Benutzerkonto verknüpft und wird bei jeder Anmeldung angewendet. Wenn das Gerät jedoch standardmäßig das Design „Hell“ verwendet, wird Ihr Anmeldebildschirm immer mit einem weißen Hintergrund angezeigt. Nach einer erfolgreichen Anmeldung wird das Design „Dunkel“ angewendet.

   HINWEIS: Berichte werden immer mit einem weißen Hintergrund angezeigt, unabhängig davon, welches Design ausgewählt ist.

   HINWEIS: Für neu erstellte Benutzer verwendet die **Administratorkonsole** das Standard-Design. Dies kann bei der nächsten Anmeldung geändert werden. Weitere Informationen hierzu finden Sie unter Konfigurieren des Standard-Designs für einen Benutzer.

Konfigurieren des Standard-Designs für einen Benutzer

In einer Standardinstallation wird das Design „Hell“ auf jedes Benutzerprofil angewendet. Je nach Bedarf können Sie ein anderes Design für Ihr Benutzerprofil auswählen. Wenn beispielsweise das Design „Hell“ standardmäßig für die Appliance auf der Systemebene eingestellt ist und Sie das Design „Dunkel“ mit ihrem Benutzerprofil verknüpfen, wird bei jeder Anmeldung das Design „Dunkel“ angewendet.

1. Führen Sie einen der folgenden Schritte aus:
   - **Melden Sie sich an der Administratorkonsole der Appliance unter `https://appliance_hostname/admin` an, wobei appliance_hostname der Hostname Ihrer Appliance ist. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die**

Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* **aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.**

- **Melden Sie sich an der Systemverwaltungskonsole der Appliance unter `https://appliance_hostname/system` an, wobei appliance_hostname der Hostname Ihrer Appliance ist. Oder wählen Sie System in der Dropdownliste oben rechts auf der Seite aus.**
- **Melden Sie sich an der Benutzerkonsole der Appliance unter `https://appliance_hostname/user` an, wobei appliance_hostname der Hostname Ihrer Appliance ist. Oder wählen Sie in der Dropdownliste oben rechts auf der Seite Benutzerkonsole aus.**

2. Wählen Sie rechts oben auf der Seite aus der Dropdown-Liste **Mein Profil**.

   Das Dialogfeld *Benutzerprofil* wird angezeigt.

3. Klicken Sie im Dialogfeld *Benutzerprofil* auf der Registerkarte *Profil* auf **Design** und wählen Sie ein Design aus, das Sie mit Ihrem Benutzerkonto verknüpfen möchten: **Hell**, **Dunkel**oder **Hybrid**.

   Das Design, das Sie so auswählen, wird mit Ihrem Benutzerkonto verknüpft und jedes Mal angewendet, wenn Sie sich anmelden. Sie können auch das Standard-Design für die Appliance konfigurieren. Weitere Informationen hierzu finden Sie unter Ändern des Standard-Designs für die Appliance.

Konfigurieren der Datenfreigabeeinstellungen

Konfigurieren Sie Datenfreigabeeinstellungen auf Systemebene. Die Datenfreigabeeinstellungen bestimmen den Umfang der Weitergabe von Informationen Ihrer Appliance an Quest. Darüber hinaus bestimmen die Datenfreigabeeinstellungen, ob Informationen aus ITNinja auf der **Administratorkonsole** angezeigt werden.

Zum Validieren der Produktlizenz sammelt Quest einige lizenzbezogene Informationen wie die MAC-Adresse der Appliance, die Version der Appliance-Software, den Lizenzschlüssel und die Zahl der verwalteten Geräte, unabhängig von den in diesem Abschnitt gewählten Datenfreigabeoptionen.

1. Navigieren Sie zur *Systemsteuerung* der Appliance:
   - **Wenn die Organisationskomponente nicht für die Appliance aktiviert ist, melden Sie sich bei der Administratorkonsole an: `https://appliance_hostname/admin`, und wählen Sie dann Einstellungen > Systemsteuerung aus.**
   - **Wenn die Organisationskomponente für die Appliance aktiviert ist, melden Sie sich bei der Systemverwaltungskonsole der Appliance an: `https://appliance_hostname/system`. Oder wählen Sie in der Dropdown-Liste rechts oben auf der Seite den Eintrag System aus, und klicken Sie dann auf Einstellungen > Systemsteuerung.**
2. Klicken Sie auf **Allgemeine Einstellungen**, um die Seite *Allgemeine Einstellungen* aufzurufen.
3. Wählen Sie im Abschnitt *An Quest weitergeben* Optionen:

Option	Beschreibung
Zusammenfassung von Nutzungsdaten weitergeben ...	(Empfohlen) Geben Sie Übersichtsinformationen an Quest weiter. Zu diesen Informationen zählen der Betriebszustand der Appliance, die Betriebszeit und der Lastdurchschnitt sowie die Zahl der Geräte, verwalteten Installationen und Anwendungen, die von der Appliance verwaltet werden. Diese Option wird empfohlen, da sie dem **Quest Support** zusätzliche Informationen liefert, falls Sie Unterstützung benötigen. Quest verwendet die weitergegebenen Daten außerdem zur Planung von Produktverbesserungen.
Detaillierte Nutzungsdaten und Absturzberichte weitergeben ...	(Empfohlen) Geben Sie detaillierte Informationen an Quest und anonyme Informationen an ITNinja.com weiter. Zu diesen Informationen zählen

Option	Beschreibung
	Absturzberichte vom Agenten und der Appliance, Statistiken zur Nutzung der Benutzeroberfläche und Inventarinformationen wie beispielsweise Anwendungstitel. Quest nutzt diese Informationen zur Verbesserung des Softwarekatalogs. ITNinja nutzt anonyme Daten zur Ermittlung relevanter Inhalte auf http://www.itninja.com für auf der Appliance **Administratorkonsole** bereitgestellte dynamische Feeds. ITNinja.com ist eine Community-Website, auf der IT-Spezialisten Informationen teilen können und eine Vielzahl von Themen in den Bereichen Systemverwaltung und Systembereitstellung finden. Der ITNinja-Feed ist eine Funktion, über die Tipps zur Softwarebereitstellung und andere kontextbezogene Informationen auf den jeweiligen Seiten in der **Administratorkonsole** der Appliance dynamisch angezeigt werden. Zum Aktivieren des ITNinja-Feeds müssen Sie **Detaillierte Nutzungsdaten weitergeben ...** auswählen. Durch diese Einstellung werden Informationen anonym an ITNinja weitergegeben. Der ITNinja-Feed ist nur verfügbar, wenn **Zusammenfassung von Nutzungsdaten weitergeben ...** ausgewählt ist. Darüber hinaus ist er nur auf Seiten mit Bezug zu Software und Bereitstellung verfügbar, beispielsweise auf den Detailseiten zu Software, verwalteter Installation oder Dateisynchronisierung. Der Feed ist nicht auf der Detailseite des *Softwarekatalogs* verfügbar. Deaktivieren Sie diese Option, um zu verhindern, dass die Appliance Inventardaten an die ITNinja Community weitergibt. Durch das Deaktivieren dieser Option werden allerdings keine Informationen entfernt, die bereits weitergegeben wurden. Weitere Informationen erhalten Sie vom .

4. Klicken Sie auf **Dienste speichern und neu starten**.

Informationen zu den DIACAP-Compliance-Anforderungen

Sie können die Appliance für die Unterstützung von Bestimmungen wie die des DIACAP (Department of Defense Information Assurance Certification and Accreditation Process) konfigurieren.

Zur Einhaltung der DIACAP-Bestimmungen führen Administratoren die folgenden Aufgaben aus:

- Aktivieren der Nutzungsrichtlinie. Siehe Nutzungsrichtlinie aktivieren bzw. deaktivieren.
- Deaktivieren des SSH- und Datenbankzugriffs. Siehe Sicherheitseinstellungen für die Appliance konfigurieren.
- Deaktivieren der Samba-Dateifreigabe. Siehe Sicherheitseinstellungen für die Appliance konfigurieren.

Nutzungsrichtlinie aktivieren bzw. deaktivieren

Legen Sie zur Einhaltung von Richtlinien und Bestimmungen wie die des DIACAP (Department of Defense Information Assurance Certification and Accreditation Process) fest, dass Benutzern eine Nutzungsrichtlinie angezeigt wird, wenn sie auf die **Administratorkonsole**, **Benutzerkonsole** oder **Befehlszeilenkonsole** zugreifen oder sich über SSH oder FTP anmelden.

Die Nutzungsrichtlinie ist eine Einstellung auf Systemebene. Ist die Organisationskomponente auf Ihrer Appliance aktiviert, aktivieren bzw. deaktivieren Sie die Nutzungsrichtlinie auf der Systemebene für alle Organisationen. Sie können die Richtlinie nicht für einzelne Organisationen aktivieren oder deaktivieren.

1. Navigieren Sie zur *Systemsteuerung* der Appliance:
   - **Wenn die Organisationskomponente nicht für die Appliance aktiviert ist, melden Sie sich bei der Administratorkonsole an: `https://appliance_hostname/admin`, und wählen Sie dann Einstellungen > Systemsteuerung aus.**
   - **Wenn die Organisationskomponente für die Appliance aktiviert ist, melden Sie sich bei der Systemverwaltungskonsole der Appliance an: `https://appliance_hostname/system`. Oder wählen Sie in der Dropdown-Liste rechts oben auf der Seite den Eintrag System aus, und klicken Sie dann auf Einstellungen > Systemsteuerung.**
2. Klicken Sie auf **Allgemeine Einstellungen**, um die Seite *Allgemeine Einstellungen* aufzurufen.
3. Wählen Sie im Abschnitt *Nutzungsrichtlinie* Richtlinieneinstellungen aus:

Option	Beschreibung
Aktiviert	Aktivieren Sie auf der Appliance die Anzeige Ihrer Richtlinie. Legen Sie fest, dass Benutzer die Bedingungen Ihrer Richtlinie akzeptieren müssen, wenn Sie auf die **Administratorkonsole**, **Benutzerkonsole** oder **Befehlszeilenkonsole** zugreifen oder sich über SSH oder FTP anmelden.
Titel	Die Kopfzeile der Richtlinie, die auf der Anmeldeseite der **Benutzerkonsole** angezeigt werden soll.
Meldung	Details der Richtlinie, die unterhalb des *Titels* auf der Anmeldeseite angezeigt werden. Benutzer müssen den Bedingungen der Richtlinie zustimmen, bevor sie sich bei der **Benutzerkonsole** anmelden können.

4. Klicken Sie auf **Dienste speichern und neu starten**.

   Wenn Benutzer die **Administratorkonsole**, **Benutzerkonsole** oder **Befehlszeilenkonsole** aufrufen oder sich über SSH oder FTP anmelden, müssen sie zuerst der Nutzungsrichtlinie zustimmen, bevor sie sich anmelden können.

   HINWEIS: Ist das einmalige Anmelden aktiviert, wird die Anmeldeseite nicht angezeigt. Benutzer sehen die Nutzungsrichtlinie nicht, bevor sie automatisch angemeldet werden. Siehe Informationen zur einmaligen Anmeldung (SSO).

Konfigurieren des Mobilgerätezugriffs

Der Mobilgerätezugriff ermöglicht die Interaktion mit der Appliance mithilfe der KACE GO App.

KACE GO ist eine App, mit der Administratoren über ihre Smartphones oder Tablets auf Service-Desk-Tickets, Inventarinformationen sowie die Anwendungsbereitstellungsfunktionen zugreifen können. Mit der App können auch Benutzer ohne Administratorberechtigungen auf ihrem Mobilgerät Service-Desk-Tickets senden, den Status von gesendeten Tickets anzeigen und Knowledge Base-Artikel lesen. Sie können K1000 GO für iOS-Geräte aus dem Apple App Store oder für Android-Geräte aus dem Google Play Store herunterladen.

HINWEIS: KACE GO ist nur auf Englisch verfügbar.

Zur Verwendung des Mobilgerätezugriffs müssen Sie diesen für die Appliance und für die Benutzer aktivieren sowie KACE GO herunterladen und auf einem Mobilgerät installieren.

Mobilgerätezugriff für die Appliance aktivieren

Standardmäßig ist der Mobilgerätezugriff deaktiviert. Um Benutzern den Zugriff auf die Appliance mit der KACE GO App zu ermöglichen, müssen Sie zuerst den Mobilgerätezugriff für die Appliance aktivieren.

Der Mobilgerätezugriff wird auf Systemebene aktiviert. Falls die Organisationskomponente in Ihrer Appliance aktiviert ist und Sie den Mobilgerätezugriff aktivieren, wird die Funktion für alle Organisationen aktiviert.

1. Navigieren Sie zur *Systemsteuerung* der Appliance:
   - **Wenn die Organisationskomponente nicht für die Appliance aktiviert ist, melden Sie sich bei der Administratorkonsole an: `https://appliance_hostname/admin`, und wählen Sie dann Einstellungen > Systemsteuerung aus.**
   - **Wenn die Organisationskomponente für die Appliance aktiviert ist, melden Sie sich bei der Systemverwaltungskonsole der Appliance an: `https://appliance_hostname/system`. Oder wählen Sie in der Dropdown-Liste rechts oben auf der Seite den Eintrag System aus, und klicken Sie dann auf Einstellungen > Systemsteuerung.**
2. Klicken Sie auf **Allgemeine Einstellungen**, um die Seite *Allgemeine Einstellungen* aufzurufen.
3. Aktivieren Sie im oberen Abschnitt das Kontrollkästchen *Mobilgerätezugriff aktivieren*.
4. Laden Sie die KACE GO-App herunter.
   a. Klicken Sie auf **Mobile App anfordern**.

      Ein Dialogfeld wird angezeigt, über das Sie KACE GO herunterladen können. Die App ist für iOS- und Android-Plattformen von den jeweiligen App Stores erhältlich.

      TIPP: Sie können auf dieses Dialogfeld auch über das Hilfefenster zugreifen. Weitere Informationen hierzu finden Sie unter Zugreifen auf die Produktdokumentation.

   b. Klicken Sie gegebenenfalls auf den Link für das Betriebssystem Ihres Mobilgeräts, um die App herunterzuladen.

   Weitere Informationen zum Herunterladen und Konfigurieren von KACE GO finden Sie unter KACE GO herunterladen und verwenden.
5. Klicken Sie auf **Dienste speichern und neu starten**.

   Der Mobilgerätezugriff wird für auf der Appliance aktiviert. Bevor Benutzer mithilfe der KACE GO App auf die Appliance zugreifen können, müssen Sie den Mobilgerätezugriff für die entsprechenden Benutzerkonten aktivieren. Siehe Mobilgerätezugriff für Benutzer aktivieren.

   Wenn die Organisationskomponente in Ihrer Appliance aktiviert ist, aktivieren Sie den für Benutzerkonten auf Organisations- oder Verwaltungsebene. Der Mobilgerätezugriff kann für Benutzerkonten nicht auf Systemebene aktiviert bzw. deaktiviert werden.

Mobilgerätezugriff für Benutzer aktivieren

Nachdem Sie den Mobilgerätezugriff für die K1000 aktiviert haben, müssen Sie den Zugriff für Benutzer aktivieren. Wenn die Organisationskomponente auf Ihrer Appliance aktiviert ist, können Sie den Zugriff für Benutzer in jeder Organisation separat aktivieren.

1. Rufen Sie die Seite *Benutzerdetails* auf.
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie auf der linken Navigationsleiste auf **Einstellungen** und anschließend auf **Benutzer**.
   c. Klicken Sie auf den Namen eines Benutzers.
2. Aktivieren Sie das Kontrollkästchen **Mobilgerätezugriff**.

   TIPP: Wenn das Kontrollkästchen für den Mobilgerätezugriff nicht angezeigt wird, überprüfen Sie, ob der Mobilgerätezugriff für die Appliance aktiviert wurde.
3. Klicken Sie auf **Speichern**.
4. So aktivieren Sie den Mobilgerätezugriff für mehrere Benutzer:
   a. Aktivieren Sie die Kontrollkästchen für die Benutzer auf der Seite *Benutzer*.
   b. Wählen Sie **Aktion auswählen** > **Mobilgerätezugriff** > **Aktivieren**.

   Der Mobilgerätezugriff wird aktiviert.

Verwandte Themen

Mobilgerätezugriff für die Appliance aktivieren

Die ausgewählten Benutzer können die KACE GO App aus dem Apple App Store oder aus Google Play herunterladen.

KACE GO herunterladen und verwenden

Sie können KACE GO aus dem Apple App Store für iOS-Geräte oder aus dem Google Play Store für Android-Geräte auf Ihr Smartphone oder Ihren Tablet-PC herunterladen.

1. Rufen Sie auf Ihrem mobilen Gerät den Apple App Store oder Google Play auf und suchen Sie nach **KACEGO**.
2. Laden Sie die App herunter und starten Sie sie.
3. Wenn Sie dazu aufgefordert werden, wählen Sie, ob Sie Push-Benachrichtigungen aktivieren möchten.

   Wenn Sie Push-Benachrichtigungen aktivieren, sendet die App Benachrichtigungen für den Service Desk an das mobile Gerät. Diese Benachrichtigungen beruhen auf der Konfiguration für **E-Mail bei Ereignissen** des Service Desks.
4. Geben Sie die folgenden Informationen an und wählen Sie die Einstellungen für die Erstkonfiguration:

Option	Beschreibung
Appliance-URL	Die IP-Adresse oder der vollständig qualifizierte Domänennamen der Appliance
Benutzername und Kennwort	Der Benutzername und das Kennwort eines Kontos mit aktiviertem Mobilgerätezugriff
Kennwort speichern	Die App speichert Ihr Kennwort auf dem Gerät. Wenn Sie diese Option wählen, erfordert Quest,

Option	Beschreibung
	dass Sie aus Sicherheitsgründen eine PIN (persönliche Identifizierungsnummer) erstellen. KACE GO speichert keine Benutzerdaten, auch nicht im Zwischenspeicher, solange Sie nicht die Option **Kennwort speichern** aktivieren.
SSL verwenden	Ermöglicht SSL-Datenübertragungen zwischen dem Gerät und der Appliance. Um diese Einstellung verwenden zu können, muss SSL auf der Appliance aktiviert sein. Wenn SSL auf der Appliance nicht aktiviert ist und Sie **SSL verwenden** wählen, schlägt die Anmeldung fehl.

Weitere Informationen finden Sie in der Hilfefunktion der KACE GO App und auf https://quest.com/products/kace-systems-management-appliance/.

Verwandte Themen

E-Mail-Auslöser konfigurieren

Sicherheitseinstellungen für die Appliance konfigurieren

Mobilgerätezugriff auf der Appliance deaktivieren

Um alle Benutzer daran zu hindern, über KACE GO auf die Appliance zuzugreifen, können Sie den Mobilgerätezugriff auf der Appliance oder der Systemebene deaktivieren.

1. Navigieren Sie zur *Systemsteuerung* der Appliance:
   - **Wenn die Organisationskomponente nicht für die Appliance aktiviert ist, melden Sie sich bei der Administratorkonsole an: `https://appliance_hostname/admin`, und wählen Sie dann Einstellungen > Systemsteuerung aus.**
   - **Wenn die Organisationskomponente für die Appliance aktiviert ist, melden Sie sich bei der Systemverwaltungskonsole der Appliance an: `https://appliance_hostname/system`. Oder wählen Sie in der Dropdown-Liste rechts oben auf der Seite den Eintrag System aus, und klicken Sie dann auf Einstellungen > Systemsteuerung.**
2. Klicken Sie auf **Allgemeine Einstellungen**, um die Seite *Allgemeine Einstellungen* aufzurufen.
3. Deaktivieren Sie im oberen Abschnitt das Kontrollkästchen *Mobilgerätezugriff aktivieren*.
4. Klicken Sie auf **Dienste speichern und neu starten**.

   Der Zugriff per KACE GO wird für alle Benutzer deaktiviert. Die Verbindung von Benutzern, die momentan mit KACE GO an der Appliance angemeldet sind, wird getrennt.

Die individuellen Benutzereinstellungen werden jedoch beibehalten und erneut gültig, falls die Funktion später wieder in der Appliance aktiviert wird. Wenn der Mobilgerätezugriff beispielsweise für ein Konto aktiviert war und Sie den Mobilgerätezugriff in der Appliance reaktivieren, wird der Mobilgerätezugriff auch für das Konto reaktiviert.

Mobilgerätezugriff für Benutzer deaktivieren

Um bestimmte Benutzer daran zu hindern, über KACE GO auf die Appliance zuzugreifen, können Sie den Mobilgerätezugriff auf Benutzerebene deaktivieren.

1. Rufen Sie die Liste *Benutzer* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen*

aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.

b. Klicken Sie auf der linken Navigationsleiste auf **Einstellungen** und anschließend auf **Benutzer**.

2. Aktivieren Sie die Kontrollkästchen neben einem oder mehreren Benutzern.
3. Wählen Sie **Aktion auswählen** > **Mobilgerätezugriff** > **Deaktivieren**.

Der Mobilgerätezugriff wird für die ausgewählten Benutzer deaktiviert. Wenn die ausgewählten Benutzer momentan über KACE GO mit der Appliance verbunden sind, wird ihre Verbindung getrennt.

Schnellen Wechsel von Organisationen und verknüpften Appliance aktivieren

Das schnelle Wechseln erlaubt die Arbeit mit mehreren Oberflächen, ohne dass Sie sich bei jedem Element extra anmelden müssen. Bei Appliances, bei denen die Organisationskomponente aktiviert ist, sind das die **Administrator- und Systemebene der Administratorkonsole**, der **Benutzerkonsole** und verknüpfte Appliances der K-Serie.

Das schnelle Wechseln ist standardmäßig bei Appliances aktiviert, bei denen die Organisationskomponente nicht aktiviert ist. Auch wird der Link zur **Benutzerkonsole** standardmäßig angezeigt, vorausgesetzt, dass der angemeldete Benutzer die Zugriffsberechtigung auf beides – **Administratorkonsole** und die **Benutzerkonsole** – besitzt.

Damit sie in der Dropdown-Liste für den schnellen Wechsel von Organisationen erscheinen, müssen Organisationen dasselbe Kennwort für das **Administratorkonto** besitzen; nur Organisationen, deren **Administratorkennwörter** übereinstimmen, werden in der Liste angezeigt. Für verknüpfte Appliances gelten ähnliche Anforderungen.

1. Rufen Sie die Seite *Allgemeine Einstellungen* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Einstellungen** und anschließend auf **Allgemeine Einstellungen**.
2. Aktivieren Sie das Kontrollkästchen *Organisationsmenü in Verwaltungskopfzeile anzeigen*.

   HINWEIS: Diese Einstellung ist nur dann verfügbar, wenn in Ihrer Appliance die Organisationskomponente aktiviert ist.
3. **Optional**: Aktivieren Sie das Kontrollkästchen *Organisationsauswahl bei Anmeldung erforderlich*, wenn Benutzer bei der Anmeldung eine Organisation auswählen sollen.

   HINWEIS: Diese Einstellung ist nur dann verfügbar, wenn in Ihrer Appliance die Organisationskomponente aktiviert ist.
4. Klicken Sie auf **Dienste speichern und neu starten**.

   Änderungen werden auf der Anmeldeseite und im oberen Abschnitt der **Administratorkonsole** angezeigt, nachdem Sie sich abgemeldet und erneut angemeldet haben. Die Dropdown Liste zeigt die verfügbaren Optionen.

Verwandte Themen

Verknüpfen von Quest KACE Appliances

Verknüpfen von Quest KACE Appliances

Das Verknüpfen von Appliances ermöglicht die Anmeldung bei einer Quest KACE Appliance und den Zugriff auf alle verknüpften Appliances über die **Administratorkonsole**.

Durch Appliance-Verknüpfung können Sie sich bei einer Appliance anmelden und über die Dropdown-Liste in der rechten oberen Ecke der **Administratorkonsole** auf alle verknüpften Appliances zugreifen, ohne dass Sie sich separat bei jeder Appliance anmelden müssen. Sie können alle Quest KACE Appliances der K Serie verknüpfen, die Sie verwalten.

Das Verknüpfen von Appliances umfasst folgende Schritte:

- Aktivieren Sie den schnellen Wechsel auf jeder Appliance mit aktivierter Organisationskomponente. Siehe Schnellen Wechsel von Organisationen und verknüpften Appliance aktivieren.
- Aktivieren Sie die Verknüpfungserstellung für alle Appliances der K Serie. Siehe Appliance-Verknüpfung aktivieren.

Wenn Sie die Verknüpfung aktivieren, werden für jede Appliance *Namen* und *Schlüssel* erstellt. Anschließend kopieren Sie die *Namen* und *Schlüssel* und fügen sie für jede Appliance auf der Seite *Details zu verknüpfter Appliance* ein.

Sie können auf mehrere Quest KACE Appliances über dieselbe **Administratorkonsole** zugreifen, aber Sie können mithilfe der Verknüpfung keine Ressourcen oder Informationen zwischen diesen übertragen. Siehe Importieren und Exportieren von Appliance-Ressourcen.

HINWEIS: Wenn Sie mehrere Quest KACE Appliances einsetzen und diese miteinander verknüpfen wollen, muss das Kennwort für das **Administratorkonto** auf jeder Appliance identisch sein.

Appliance-Verknüpfung aktivieren

Sie können die Verknüpfung von Appliances auf der Appliance oder in den allgemeinen Einstellungen auf Systemebene aktivieren. Anweisungen zur KACE SDA finden Sie in der Hilfe zur jeweiligen Appliance.

1. Navigieren Sie zur *Systemsteuerung* der Appliance:
   - **Wenn die Organisationskomponente nicht für die Appliance aktiviert ist, melden Sie sich bei der Administratorkonsole an: `https://appliance_hostname/admin`, und wählen Sie dann Einstellungen > Systemsteuerung aus.**
   - **Wenn die Organisationskomponente für die Appliance aktiviert ist, melden Sie sich bei der Systemverwaltungskonsole der Appliance an: `https://appliance_hostname/system`. Oder wählen Sie in der Dropdown-Liste rechts oben auf der Seite den Eintrag System aus, und klicken Sie dann auf Einstellungen > Systemsteuerung.**
2. Klicken Sie auf **Link-Einstellungen**, um die Seite *Aktivierung von verknüpften Appliances* anzuzeigen.
3. Aktivieren Sie das Kontrollkästchen **Appliance-Verknüpfung aktivieren**.
4. Geben Sie die folgenden Informationen an:

Option	Beschreibung
Name	Ein eindeutiger, logischer Name für die Appliance. Dieser Name wird in der Dropdown-Liste in der oberen rechten Ecke der Seite neben den Anmeldeinformationen angezeigt, wenn Appliances verknüpft werden.
Ablauf der Anmeldung	Die Anzahl der Minuten, die die Verknüpfung offen bleiben soll. Wenn diese Zeitspanne abgelaufen ist, müssen Sie beim Wechseln zu einer verknüpften

Option	Beschreibung
	Appliance Anmeldeinformationen eingeben. Der Standardwert lautet 120 Minuten.
Timeout	Die Anzahl der Minuten, die die Appliance auf die Antwort einer Remote-Appliance auf eine Verknüpfungsanforderung wartet. Der Standardwert ist zehn Sekunden.

5. Wählen Sie das Kontrollkästchen **Federation API-Zugriffseinstellungen**.

   HINWEIS: Die Aktivierung dieser Option ermöglicht Ihnen die Federation API-Zugriffseinstellungen für verknüpfte Geräte zu aktivieren. Weitere Informationen hierzu finden Sie unter Den Zugriff auf Federation-API-Einstellungen aktivieren.

6. Klicken Sie auf **Speichern**, um Appliance-Verknüpfungsinformationen anzuzeigen.
7. Kopieren Sie den Text in den Feldern *Name* und *Schlüssel* und fügen Sie ihn an einem zentralen Ort ein, beispielsweise in einer Notepad-Datei.
8. Wiederholen Sie die vorstehenden Schritte für jede Appliance, die Sie verknüpfen möchten.

Wenn die Verknüpfung in allen Appliances aktiviert ist, konfigurieren Sie die Verknüpfungen. Siehe Namen und Schlüssel zu Appliances hinzufügen.

Namen und Schlüssel zu Appliances hinzufügen

Fügen Sie zum Verknüpfen von Quest KACE Appliances die Namen und Schlüssel der Appliance in der **Administratorkonsole** hinzu.

In den folgenden Anweisungen wird das Verknüpfen von KACE SMAs beschrieben. Anweisungen zur KACE SDA finden Sie in der Hilfe zur jeweiligen Appliance.

Bevor Sie Appliances verknüpfen können, müssen Sie die Verknüpfung in jeder Appliance aktivieren und den Namen und Schlüssel aller Appliances an einen zentralen Ort kopieren. Siehe Appliance-Verknüpfung aktivieren.

1. Navigieren Sie zur *Systemsteuerung* der Appliance:
   - **Wenn die Organisationskomponente nicht für die Appliance aktiviert ist, melden Sie sich bei der Administratorkonsole an: `https://appliance_hostname/admin`, und wählen Sie dann Einstellungen > Systemsteuerung aus.**
   - **Wenn die Organisationskomponente für die Appliance aktiviert ist, melden Sie sich bei der Systemverwaltungskonsole der Appliance an: `https://appliance_hostname/system`. Oder wählen Sie in der Dropdown-Liste rechts oben auf der Seite den Eintrag System aus, und klicken Sie dann auf Einstellungen > Systemsteuerung.**
2. Klicken Sie auf **Verknüpfte Appliances**, um die Seite *Verknüpfte Appliances* anzuzeigen.

   HINWEIS: Wenn die Appliance-Verknüpfung nicht aktiviert ist, werden Sie auf die Seite *Aktivierung von verknüpften Appliances* umgeleitet.

3. Wählen Sie **Aktion auswählen** > **Neu**, um die Seite *Details zu verknüpften Appliances* aufzurufen.
4. Fügen Sie im Feld *Hostname* den Namen der Appliance ein, die Sie verknüpfen möchten.

   Dabei handelt es sich um den Namen, den Sie gemäß den Anweisungen unter Appliance-Verknüpfung aktivieren kopiert haben.

5. Wählen Sie **Zugriff auf Port 80 deaktivieren**, um Port 443 für die sichere Kommunikation zu verwenden. Die Kommunikation über Port 80 und Port 443 ist verschlüsselt.
6. Fügen Sie im Feld *Schlüssel* den Schlüssel der zu verknüpfenden Appliance ein.

Dabei handelt es sich um den Schlüssel, den Sie gemäß den Anweisungen unter Appliance-Verknüpfung aktivieren kopiert haben.

7. Klicken Sie auf **Speichern**, um die Schaltfläche *Verbindung testen* anzuzeigen.
8. Klicken Sie auf **Verbindung testen**, um die Verbindung zwischen den beiden verknüpften Appliances zu überprüfen.

   Wenn die Einstellungen korrekt konfiguriert sind, wird die Meldung *Verbindung wurde hergestellt* angezeigt.
9. Melden Sie sich bei der zweiten Appliance an und wiederholen Sie die vorstehenden Schritte, um der zweiten Appliance den *Namen* und den *Schlüssel* der ersten Appliance hinzuzufügen.
10. Klicken Sie auf **Speichern**, um die Schaltfläche **Verbindung testen** anzuzeigen.
11. Klicken Sie auf **Verbindung testen**, um die Verbindung zwischen den beiden verknüpften Appliances zu überprüfen.

    Wenn die Einstellungen korrekt konfiguriert sind, wird die Meldung *Verbindung wurde hergestellt* angezeigt.

Wenn Sie sich erneut bei der Appliance angemeldet haben, werden die anderen verknüpften Appliances in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen angezeigt. Um zu einer Appliance zu wechseln, wählen Sie ihren Namen in der Dropdown-Liste aus.

Den Zugriff auf Federation-API-Einstellungen aktivieren

Wenn Ihre Umgebung Federated KACE SMAs verwendet, ermöglicht es die Seite Federation-API-Einstellungen, den API Zugang für verknüpften Appliances zuzulassen.

Die folgenden Optionen müssen auf der Seite *Aktivierung von verknüpften Appliances* gewählt sein:

- **Appliance-Vernüpfung aktivieren**
- **Federation API-Zugriffseinstellungen**

Weitere Informationen hierzu finden Sie unter Appliance-Verknüpfung aktivieren.

1. Melden Sie sich bei der Administratorkonsole der Appliance an, `http://`**appliance_hostname**`/admin`, und klicken Sie dann auf **Einstellungen**.
2. Klicken sie auf der *Systemsteuerung* der Appliance auf **Federation-API-Einstellungen**, um die Seite *Federation-API-Einstellungen* anzuzeigen.
3. Wählen sie auf der Seite *Federation-API-Einstellungen* das Kontrollkästchen **Zugriff aktivieren**.
4. Im angezeigten Bereich *Remote-Systeme* geben Sie nach Bedarf die Zugriffsebene für jede verknüpfte Appliance an.
   a. In der Zeile des Geräts, dessen Rolle, die Sie konfigurieren möchten, klicken Sie auf die Spalte *Rolle* und wählen eine der folgenden Optionen: **Administrator**, **Administrator mit Lesebrechtigung** oder **Benutzerkonsole**.
   b. Klicken Sie auf **Speichern**.
5. Klicken Sie auf **Speichern**, um Appliance-Verknüpfungsinformationen anzuzeigen.

Appliance-Verknüpfungen deaktivieren

Nachdem Quest KACE Appliances verknüpft wurden, können Sie die Verknüpfung nach Bedarf deaktivieren. Nachdem die Appliance-Verknüpfung deaktiviert wurde, können Sie weiterhin zu anderen Appliances wechseln und diese steuern, bis Sie sich abmelden.

HINWEIS: In diesem Abschnitt wird erläutert, wie Sie Verknüpfungen auf der Appliance deaktivieren können. Anweisungen zur KACE SDA finden Sie in der Hilfe zur jeweiligen Appliance.

1. Navigieren Sie zur *Systemsteuerung* der Appliance:
   - **Wenn die Organisationskomponente nicht für die Appliance aktiviert ist, melden Sie sich bei der Administratorkonsole an: `https://appliance_hostname/admin`, und wählen Sie dann Einstellungen > Systemsteuerung aus.**
   - **Wenn die Organisationskomponente für die Appliance aktiviert ist, melden Sie sich bei der Systemverwaltungskonsole der Appliance an: `https://appliance_hostname/system`. Oder wählen Sie in der Dropdown-Liste rechts oben auf der Seite den Eintrag System aus, und klicken Sie dann auf Einstellungen > Systemsteuerung.**
2. Klicken Sie auf **Link-Einstellungen**, um die Seite *Aktivierung von verknüpften Appliances* anzuzeigen.
3. Deaktivieren Sie das Kontrollkästchen *Appliance-Verknüpfung aktivieren*.
4. Klicken Sie auf **Speichern**.

Konfigurieren der Verlaufseinstellungen

Sie können den Änderungsverlauf für Einstellungen, Assets und Objekte der Appliance konfigurieren (abonnieren) und anzeigen.

Informationen zu den Verlaufseinstellungen

Die Appliance ermöglicht das Konfigurieren (Abonnieren) und Anzeigen des Änderungsverlaufs für Einstellungen, Assets und Objekte.

- **Einstellungen**: Nachverfolgt werden unter anderem allgemeine Einstellungen sowie Einstellungen für ausstehende Geräte, Patch-Abonnements und die Benutzerauthentifizierung. Siehe Verwalten des Einstellungsverlaufs.
- **Assets**: Nachverfolgt werden Geräte, Kostenstellen, Abteilungen, Lizenzen, Standorte, Anwendungen, Hersteller und vom Benutzer erstellte Asset-Typen. Siehe Asset-Verlauf verwalten.
- **Objekte**: Nachverfolgt werden unter anderem Warnungen, Labels, Patch-Zeitpläne, Replikationsfreigaben, Berichte, Skripte und Anwendungen. Siehe Objektverlauf verwalten.

Dieser Verlauf beinhaltet auch das Datum der Änderung, den Benutzer, der zum Zeitpunkt der Änderung angemeldet war, und die Art der Änderung. Diese Informationen können bei der Behebung von Systemverwaltungsproblemen nützlich sein. Sie können im CSV-Format (durch Komma getrennte Werte) oder im benutzerdefinierten Berichtsformat exportiert werden.

Verlaufslisten sind rein informativ. Sie können in Verlaufslisten keine früheren Zustände wiederherstellen oder Änderungen rückgängig machen.

Verwalten des Einstellungsverlaufs

Sie können den Verlauf von Änderungen an Einstellungen konfigurieren (abonnieren) und anzeigen. Die Konfigurationsoptionen können unterschiedlich sein, je nachdem, ob die Organisationskomponente auf Ihrer Appliance aktiviert ist.

- Wenn die Organisationskomponente nicht aktiviert ist: Zeigen Sie alle Verlaufslisten und Konfigurationseinstellungen unter **Einstellungen** > **Verlauf** an. Anleitungen dazu finden Sie unter Einstellungsverlaufsabonnements für Organisationen konfigurieren.
- Wenn die Organisationskomponente aktiviert ist: Zeigen Sie Verlaufslisten und Konfigurationseinstellungen für die einzelnen Organisationen und für die Systemebene separat an. Anleitungen dazu finden Sie unter Einstellungsverlaufsabonnements auf Systemebene mit aktivierter Organisationskomponente konfigurieren.

Einstellungsverlaufsabonnements für Organisationen konfigurieren

Sie können die Einstellungsverlaufabonnements für die Appliance oder, sofern die Organisationskomponente aktiviert ist, für die ausgewählte Organisation konfigurieren.

1. Rufen Sie die Seite *Einstellungsverlaufskonfiguration* auf.
   a. Melden Sie sich bei der Systemadministratorkonsole der Appliance an: `http://`**appliance_hostname**`/system`. Oder wählen Sie in der Dropdown-Liste rechts oben auf der Seite den Eintrag **System** aus.
   b. Klicken Sie auf der linken Navigationsleiste auf **Einstellungen** und anschließend auf **Verlauf**.
   c. Klicken Sie im Abschnitt *Abonnements* auf **Einstellungen**.

   Die Optionen auf dieser Seite unterscheiden sich je nachdem, ob die Organisationskomponente in Ihrer Appliance aktiviert ist. Für Appliances mit aktivierter Organisationskomponente sind auf der Systemebene weitere Optionen verfügbar.
2. Wählen Sie in der Dropdown-Liste für die Aufbewahrung des Verlaufs den Zeitraum aus, für den Änderungen von der Appliance aufbewahrt und in der Verlaufsliste angezeigt werden sollen. Wählen Sie **Unbegrenzt** aus, um alle Änderungen beizubehalten. Wählen Sie **Deaktiviert** aus, um die bestehende Verlaufsliste zu löschen und zu verhindern, dass die Appliance der Liste Änderungen hinzufügt.

   WICHTIG: Wenn Sie den Verlauf über einen sehr langen Zeitraum speichern, beispielsweise mehrere Monate oder *Unbegrenzt***, wird die Elementseite im Bereich** *Inventar* **möglicherweise langsamer geladen.**
3. Aktivieren Sie im Abschnitt *Kategorie- und Feldauswahl* die Kontrollkästchen neben den Einstellungen, die Sie nachverfolgen möchten; deaktivieren Sie die Kontrollkästchen neben den Einstellungen, die Sie nicht nachverfolgen möchten.
4. So wählen Sie Felder innerhalb einer Einstellung aus:
   a. Klicken Sie bei aktiviertem Kontrollkästchen einer Einstellung auf die danebenliegende Schaltfläche **Bearbeiten**: .

      Das Dialogfeld zur Feldauswahl wird angezeigt.
   b. Wählen Sie die Felder aus, deren Verlauf Sie nachverfolgen möchten, und klicken Sie auf **OK**.
5. Klicken Sie auf **Speichern**.
6. **Optional**: Wenn Sie mehrere Organisationen haben, wiederholen Sie die oben aufgeführten Schritte für jede Organisation.

Verwandte Themen

Einstellungsverlaufsabonnements auf Systemebene mit aktivierter Organisationskomponente konfigurieren

Einstellungsverlaufsabonnements auf Systemebene mit aktivierter Organisationskomponente konfigurieren

Wenn die Organisationskomponente auf Ihrer Appliance aktiviert ist, können Sie Einstellungsverlaufsabonnements auf Systemebene konfigurieren.

Informationen zu Verlaufseinstellungen auf Organisationsebene finden Sie unter Verwalten des Einstellungsverlaufs.

1. Rufen Sie die Seite *Einstellungsverlaufskonfiguration* auf.
   a. Melden Sie sich bei der Systemadministratorkonsole der Appliance an: `http://`**appliance_hostname**`/system`. Oder wählen Sie in der Dropdown-Liste rechts oben auf der Seite den Eintrag **System** aus.
   b. Klicken Sie auf der linken Navigationsleiste auf **Einstellungen** und anschließend auf **Verlauf**.

c. Klicken Sie im Fensterbereich *Verlauf* im Abschnitt *Abonnements* auf **Einstellungen**.

2. Aktivieren Sie im Abschnitt *Kategorie- und Feldauswahl* die Kontrollkästchen neben den Einstellungen, die Sie nachverfolgen möchten; deaktivieren Sie die Kontrollkästchen neben den Einstellungen, die Sie nicht nachverfolgen möchten.
3. So wählen Sie Felder innerhalb einer Einstellung aus:
   a. Klicken Sie bei aktiviertem Kontrollkästchen einer Einstellung auf die danebenliegende Schaltfläche **Bearbeiten**: .

      Das Dialogfeld zur Feldauswahl wird angezeigt.

   b. Wählen Sie die Felder aus, deren Verlauf Sie nachverfolgen möchten, und klicken Sie auf **OK**.
4. Klicken Sie auf **Speichern**.

Einstellungsverlauf anzeigen

Wenn Verlaufsabonnements für die Aufbewahrung von Informationen konfiguriert sind, können Sie den Verlauf der an Einstellungen vorgenommenen Änderungen anzeigen.

1. Navigieren Sie zur *Systemsteuerung* der Appliance:
   - **Wenn die Organisationskomponente nicht für die Appliance aktiviert ist, melden Sie sich bei der Administratorkonsole an: `https://appliance_hostname/admin`, und wählen Sie dann Einstellungen > Systemsteuerung aus.**
   - **Wenn die Organisationskomponente für die Appliance aktiviert ist, melden Sie sich bei der Systemverwaltungskonsole der Appliance an: `https://appliance_hostname/system`. Oder wählen Sie in der Dropdown-Liste rechts oben auf der Seite den Eintrag System aus, und klicken Sie dann auf Einstellungen > Systemsteuerung.**
2. Klicken Sie auf *Verlauf*.
3. Klicken Sie im Abschnitt *Berichterstellung* auf **Einstellungen**, um die Seite *Einstellungsverlauf* anzuzeigen.
4. Um die Liste zu filtern, wählen Sie über der Tabelle den Eintrag **Typ** oder **Benutzer** auf der rechten Seite in der Dropdown-Liste *Anzeigen nach* aus.

   Die Liste zeigt nun nur die Elemente an, die dem *Typ* bzw. dem *Benutzer* entsprechen, den Sie ausgewählt haben.

Asset-Verlauf verwalten

Sie können den Änderungsverlauf für Asset-Informationen wie Geräte, Kostenstellen, Abteilungen, Lizenzen, Standorte, Anwendungen, Hersteller und vom Benutzer erstellte Asset-Typen konfigurieren (abonnieren) und anzeigen.

Asset-Verlaufsabonnements konfigurieren

Sie können die Asset-Verlaufsabonnements für die Appliance oder für die ausgewählte Organisation konfigurieren, sofern die Organisationskomponente aktiviert ist.

1. Rufen Sie die Seite *Asset-Verlaufskonfiguration* auf.
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie auf der linken Navigationsleiste auf **Einstellungen** und anschließend auf **Verlauf**.
   c. Klicken Sie im Abschnitt "Abonnements" im *Verlaufsbereich* auf **Assets**.
2. Wählen Sie in der Dropdown-Liste für die Aufbewahrung des Verlaufs den Zeitraum aus, für den Änderungen von der Appliance aufbewahrt und in der Verlaufsliste angezeigt werden sollen. Wählen Sie

Unbegrenzt aus, um alle Änderungen beizubehalten. Wählen Sie **Deaktiviert** aus, um die bestehende Verlaufsliste zu löschen und zu verhindern, dass die Appliance der Liste Änderungen hinzufügt.

> **WICHTIG: Wenn Sie den Verlauf über einen sehr langen Zeitraum speichern, beispielsweise mehrere Monate oder *Unbegrenzt*, wird die Elementseite im Bereich *Inventar* möglicherweise langsamer geladen.**

3. Aktivieren Sie im Abschnitt *Asset-Typ und Feldauswahl* die Kontrollkästchen neben den Asset-Typen, die Sie nachverfolgen möchten. Deaktivieren Sie die Kontrollkästchen neben den Asset-Typen, die Sie nicht nachverfolgen möchten.
4. So wählen Sie Felder innerhalb eines Asset-Typs aus:
   a. Klicken Sie bei aktiviertem Kontrollkästchen eines Asset-Typs auf die Schaltfläche **Bearbeiten** neben dem Asset-Typ: .

      Das Dialogfeld zur Feldauswahl wird angezeigt.

   b. Wählen Sie die Felder aus, deren Verlauf Sie nachverfolgen möchten, und klicken Sie auf **OK**.
5. Klicken Sie auf **Speichern**.
6. **Optional**: Wenn Sie mehrere Organisationen haben, wiederholen Sie die oben aufgeführten Schritte für jede Organisation.

Asset-Verlauf anzeigen

Wenn Verlaufsabonnements für die Aufbewahrung von Informationen konfiguriert sind, können Sie den Verlauf der an Assets vorgenommenen Änderungen anzeigen.

1. Rufen Sie die Liste *Asset-Verlauf* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie auf der linken Navigationsleiste auf **Einstellungen** und anschließend auf **Verlauf**.
   c. Klicken Sie im Abschnitt "Berichterstellung" im *Verlaufsbereich* auf **Assets**.
2. Um die Liste zu filtern, wählen Sie über der Tabelle den Eintrag **Typ** oder **Benutzer** auf der rechten Seite in der Dropdown-Liste *Anzeigen nach* aus.

Die Liste zeigt nun nur die Elemente an, die dem *Typ* bzw. dem *Benutzer* entsprechen, den Sie ausgewählt haben.

Objektverlauf verwalten

Sie können den Änderungsverlauf für Objekte wie Labels, Patch-Zeitpläne, Replikationsfreigaben, Benutzer und andere Objekte konfigurieren (abonnieren) und anzeigen.

Objektverlauf konfigurieren

Sie können die Objektverlaufabonnements für die Appliance oder für die ausgewählte Organisation konfigurieren, sofern die Organisationskomponente aktiviert ist.

1. Rufen Sie die Seite *Objektverlaufskonfiguration* auf.
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie auf der linken Navigationsleiste auf **Einstellungen** und anschließend auf **Verlauf**.

c. Klicken Sie im Fensterbereich *Verlauf* im Abschnitt *Abonnements* auf **Objekte**.

2. Wählen Sie in der Dropdown-Liste für die Aufbewahrung des Verlaufs den Zeitraum aus, für den Änderungen von der Appliance aufbewahrt und in der Verlaufsliste angezeigt werden sollen. Wählen Sie **Unbegrenzt** aus, um alle Änderungen beizubehalten. Wählen Sie **Deaktiviert** aus, um die bestehende Verlaufsliste zu löschen und zu verhindern, dass die Appliance der Liste Änderungen hinzufügt.

   WICHTIG: **Wenn Sie den Verlauf über einen sehr langen Zeitraum speichern, beispielsweise mehrere Monate oder** *Unbegrenzt***, wird die Elementseite im Bereich** *Inventar* **möglicherweise langsamer geladen.**

3. Aktivieren Sie im Abschnitt *Objekttyp und Feldauswahl* die Kontrollkästchen neben den Objekttypen, die Sie nachverfolgen möchten. Deaktivieren Sie die Kontrollkästchen neben den Objekttypen, die Sie nicht nachverfolgen möchten.
4. So wählen Sie Felder innerhalb eines Objekttyps aus:
   a. Klicken Sie bei aktiviertem Kontrollkästchen eines Objekttyps auf die danebenliegende Schaltfläche **Bearbeiten**: .

   Das Dialogfeld zur Feldauswahl wird angezeigt.

   b. Wählen Sie die Felder aus, deren Verlauf Sie nachverfolgen möchten, und klicken Sie auf **OK**.
5. Klicken Sie auf **Speichern**.
6. **Optional**: Wenn Sie mehrere Organisationen haben, wiederholen Sie die oben aufgeführten Schritte für jede Organisation.

Objektverlauf anzeigen

Wenn Verlaufsabonnements für die Aufbewahrung von Informationen konfiguriert sind, können Sie den Verlauf der an Objekten vorgenommenen Änderungen anzeigen.

1. Rufen Sie die Seite *Objekte* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie auf der linken Navigationsleiste auf **Einstellungen** und anschließend auf **Verlauf**.
   c. Klicken Sie im Fensterbereich *Verlauf* im Abschnitt *Berichterstellung* auf **Objekte**.
2. Um die Liste zu filtern, wählen Sie über der Tabelle den Eintrag **Typ** oder **Benutzer** auf der rechten Seite in der Dropdown-Liste *Anzeigen nach* aus.

Die Liste zeigt nun nur die Elemente an, die dem *Typ* bzw. dem *Benutzer* entsprechen, den Sie ausgewählt haben.

Änderungsverlaufsinformationen verwenden

Sie können den Änderungsverlauf eines Elements anzeigen, nach Elementen in Änderungsverlaufslisten suchen, Verlaufsdatensätze löschen, Verlaufsdatensätze exportieren und Berichte aus Verlaufsdatensätzen erstellen.

Änderungsverlauf von Elementen anzeigen

Sie können den Änderungsverlauf eines Elements anzeigen, wenn Sie Details zu dem Element anzeigen.

1. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
2. Rufen Sie die *Details* eines Elements auf. Klicken Sie beispielsweise auf **Skripterstellung** und anschließend auf den Namen eines Skripts.
3. Klicken Sie oben auf der Seite auf den Link **Gesamten Verlauf anzeigen**.

Änderungen werden aufgelistet. Wenn keine Änderungen vorgenommen wurden oder der Änderungsverlauf nicht aktiviert ist, ist die Seite leer.

Nach Elementen in Änderungsverlaufslisten suchen

Sie können nach Elementen in Änderungsverlaufslisten suchen.

1. Rufen Sie die Verlaufsliste für Einstellungen, Assets oder Objekte auf:
   - Einstellungsverlauf anzeigen
   - Asset-Verlauf anzeigen
   - Objektverlauf anzeigen
2. Klicken Sie oberhalb der Liste auf der rechten Seite auf die Registerkarte **Erweiterte Suche**, um den Bereich *Erweiterte Suche* anzuzeigen.
3. Wählen Sie Sucheigenschaften aus und klicken Sie auf **Suchen**.

   Das Suchergebnis wird angezeigt.

Verlaufsdatensätze löschen

Sie können Verlaufsdatensätze aus Verlaufslisten löschen.

1. Rufen Sie die Verlaufsliste für Einstellungen, Assets oder Objekte auf.
   - Einstellungsverlauf anzeigen
   - Asset-Verlauf anzeigen
   - Objektverlauf anzeigen
2. Aktivieren Sie das Kontrollkästchen neben einem oder mehreren Einträgen.
3. Wählen Sie **Aktion auswählen** > **Löschen** und klicken Sie dann zum Bestätigen auf **Ja**.

Verlaufsdatensätze exportieren

Sie können Verlaufsdatensätze im CSV-, Excel- und TSV-Format exportieren.

1. Rufen Sie die Verlaufsliste für Einstellungen, Assets oder Objekte auf.
   - Einstellungsverlauf anzeigen
   - Asset-Verlauf anzeigen
   - Objektverlauf anzeigen
2. **Optional**: Um Elemente eines bestimmten Typs, beispielsweise **Hinzufügen**, zu exportieren, wählen Sie den Elementtyp in der Dropdown-Liste *Anzeigen nach* aus.

   Wenn Sie die Liste nicht filtern, werden alle Elemente exportiert. Durch das Aktivieren des Kontrollkästchens eines Elements wird das Element noch nicht für den Export ausgewählt.
3. Wählen Sie **Aktion auswählen** > **Exportieren** > **Format** aus.

Einrichten und Verwenden von Labels für die Verwaltung von Elementgruppen

Sie können manuelle Labels, Smart Labels, LDAP-Labels und Labelgruppen zum Verwalten von Elementgruppen (beispielsweise Geräte) einrichten.

Informationen zu den Labels

Labels sind Container zum Organisieren und Kategorisieren von Elementen wie etwa Geräten, sodass diese als Gruppe verwaltet werden können.

Beispielsweise können Sie Labels verwenden, um Geräte mit dem gleichen Betriebssystem oder am gleichen geografischen Standort zu kennzeichnen. Sie können dann Aktionen initiieren wie das Verteilen von Software oder das Bereitstellen von Patches auf allen Geräten mit dem Label. Labels können entweder spezifischen Elementen manuell zugewiesen werden oder sie können Elementen durch Zuweisung zu Kriterien wie SQL- oder LDAP-Abfragen automatisch zugewiesen werden. Für die folgenden Elementtypen können Labels zugewiesen werden:

- Inventarelemente wie Geräte, Anwendungen, Prozesse, Startelemente und Services
- Asset-Elemente wie Standorte, Lizenzen und Hersteller
- Erkennungsergebnisse
- Patches
- Dell Aktualisierungspakete
- Benutzer

Manuelle Labels werden manuell zugewiesen und entfernt, während Smart Labels und LDAP-Labels automatisch zugewiesen und entfernt werden. Siehe:

- Informationen zu Smart Labels
- Informationen zu LDAP-Labels

Informationen zu Smart Labels

Smart Labels sind Labels, die auf der Grundlage festgelegter Kriterien automatisch zugewiesen und entfernt werden.

Um beispielsweise Notebooks an einem bestimmten Standort (z. B. dem Büro in San Francisco) zu verfolgen oder zu verwalten, können Sie ein Smart Label namens **Büro San Francisco** erstellen, das auf dem IP-Adressbereich oder dem -Subnetz der Geräte an diesem Standort basiert. Wenn eine Inventarisierung der Geräte durchgeführt wird, wird das Smart Label **San Francisco** automatisch auf Geräte im entsprechenden IP-Adressbereich angewendet. Wenn Geräte den IP-Adressbereich verlassen und daraufhin eine neue Inventarisierung durchgeführt wird, wird das Label automatisch entfernt.

Smart Labels werden auf verwaltete Geräte angewendet bzw. entfernt, wenn die Geräte eine Verbindung mit der Appliance herstellen. Wenn Sie also ein Smart Label erstellen, das die Erfassung der Nutzung auf Geräten ermöglicht, kann es einige Zeit dauern, bis das Smart Label auf die Geräte angewendet wird und die Geräte mit der Meldung von Erfassungsinformationen beginnen. Die Erfassung der Nutzung wird für Geräte, die den

Smart Label-Kriterien entsprechen, erst aktiviert, nachdem die Appliance das Geräteinventar verarbeitet hat und das Smart Label angewendet wurde.

Verwandte Themen

Verwalten von Smart Labels

Informationen zu LDAP-Labels

LDAP-Labels sind Labels, die mit LDAP-Servern interagieren. Diese Labels werden automatisch Geräte- oder Benutzerdatensätzen zugewiesen, die LDAP-Abfragen oder Suchfilter verwenden.

Es gibt zwei Arten von LDAP-Labels:

- **Gerät**: Labels, die Gerätedatensätzen zugewiesen werden. Sie sind hilfreich, falls Sie Geräte automatisch nach Name, Beschreibung oder anderen LDAP-Kriterien gruppieren möchten. Jedes Mal, wenn ein Gerät inventarisiert wird, wird diese Abfrage an den LDAP-Server gesendet. Der *Admin*-Wert im Feld *Suchfilter* wird durch den Namen des Benutzers ersetzt, der an diesem Gerät angemeldet ist. Wenn ein Ergebnis zurückgegeben wird, wird dem Gerät das im Feld *Verknüpfter Labelname* angegebene Label zugewiesen.
- **Benutzer**: Labels, die Benutzerdatensätzen zugewiesen werden. Sie sind hilfreich, falls Sie Benutzer automatisch nach Domäne, Standort, Budgetcode oder anderen LDAP-Kriterien gruppieren möchten. LDAP-Labels werden auf Benutzerdatensätze angewendet oder aus diesen entfernt, wenn Benutzer manuell oder nach einem Zeitplan in die Appliance importiert werden.

Verwandte Themen

Verwalten von LDAP-Labels

Informationen zu Labelgruppen

Sie können Labels organisieren, indem Sie sie Labelgruppen zuweisen. Labelgruppen geben ihre Typen an die in ihnen enthaltenen Labels weiter.

Eine Labelgruppe kann nicht nur mehrere Labels beinhalten, sondern auch mehreren Labelgruppen zugewiesen sein. Labels erben sämtliche Einschränkungen der Gruppen, denen sie angehören.

Verwandte Themen

Labelgruppen hinzufügen, anzeigen oder bearbeiten

Informationen zu Organisationsfiltern

Organisationsfilter ähneln Labels, sie dienen jedoch einem bestimmten Zweck: Organisationfilter weisen bei der Inventarerfassung von Geräten diese automatisch an Organisationen zu.

Es gibt zwei Arten von Organisationsfiltern:

- **Datenfilter**: Weist Geräte basierend auf Suchkriterien automatisch Organisationen zu. Bei der Inventarerfassung von Geräten werden diese der Organisation zugewiesen, wenn sie den Kriterien entsprechen. Dieser Filter ähnelt Smart Labels dahingehend, dass er Geräte automatisch Organisationen zuweist, wenn sie den angegebenen Kriterien entsprechen.
- **LDAP-Filter**: Weisen Geräte basierend auf LDAP- oder Active Directory-Interaktionen automatisch Organisationen zu. Bei der Inventarerfassung von Geräten wird die Abfrage an den LDAP-Server gesendet. Wenn Geräte den Kriterien entsprechen, werden sie automatisch der Organisation zugewiesen.

Verwandte Themen

Verwalten von Organisationsfiltern

Verfolgen von Änderungen an Labeleinstellungen

Wenn Verlaufsabonnements zur Aufbewahrung von Informationen konfiguriert wurden, können Sie Details zu den an Einstellungen, Assets und Objekten vorgenommenen Änderungen anzeigen.

Diese Informationen beinhalten auch das Datum der Änderung und den Benutzer, der diese vorgenommen hat. Dies kann bei der Fehlerbehebung nützlich sein.

Verwandte Themen

Informationen zu den Verlaufseinstellungen

Verwalten manueller Labels

Sie können Labels im Abschnitt *Label* der **Administratorkonsole** verwalten. Labels können auch über Listenseiten anderer Abschnitte wie *Inventar* und *Sicherheit* hinzugefügt und zugewiesen werden, indem Sie **Aktion auswählen** > **Label hinzufügen** auswählen.

Manuelle Labels hinzufügen oder bearbeiten

Sie können manuelle Labels nach Bedarf hinzufügen oder bearbeiten.

1. Rufen Sie die Seite *Label-Detail* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste im Abschnitt **Startseite** auf **Label-Verwaltung**.
   c. Klicken Sie im Bereich für die Label-Verwaltung auf **Labels**.
   d. Führen Sie einen der folgenden Schritte aus, um die Seite *Label-Detail* anzuzeigen:
   - Klicken Sie auf den Namen eines Labels.
   - Klicken Sie auf **Aktion auswählen** > **Neu** > **Manuelles Label**.

   TIPP: Vermeiden Sie in Labelnamen die Verwendung des umgekehrten Schrägstrichs (\). Wenn Sie einen umgekehrten Schrägstrich in einem Labelnamen verwenden müssen, fügen Sie einen zweiten umgekehrten Schrägstrich hinzu (\\), damit er nicht als Befehl interpretiert wird.

2. Geben Sie die folgenden Informationen an:

Option	Beschreibung
Name	Der Name des Labels. Dieser Name wird in der Liste Labels angezeigt.
Beschreibung	Geben Sie nach Bedarf beliebige weitere Informationen ein.
Alternativer Speicherort	(Optional) Die alternative Download-Quelle für verwaltete Installationen, Dateisynchronisierungen und andere Bereitstellungen, die auf den diesem

Option	Beschreibung
	Label zugeordneten Elementen ausgeführt werden. Die Quelle, die Sie angeben, überschreibt die Zeichenfolge KACE_ALT_LOCATION. **VORSICHT: Weisen Sie Geräten nicht zwei Labels zu, die beide einen Wert in diesem Feld festlegen.**
Pfad	Geben Sie bei Angabe einer alternativen Downloadquelle den Pfad zu dieser Quelle an.
Anmeldung **Kennwort**	Wenn Sie eine alternative Download-Quelle angeben, geben Sie den Benutzernamen und das Kennwort für die Quelle an.
Labelnutzung beschränken auf	(Optional) Die Kategorien der Elemente, auf die das Label oder die Labelgruppe angewendet werden können. Wenn Sie die Labelnutzung nicht beschränken, können das Label bzw. die Labelgruppe auf jedes beliebige Element angewendet werden. Wenn Sie jedoch das Label oder die Labelgruppe auf Kategorien wie Anwendungen und Patches beschränken, kann dieses Label bzw. diese Labelgruppe nur auf Anwendungen und Patches angewendet werden, und nicht auf andere Elemente wie beispielsweise Geräte.
Erfassung der Softwarenutzung	Aktiviert die Nutzungserfassung auf Geräten, die dieses Label aufweisen. Es kann damit nur die Nutzungserfassung von Geräten aktiviert werden. Um auch die Nutzung von Software zu erfassen, müssen Sie auch die Nutzungserfassung für einzelne Anwendungen aktivieren.
Anwendungssteuerung zulassen	Aktivieren Sie die Anwendungssteuerung auf Geräten. Software, die als "Nicht zulässig" gekennzeichnet wurde, kann nicht auf den Geräten ausgeführt werden, auf die das Label angewendet wurde.
Labelgruppe	(Optional) Die Labelgruppe, der das Label zugeordnet ist. Um das Label einer Labelgruppe zuzuordnen, klicken Sie auf **Bearbeiten** neben dem Feld *Labelgruppe* und wählen dann eine Labelgruppe aus. Dies ist nützlich, wenn Sie über eine große Zahl von Labels verfügen, die Sie in Unter-Labels gruppieren möchten. Sie können beispielsweise die Labels Ihrer lizenzierten Anwendungen in einer Labelgruppe namens *Lizenzen* zusammenfassen. Labels erben außerdem sämtliche Einschränkungen der Gruppen, denen sie angehören.
Auf Benutzerrolle angepasst	Die zu diesem Label zugewiesene Benutzerrolle. Wenn ein Label einer Benutzerrolle zugewiesen

Option	Beschreibung
	ist, sind die Benutzer-Aktionen auf die Geräte, Skripte und Zeitpläne beschränkt, die dem Label zugewiesen sind. Weitere Informationen zu Benutzerrollen finden Sie unter Benutzerrollen hinzufügen oder bearbeiten.

3. Klicken Sie auf **Speichern**.

Verwandte Themen

Anwendungssteuerungslabel zu Geräten zuweisen

Details zu manuellen Labels anzeigen

Sie können Details zu manuellen Labels anzeigen, beispielsweise die Mitglieder eines Labels, Einschränkungen für die Labelnutzung und Informationen zum alternativen Speicherort.

1. Rufen Sie die Seite *Label-Detail* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste im Abschnitt **Startseite** auf **Label-Verwaltung**.
   c. Klicken Sie im Bereich für die Label-Verwaltung auf **Labels**.
2. Um Labelgruppen anzuzeigen bzw. auszublenden, wählen Sie im Menü *Aktion auswählen* die Option **Labelgruppen anzeigen** bzw. **Labelgruppen ausblenden** aus.
3. Um die Mitglieder eines Labels anzuzeigen, klicken Sie auf eine Zahl unterhalb in einer Spalte, beispielsweise *Geräte*, *Benutzer*, *Software* usw.
4. Klicken Sie auf den verknüpften Namen eines Labels, um die Label-Details anzuzeigen.

   Die Seite *Label-Detail* wird angezeigt.
5. Klicken Sie im Abschnitt *Elemente mit Label* auf das die Schaltfläche **Hinzufügen** neben den Abschnittsüberschriften, um die Anzeige zu erweitern bzw. zu reduzieren: +.

Manuelle Labels löschen

Bevor Sie ein manuelles Label löschen können, müssen Sie es aus allen Elementen entfernen, denen es zugewiesen wurde. Es ist nicht möglich, manuelle Labels zu löschen, die auf Elemente angewendet sind.

Falls ein manuelles Label außerdem ein Smart Label oder ein LDAP-Label enthält, müssen Sie auch das Smart Label bzw. LDAP-Label löschen, bevor Sie das manuelle Label löschen können. Es ist nicht möglich, manuelle Labels zu löschen, die Smart Labels oder LDAP-Labels enthalten.

1. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
2. Entfernen Sie das Label von allen Elementen, denen es zugewiesen wurde. So entfernen Sie beispielsweise ein Label von einem Gerät:
   a. Klicken Sie auf **Inventar**.

      Die Seite *Geräte* wird angezeigt.
   b. Wählen Sie in der Dropdown-Liste *Anzeigen nach* die Option **Label > Labelname** aus.

      Auf der Seite *Geräte* werden die Elemente angezeigt, denen das Label zugewiesen ist.

c. Wählen Sie alle Elemente aus der Liste aus.

d. Klicken Sie auf **Aktion auswählen** > **Label entfernen** > **Labelname**.

3. Nachdem das Label von allen Elementen entfernt wurde, klicken Sie auf **Startseite** > **Labels** > **Label-Verwaltung**.

   Die Seite *Labels* wird angezeigt.

4. Aktivieren Sie die Kontrollkästchen neben einem oder mehreren Labels.
5. Wählen Sie **Aktion auswählen** > **Löschen** und klicken Sie dann zum Bestätigen auf **Ja**.

Verwalten von Smart Labels

Sie können Smart Labels für Geräte, Anwendungen auf der Seite Software, Patches, Erkennungsergebnisse und Dell Aktualisierungspakete hinzufügen.

Smart Labels können nicht für Anwendungen auf der Seite *Softwarekatalog* erstellt werden.

Smart Labels hinzufügen

Sie können Smart Labels im Abschnitt *Labels* und auf Listenseiten, auf denen Smart Labels verwendet werden (beispielsweise die Liste *Geräte*), hinzufügen.

1. Rufen Sie die Seite *Label-Detail* auf:

   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.

   b. Klicken Sie in der linken Navigationsleiste im Abschnitt **Startseite** auf **Label-Verwaltung**.

   c. Klicken Sie im Bereich für die Label-Verwaltung auf **Smart Labels**.

   d. Klicken Sie auf **Aktion auswählen** > **Neu** > **Smart Label type** (Smart Label-Typ).

      Die Appliance zeigt für den von Ihnen gewählten Labeltyp die *Smart Label*-Kriterien an. Wenn Sie beispielsweise **Neu** > **Software Smart Label** auswählen, werden die Softwarekriterien angezeigt. Wenn Sie **Neu** > **Smart Label für Gerät** auswählen, werden die *Geräte*-Kriterien angezeigt.

2. Legen Sie die Suchkriterien anhand der verfügbaren Felder fest.

   - Klicken Sie zum Hinzufügen einer Zeile auf **Zeile hinzufügen**.
   - Um einen Unterregelsatz hinzuzufügen, wählen Sie in der Dropdown-Liste für Operatoren rechts neben den Smart Label-Kriterien **UND** oder **ODER** aus und klicken anschließend auf **Gruppe hinzufügen**.

3. Klicken Sie auf **Testen**, um Elemente anzuzeigen, die den angegebenen Kriterien entsprechen.
4. Passen Sie die Kriterien an, bis die Ergebnisse Ihren Erwartungen entsprechen.
5. Führen Sie im Menü *Label auswählen* einen der folgenden Schritte aus:

   - **Wählen Sie ein vorhandenes Label aus, um es mit diesem Smart Label zu verknüpfen. Geben Sie in das Feld** *Label auswählen* **einen Begriff ein, um nach vorhandenen Labels zu suchen.**

HINWEIS: Wenn Sie statt eines Labels eine Labelgruppe auswählen, können Sie das Smart Label nicht auf einen Patching-Zeitplan anwenden. Patch-Zeitpläne können nur Smart Labels verwenden, die auf einem einzelnen Element basieren.

- **Geben Sie einen neuen Namen für das Smart Label im Feld** *Label auswählen* **ein und drücken Sie Enter bzw. die Eingabetaste.**

HINWEIS: Drücken Sie **Enter** bzw. die **Eingabetaste**, nachdem Sie einen neuen Smart Label-Namen eingegeben haben, um den Text aus dem Suchfeld in das Label-Feld zu verschieben.

6. Klicken Sie auf **Speichern**.

Verwandte Themen

Geräte mithilfe von Labels gruppieren

Smart Labels für Erkennungsergebnisse verwenden

Beispiel: Smart Labels zum Identifizieren von Geräten kombinieren

Dieses Beispiel zeigt, wie drei Smart Labels kombiniert werden, um Geräte zu identifizieren, auf denen Windows XP oder Windows 8 ausgeführt wird und die VirusScan®-Anwendung von McAfee® nicht installiert ist.

Die folgenden drei Smart Labels werden in diesem Beispiel erstellt:

- Das erste Smart Label, *Win78*, wird Geräten unter den Betriebssystemen Windows XP oder Windows 8 zugewiesen. Die Ausführungsreihenfolge dieses Labels ist 1.
- Das zweite Smart Label, *MissingVirusScan*, wird Geräten zugewiesen, auf denen die VirusScan-Anwendung nicht installiert ist. Die Ausführungsreihenfolge dieses Labels ist ebenfalls 1.
- Das dritte Smart Label, *Win78MissingVirusScan*, wird Geräten mit den Smart Labels *Win78* und *MissingVirusScan* zugewiesen. Die Ausführungsreihenfolge dieses Labels ist 2, damit es nach den ersten beiden Labels ausgeführt wird.

1. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
2. Erstellen Sie ein Geräte-Smart Label zur Identifizierung des Betriebssystems:
   a. Klicken Sie in der linken Navigationsleiste auf **Inventar** und anschließend auf **Dashboard**.
   b. Klicken Sie rechts oberhalb der Liste auf die Registerkarte **Smart Label**.

      Der Bereich *Smart Label* wird angezeigt.

   c. Legen Sie die erforderlichen Kriterien für das Betriebssystem Windows XP fest:

      `Betriebssystem: Name des Betriebssystems | hat | Windows 7`

   d. Wählen Sie in der Dropdown-Liste "Operator" die Option **ODER** aus, klicken Sie auf **Zeile hinzufügen**, und geben Sie dann die erforderlichen Kriterien für das Betriebssystem Windows 8 an:

      `Betriebssystem: Name des Betriebssystems | hat | Windows 8`

e. Geben Sie in der Dropdown-Liste *Label auswählen* einen Namen für das Label ein, beispielsweise Win78, und klicken Sie anschließend auf **Smart Label**.

3. Erstellen Sie ein Geräte-Smart Label zum Ermitteln von Geräten, auf denen die VirusScan-Anwendung nicht installiert ist:
   a. Geben Sie auf der Seite *Geräte* im Fensterbereich *Smart Label* die Kriterien an, die für die Suche nach Geräten ohne VirusScan-Anwendung erforderlich sind:

   ```
   Software: Softwaretitel | hat nicht | VirusScan
   ```

   b. Geben Sie in der Dropdown-Liste *Label auswählen* einen Namen für das Label ein, beispielsweise MissingVirusScan, und klicken Sie anschließend auf **Smart Label**.
4. Erstellen Sie ein Geräte-Smart Label, das die in den vorhergehenden Schritten erstellten Smart Labels verwendet.
5. Erstellen Sie ein Smart Label für die Anwendung:
   a. Geben Sie auf der Seite *Geräte* im Bereich *Smart Label* die Kriterien zur Identifizierung von Geräten mit dem Smart Label *Win78* ein.

   ```
   Identitätsinformationen des Geräts: Labelnamen | = | Win78
   ```

   b. Wählen Sie in der Dropdown-Liste „Operator“ die Option **UND** aus, klicken Sie auf **Zeile hinzufügen** und geben Sie dann die erforderlichen Kriterien zum Identifizieren von Geräten mit dem Smart Label *MissingVirusScan* an:

   ```
   Identitätsinformationen des Geräts: Labelnamen | = | MissingVirusScan
   ```

   c. Geben Sie in der Dropdown-Liste *Label auswählen* einen Namen für das Label ein, beispielsweise Win78MissingVirusScan, und klicken Sie anschließend auf **Smart Label**.
6. Legen Sie die Reihenfolge fest, in der die Smart Labels ausgeführt werden:
   a. Klicken Sie in der linken Navigationsleiste im Abschnitt **Startseite** auf **Label-Verwaltung**.
   b. Klicken Sie im Bereich für die Label-Verwaltung auf **Smart Labels**.
   c. Klicken Sie auf **Aktion auswählen** > **Reihenfolge für Labels festlegen** > **Smart Labels für Gerät**.

      Die Seite *Reihenfolge der Smart Labels für Geräte festlegen* wird angezeigt.

   d. Klicken Sie ganz rechts neben der Label-Zeile *Win78* auf die Schaltfläche **Bearbeiten**: .
   e. Klicken Sie in der Spalte *Reihenfolge* auf 1 und anschließend auf **Speichern**.
   f. Klicken Sie ganz rechts neben der Label-Zeile *MissingVirusScan* auf die Schaltfläche **Bearbeiten**: .
   g. Klicken Sie in der Spalte *Reihenfolge* auf 1 und anschließend auf **Speichern**.
   h. Klicken Sie ganz rechts neben der Label-Zeile *Win78MissingVirusScan* auf die Schaltfläche **Bearbeiten**: .
   i. Klicken Sie in der Spalte *Reihenfolge* auf 2 und anschließend auf **Speichern**.
   j. Klicken Sie unten in der Liste auf **Speichern**.

      Die Labels *Win78* und *MissingVirusScan* wurden so festgelegt, dass sie vor dem Label *Win78MissingVirusScan* ausgeführt werden. Dadurch wird sichergestellt, dass Geräten mit Windows XP und 8, auf denen die VirusScan-Anwendung nicht installiert ist, ein Label zugewiesen wird, bevor das Label *Win78MissingVirusScan* ausgeführt wird.

Smart Labels bearbeiten

Sie können die in Smart Labels verwendeten SQL-Abfragen nach Bedarf ändern.

Wenn Sie die SQL-Abfrage für das Smart Label einer Software ändern, wird das Smart Label sofort auf Elemente angewendet bzw. von ihnen entfernt, je nachdem, ob die Elemente den neuen Kriterien entsprechen.

Smart Labels von Geräten werden auf die Geräte angewendet bzw. von diesen entfernt, sobald die Inventarinformationen des Geräts aktualisiert werden.

Wenn Sie den SQL-Code eines Smart Labels manuell bearbeiten, können Sie das Label nicht mehr über die Smart Label Vorlage bearbeiten. Der Grund dafür ist, dass über die Vorlage kein benutzerdefinierter SQL-Code bearbeitet werden kann.

1. Rufen Sie die Seite *Label-Detail* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste im Abschnitt **Startseite** auf **Label-Verwaltung**.
   c. Klicken Sie im Bereich für die Label-Verwaltung auf **Smart Labels**.
   d. Klicken Sie auf den Namen eines Smart Labels oder klicken Sie auf die Schaltfläche **Bearbeiten** links neben dem Namen des Smart Labels.

   HINWEIS: Wenn der SQL-Code des Smart Labels manuell bearbeitet wurde, wird die Schaltfläche *Bearbeiten* nicht angezeigt.
2. Führen Sie einen der folgenden Schritte aus:
   - **Aktivieren oder deaktivieren Sie das Kontrollkästchen** *Nutzungserfassung aktivieren* **zur Aktivierung bzw. Deaktivierung der Nutzungserfassung für Smart Labels.**
   - **Wählen Sie im Feld** *Zugewiesenes Label* **das Label aus, das Sie mit dem Smart Label verknüpfen möchten.**
   - **Klicken Sie auf Details, um die Detailseite für das zugewiesene Label anzuzeigen.**
   - **Falls das Smart Label mit der Smart Label-Vorlage erstellt und der SQL-Code nicht manuell bearbeitet wurde, klicken Sie auf den Link neben** *Zur Überarbeitung des Smart Label mit dem ursprünglichen Editor***.**
   - **Um den Smart Label SQL-Code manuell zu bearbeiten, klicken Sie auf den Link neben** *mit diesem Editor zu bearbeiten***.**

   VORSICHT: Wenn Sie den SQL-Code eines Smart Labels manuell bearbeiten, können Sie das Label nicht mehr über die Smart Label Vorlage bearbeiten. Der Grund dafür ist, dass der Assistent keinen benutzerdefinierten SQL-Code bearbeiten kann.
3. **Optional**: Klicken Sie auf **Duplizieren**, um ein neues Smart Label zu erstellen, das dieselbe SQL-Abfrage verwendet.
4. Klicken Sie auf **Speichern**.

   HINWEIS: Wenn Sie auf **Duplizieren** klicken, um ein Label zu erstellen, können Sie es nur einem neuen Label zuweisen.

Labels für Benutzerkonten festlegen

Sie können Benutzerkonten auf die gleiche Weise mithilfe von Labels gruppieren, wie Sie Geräte und Software im Abschnitt *Inventar* mit Labels gruppieren. Außerdem können Smart Labels verwendet werden, um Zugriffsstufen für Benutzer zu erteilen. Sie können beispielsweise mit Labels festlegen, welche Benutzer zum Senden, Annehmen, Ablehnen, Bearbeiten und Lösen von Service-Desk-Tickets berechtigt sind.

Außerdem lassen sich alle Labels, die Sie innerhalb des Abschnitts *Inventar* erstellen, als Benutzerlabel im Service Desk verwenden, sofern die Labels ohne Beschränkungen erstellt wurden. Wenn die Labels mit Einschränkungen erstellt wurden, können Sie sie ändern oder im Abschnitt *Inventar* Labels ohne Einschränkungen erstellen.

Label "Alle Ticketbesitzer" hinzufügen

Wenn Sie Benutzern die Berechtigung gewähren möchten, Besitzer von Service-Desk-Tickets zu sein, können Sie ein Label "Alle Ticketbesitzer" erstellen und Benutzerkonten zuweisen.

1. Rufen Sie die Seite *Label-Detail* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste im Abschnitt **Startseite** auf **Label-Verwaltung**.
   c. Klicken Sie im Bereich für die Label-Verwaltung auf **Labels**.
   d. Klicken Sie auf **Aktion auswählen** > **Neues manuelles Label**.

   TIPP: Vermeiden Sie in Labelnamen die Verwendung des umgekehrten Schrägstrichs (\). Wenn Sie einen umgekehrten Schrägstrich in einem Labelnamen verwenden müssen, fügen Sie einen zweiten umgekehrten Schrägstrich hinzu (\\), damit er nicht als Befehl interpretiert wird.

2. Geben Sie die folgenden Informationen an:

Option	Beschreibung
Name	Der Name des Labels. Dieser Name wird in der Liste *Labels* angezeigt. Geben Sie einen Namen wie beispielsweise Alle Ticketbesitzer ein.
Beschreibung	Geben Sie nach Bedarf beliebige weitere Informationen ein.

3. Klicken Sie auf **Speichern**.

Das neue Label ist im Menü **Aktion auswählen** > **Label zuweisen** auf der Seite *Benutzer* verfügbar. Informationen zum Zuweisen des Labels zu Service Desk-Mitarbeitern beim Importieren von Benutzerdaten finden Sie unter Importieren von Benutzern aus einem LDAP-Server.

Smart Labels für Patches verwenden

Sie können Smart Labels verwenden, um Patches und Geräte automatisch zu gruppieren. Sie können Patches und Geräten auch manuell Labels zuweisen. Smart Labels sind meist effizienter, da sie automatisch angewendet und entfernt werden.

So können Sie beispielsweise ein Smart Label erstellen, das allen Windows XP Server-Patches entspricht. Jedes Mal, wenn einer dieser Patches für das Gerät verfügbar wird, wird das Label auf den Patch angewendet. Wenn Sie einen Patch-Zeitplan einrichten, um dieses Label automatisch zu erkennen und auf Geräten bereitzustellen, wird der Patch automatisch auf den Windows XP Servern im Inventar angewendet.

Sie können ein Label-Schema erstellen, mit dem Patches nach Betriebssystem und Wichtigkeit sortiert werden, beispielsweise **P (Patch) Betriebssystem/Wichtigkeit**. Beispiel:

- P Win7
- P Win7 Kritisch
- P Win7 Wichtig
- P MS Office
- P Leopard
- P Mac10.8 Kritischer Test

Auf ähnliche Weise erstellen Sie Geräte-Smart Labels, um die Geräte (G) anzugeben, auf denen Sie Patches installieren möchten:

- G Alle Desktops
- G Alle Server
- G Alle Desktops

Die Appliance wertet die von den Agenten bei der Anmeldung bereitgestellten Informationen aus und weist Geräte-Smart Labels zu, wenn die Daten den Labelkriterien entsprechen.

Patch-Smart Labels werden vorhandenen Patches, die den Kriterien entsprechen, sofort zugewiesen. Das Label wird neuen Patches nach dem Herunterladen hinzugefügt, wenn sie die Kriterien erfüllen.

Smart Labels für kritische Betriebssystem-Patches hinzufügen

Sie können ein Smart Label erstellen, um kritische Betriebssystem-Patches zu kennzeichnen.

1. Rufen Sie die Liste *Patch-Katalog* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Sicherheit** und anschließend auf **Patch-Verwaltung**.
   c. Klicken Sie im Fensterbereich *Patch-Verwaltung* auf **Katalog**.
2. Klicken Sie rechts oberhalb der Liste auf die Registerkarte **Smart Label**.

   Der Bereich *Smart Label* wird angezeigt.

3. Geben Sie Kriterien für Smart Labels an:
   a. Geben Sie Kriterien an, die aktive Patches kennzeichnen:

   `Patch-Listeninformationen: Status | ist | Aktiv`

   b. Klicken Sie auf **Zeile hinzufügen** und geben Sie anschließend Kriterien zum Kennzeichnen kritischer Patches an:

   `UND | Patch-Listeninformationen: Schweregrad | ist | Kritisch`

c. Klicken Sie auf **Zeile hinzufügen** und geben Sie anschließend Kriterien zum Kennzeichnen von Windows Patches an:

```
UND | Patch-Listeninformationen: Betriebssystem| ist | Windows
```

d. Klicken Sie auf **Zeile hinzufügen** und geben Sie anschließend Kriterien zum Kennzeichnen von Betriebssystem-Patches an:

```
UND | Patch-Listeninformationen: Kategorie | ist | Betriebssystem
```

4. Klicken Sie auf **Testen**, um Elemente anzuzeigen, die den Suchkriterien entsprechen.
5. Passen Sie die Kriterien an, bis die Ergebnisse Ihren Erwartungen entsprechen.
6. Führen Sie im Menü *Label auswählen* einen der folgenden Schritte aus:
   - **Wählen Sie ein vorhandenes Label aus, um es mit diesem Smart Label zu verknüpfen. Geben Sie in das Feld** *Label auswählen* **einen Begriff ein, um nach vorhandenen Labels zu suchen.**

     HINWEIS: Wenn Sie statt eines Labels eine Labelgruppe auswählen, können Sie das Smart Label nicht auf einen Patching-Zeitplan anwenden. Patch-Zeitpläne können nur Smart Labels verwenden, die auf einem einzelnen Element basieren.

   - **Geben Sie einen neuen Namen für das Smart Label im Feld** *Label auswählen* **ein und drücken Sie Enter bzw. die Eingabetaste.**

     HINWEIS: Drücken Sie **Enter** bzw. die **Eingabetaste**, nachdem Sie einen neuen Smart Label-Namen eingegeben haben, um den Text aus dem Suchfeld in das Label-Feld zu verschieben.
7. Klicken Sie auf **Speichern**.

Das Smart Label wird vorhandenen Patches, die den Kriterien entsprechen, sofort zugewiesen. Das Label wird neuen Patches nach dem Herunterladen hinzugefügt, wenn sie die Kriterien erfüllen.

Abonnieren Sie Patches. Siehe Abonnieren und Herunterladen von Patches.

Smart Labels für neue Patches hinzufügen

Sie können ein Smart Label erstellen, damit neue Patches, die bereitgestellt werden müssen, schnell erkannt werden.

1. Rufen Sie die Liste *Patch-Katalog* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Sicherheit** und anschließend auf **Patch-Verwaltung**.
   c. Klicken Sie im Fensterbereich *Patch-Verwaltung* auf **Katalog**.
2. Klicken Sie rechts oberhalb der Liste auf die Registerkarte **Smart Label**.

   Der Bereich *Smart Label* wird angezeigt.

3. Geben Sie Kriterien für Smart Labels an:
   a. Geben Sie die Suchkriterien ein, die nach einem bestimmten Datum veröffentlichte Patches kennzeichnen:

```
Patch-Listeninformationen: Herausgabedatum | > <Datum jjjj-mm-tt>
```

b. Klicken Sie auf **Zeile hinzufügen** und geben Sie anschließend Kriterien zum Kennzeichnen nicht kritischer Patches an:

```
UND | Patch-Listeninformationen: Auswirkungen| ist kritisch | kritisch
```

c. Klicken Sie auf **Zeile hinzufügen** und geben Sie anschließend Kriterien zum Kennzeichnen aktiver Patches an:

```
UND | Patch-Listeninformationen: Status | ist | Aktiv
```

4. Klicken Sie auf **Testen**.

   Alle nicht kritischen Patches, die nach dem angegebenen Datum hinzugefügt wurden, werden angezeigt.

5. Führen Sie im Menü *Label auswählen* einen der folgenden Schritte aus:

   - **Wählen Sie ein vorhandenes Label aus, um es mit diesem Smart Label zu verknüpfen. Geben Sie in das Feld *Label auswählen* einen Begriff ein, um nach vorhandenen Labels zu suchen.**

     HINWEIS: Wenn Sie statt eines Labels eine Labelgruppe auswählen, können Sie das Smart Label nicht auf einen Patching-Zeitplan anwenden. Patch-Zeitpläne können nur Smart Labels verwenden, die auf einem einzelnen Element basieren.

   - **Geben Sie einen neuen Namen für das Smart Label im Feld *Label auswählen* ein und drücken Sie Enter bzw. die Eingabetaste.**

     HINWEIS: Drücken Sie **Enter** bzw. die **Eingabetaste**, nachdem Sie einen neuen Smart Label-Namen eingegeben haben, um den Text aus dem Suchfeld in das Label-Feld zu verschieben.

6. Klicken Sie auf **Speichern**.

   Das Smart Label wird vorhandenen Patches, die den Kriterien entsprechen, sofort zugewiesen. Das Label wird neuen Patches nach dem Herunterladen hinzugefügt, wenn sie die Kriterien erfüllen.

Abonnieren Sie Patches. Siehe Abonnieren und Herunterladen von Patches.

Smart Labels für Erkennungsergebnisse verwenden

Mithilfe von Smart Labels können Erkennungsergebnissen, die bestimmte Kriterien erfüllen, automatisch Labels zugewiesen werden. Dies schließt DNS-, Socket- und SNMP-Ergebnisse in einem einzelnen Subnetz oder in mehreren Subnetzen ein.

Smart Labels für Erkennungsergebnisse hinzufügen

Sie können Smart Labels für Erkennungsergebnisse hinzufügen, um Ergebnisse zu gruppieren und zu verwalten.

1. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
2. Klicken Sie auf **Inventar** > **Erkennungsergebnisse**, um die Seite *Erkennungsergebnisse* anzuzeigen.
3. Klicken Sie über der Liste auf der rechten Seite auf die Registerkarte **Smart Label**, um den Fensterbereich *Smart Label* anzuzeigen.

4. Wählen Sie die Kriterien für Smart Labels aus:
   - **Wählen Sie in der Dropdown-Liste ganz links ein Attribut aus. Beispiel: Geräteinfo: Ping-Test**
   - **Wählen Sie in der mittleren Dropdown-Liste eine Bedingung aus. Beispiel: hat.**
   - **Wählen Sie in der nächsten Dropdown-Liste das Statusattribut aus. Beispiel: Fehler.**
5. Klicken Sie auf **Testen**, um Elemente anzuzeigen, die den Suchkriterien entsprechen.
6. Passen Sie die Kriterien an, bis die Ergebnisse Ihren Erwartungen entsprechen.
7. Führen Sie im Menü *Label auswählen* einen der folgenden Schritte aus:
   - **Wählen Sie ein vorhandenes Label aus, um es mit diesem Smart Label zu verknüpfen. Geben Sie in das Feld *Label auswählen* einen Begriff ein, um nach vorhandenen Labels zu suchen.**

     HINWEIS: Wenn Sie statt eines Labels eine Labelgruppe auswählen, können Sie das Smart Label nicht auf einen Patching-Zeitplan anwenden. Patch-Zeitpläne können nur Smart Labels verwenden, die auf einem einzelnen Element basieren.
   - **Geben Sie einen neuen Namen für das Smart Label im Feld *Label auswählen* ein und drücken Sie Enter bzw. die Eingabetaste.**

   HINWEIS: Drücken Sie **Enter** bzw. die **Eingabetaste**, nachdem Sie einen neuen Smart Label-Namen eingegeben haben, um den Text aus dem Suchfeld in das Label-Feld zu verschieben.
8. Klicken Sie auf **Speichern**.

Das Smart Label wird automatisch zugewiesen oder von den Erkennungsergebnissen entfernt, die den angegebenen Kriterien entsprechen. Bei der nächsten Ausführung des Erkennungszeitplans wird das Smart Label den ermittelten Geräten zugewiesen.

Ausführungsreihenfolge von Smart Labels für Erkennungsergebnisse ändern

Sie können die Reihenfolge festlegen, in der Smart Labels ausgeführt werden, indem Sie die Reihenfolgenwerte bearbeiten.

Smart Labels weisen den Standardreihenfolgenwert 100 auf. Smart Labels mit niedrigeren Werten werden vor Smart Labels mit höheren Werten ausgeführt. Siehe Ausführungsreihenfolge von Smart Labels zuweisen.

Smart Labels für Geräte hinzufügen

Mithilfe von Smart Labels können Sie Geräte nach Typ sortieren, beispielsweise Desktop, Server und Notebook. Nach dem Erstellen von Smart Labels für Geräte können Sie basierend auf diesen Labels die Patch-Bereitstellung planen.

Smart Labels für Desktops hinzufügen

Sie können ein Smart Label erstellen, um Geräte zu kennzeichnen, bei denen Desktop-Patches erforderlich sind.

1. Rufen Sie die Liste *Geräte* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen*

aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.

b. Klicken Sie in der linken Navigationsleiste auf **Inventar** und anschließend auf **Dashboard**.

2. Klicken Sie rechts oberhalb der Liste auf die Registerkarte **Smart Label**.

   Der Bereich *Smart Label* wird angezeigt.

3. Geben Sie Kriterien für Smart Labels an:

   a. Geben Sie die Kriterien an, die zum Ausblenden von Servern erforderlich sind:

   `Betriebssystem: Name | hat nicht | Server`

   b. Klicken Sie auf **Zeile hinzufügen** und geben Sie anschließend die erforderlichen Kriterien zum Ausschließen von Notebooks ein:

   `UND | BIOS-Hersteller: Gehäusetyp | hat nicht | Notebook`

   Weitere nützliche Kriterien zum Kennzeichnen von Desktops:

   - Systemnamen, wenn Sie allen Desktops einen ähnlichen Namen geben.
   - Systemmodelle, beispielsweise alle Systeme, deren Modellname den Text **XPS** enthält.
   - IP-Adressen oder Teile von IP-Adressen mit dem Kriterium **enthält**.
   - BIOS-Seriennummern oder das Kriterium **Enthält Teil-Seriennummer**. Dies ist hilfreich, wenn Sie Desktops mit Seriennummern erworben haben. Weitere Informationen erhalten Sie beim Hersteller.
   - Softwaretitel, wenn Desktops einen gemeinsamen Titel haben.

4. Klicken Sie auf **Testen**, um Elemente anzuzeigen, die den Suchkriterien entsprechen.
5. Führen Sie im Menü *Label auswählen* einen der folgenden Schritte aus:

   - **Wählen Sie ein vorhandenes Label aus, um es mit diesem Smart Label zu verknüpfen. Geben Sie in das Feld** *Label auswählen* **einen Begriff ein, um nach vorhandenen Labels zu suchen.**

     HINWEIS: Wenn Sie statt eines Labels eine Labelgruppe auswählen, können Sie das Smart Label nicht auf einen Patching-Zeitplan anwenden. Patch-Zeitpläne können nur Smart Labels verwenden, die auf einem einzelnen Element basieren.

   - **Geben Sie einen neuen Namen für das Smart Label im Feld** *Label auswählen* **ein und drücken Sie Enter bzw. die Eingabetaste.**

     HINWEIS: Drücken Sie **Enter** bzw. die **Eingabetaste**, nachdem Sie einen neuen Smart Label-Namen eingegeben haben, um den Text aus dem Suchfeld in das Label-Feld zu verschieben.

6. Klicken Sie auf **Speichern**, um das Smart Label zu erstellen.
7. **Optional**: Um zu überprüfen, ob das neue Label in der Liste *Labels* angezeigt wird, klicken Sie auf **Startseite** > **Labels** > **Smart Labels** oder **Label-Verwaltung**.

   Das neue Label ist zunächst leer. Wenn Geräte inventarisiert werden, wird ihnen das Label zugewiesen, sofern sie den Smart Label-Kriterien entsprechen.

8. Testen Sie das Smart Label:

   a. Klicken Sie auf **Inventar** > **Geräte**, um die Seite *Geräte* anzuzeigen.

b. Klicken Sie auf den Namen eines Geräts, das den Kriterien entspricht, dem das Label jedoch noch nicht zugewiesen wurde.

c. Klicken Sie auf der Seite *Gerätedetail* auf **Inventar erzwingen**.

Wenn das Smart Label ordnungsgemäß funktioniert, wird das Gerät angemeldet und das Label dem Gerät zugewiesen.

Die Option **Inventar erzwingen** ist nur verfügbar, wenn die Verbindung über das Agenten-Messaging-Protokoll zu einem von einem Agenten verwalteten Gerät aktiv ist oder wenn bei Geräten ohne Agenten das Gerät erreichbar ist.

Smart Labels für Server hinzufügen

Sie können ein Smart Label erstellen, um Geräte zu kennzeichnen, bei denen Server-Patches erforderlich sind.

1. Rufen Sie die Liste *Geräte* auf:

   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.

   b. Klicken Sie in der linken Navigationsleiste auf **Inventar** und anschließend auf **Dashboard**.

2. Klicken Sie rechts oberhalb der Liste auf die Registerkarte **Smart Label**.

   Der Bereich *Smart Label* wird angezeigt.

3. Geben Sie Suchkriterien an:

   a. Geben Sie die Kriterien an, die zum Kennzeichnen von Servern erforderlich sind:

   `Betriebssystem: Name | hat | Server`

   b. Klicken Sie auf **Zeile hinzufügen** und geben Sie anschließend die erforderlichen Kriterien zum Ausschließen von Notebooks ein:

   `UND | BIOS-Hersteller: Gehäusetyp | hat nicht | Notebook`

   Weitere nützliche Kriterien zum Kennzeichnen von Servern:

   - Systemnamen, wenn Sie allen Servern einen ähnlichen Namen geben.
   - IP-Adressen oder Teile von IP-Adressen mit dem Kriterium **enthält**.
   - BIOS-Seriennummern oder das Kriterium **Enthält Teil-Seriennummer**. Dies ist hilfreich, wenn Sie Server mit Seriennummern erworben haben. Weitere Informationen erhalten Sie beim Hersteller.
   - Softwaretitel, wenn Server einen gemeinsamen Titel haben.

4. Klicken Sie auf **Testen**, um Elemente anzuzeigen, die den Suchkriterien entsprechen.

5. Führen Sie im Menü *Label auswählen* einen der folgenden Schritte aus:

   - **Wählen Sie ein vorhandenes Label aus, um es mit diesem Smart Label zu verknüpfen. Geben Sie in das Feld** *Label auswählen* **einen Begriff ein, um nach vorhandenen Labels zu suchen.**

HINWEIS: Wenn Sie statt eines Labels eine Labelgruppe auswählen, können Sie das Smart Label nicht auf einen Patching-Zeitplan anwenden. Patch-Zeitpläne können nur Smart Labels verwenden, die auf einem einzelnen Element basieren.

- **Geben Sie einen neuen Namen für das Smart Label im Feld** *Label auswählen* **ein und drücken Sie Enter bzw. die Eingabetaste.**

HINWEIS: Drücken Sie **Enter** bzw. die **Eingabetaste**, nachdem Sie einen neuen Smart Label-Namen eingegeben haben, um den Text aus dem Suchfeld in das Label-Feld zu verschieben.

6. Klicken Sie auf **Speichern**.
7. **Optional**: Um zu überprüfen, ob das neue Label in der Liste *Labels* angezeigt wird, klicken Sie auf **Startseite** > **Labels** > **Smart Labels** oder **Label-Verwaltung**.

   Das neue Label ist zunächst leer. Wenn Geräte inventarisiert werden, wird ihnen das Label zugewiesen, sofern sie den Smart Label-Kriterien entsprechen.
8. Testen Sie das Smart Label:
   a. Klicken Sie auf **Inventar** > **Geräte**, um die Seite *Geräte* anzuzeigen.
   b. Klicken Sie auf den Namen eines Geräts, das den Kriterien entspricht, dem das Label jedoch noch nicht zugewiesen wurde.
   c. Klicken Sie auf der Seite *Gerätedetail* auf **Inventar erzwingen**.

      Wenn das Smart Label ordnungsgemäß funktioniert, wird das Gerät angemeldet und das Label dem Gerät zugewiesen.

   Die Option **Inventar erzwingen** ist nur verfügbar, wenn die Verbindung über das Agenten-Messaging-Protokoll zu einem von einem Agenten verwalteten Gerät aktiv ist oder wenn bei Geräten ohne Agenten das Gerät erreichbar ist.

Smart Labels für Laptops hinzufügen

Sie können ein Smart Label erstellen, um Geräte zu kennzeichnen, bei denen Notebook-Patches erforderlich sind.

1. Rufen Sie die Liste *Geräte* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Inventar** und anschließend auf **Dashboard**.
2. Klicken Sie rechts oberhalb der Liste auf die Registerkarte **Smart Label**.

   Der Bereich *Smart Label* wird angezeigt.

3. Geben Sie Suchkriterien an:
   a. Geben Sie die Kriterien an, die zum Ausblenden von Servern erforderlich sind:

      `Betriebssystem: Name | hat nicht | Server`

   b. Klicken Sie auf **Zeile hinzufügen** und geben Sie anschließend die erforderlichen Kriterien zum Kennzeichnen von Notebooks ein:

```
UND | BIOS-Hersteller: Gehäusetyp | hat | Notebook
```

Weitere nützliche Kriterien zum Kennzeichnen von Notebooks:

- Systemnamen, wenn Sie allen Notebooks einen ähnlichen Namen geben.
- IP-Adressen oder Teile von IP-Adressen mit dem Kriterium **enthält**.
- BIOS-Seriennummern oder das Kriterium **Enthält Teil-Seriennummer**. Dies ist hilfreich, wenn Sie Notebooks mit Seriennummern erworben haben. Weitere Informationen erhalten Sie beim Hersteller.
- Softwaretitel, wenn Notebooks einen gemeinsamen Titel haben.

4. Klicken Sie auf **Testen**, um Elemente anzuzeigen, die den Suchkriterien entsprechen.
5. Führen Sie im Menü *Label auswählen* einen der folgenden Schritte aus:
   - **Wählen Sie ein vorhandenes Label aus, um es mit diesem Smart Label zu verknüpfen. Geben Sie in das Feld *Label auswählen* einen Begriff ein, um nach vorhandenen Labels zu suchen.**

     HINWEIS: Wenn Sie statt eines Labels eine Labelgruppe auswählen, können Sie das Smart Label nicht auf einen Patching-Zeitplan anwenden. Patch-Zeitpläne können nur Smart Labels verwenden, die auf einem einzelnen Element basieren.

   - **Geben Sie einen neuen Namen für das Smart Label im Feld *Label auswählen* ein und drücken Sie Enter bzw. die Eingabetaste.**

     HINWEIS: Drücken Sie **Enter** bzw. die **Eingabetaste**, nachdem Sie einen neuen Smart Label-Namen eingegeben haben, um den Text aus dem Suchfeld in das Label-Feld zu verschieben.
6. Klicken Sie auf **Speichern**, um das Smart Label zu erstellen.
7. **Optional**: Um zu überprüfen, ob das neue Label in der Liste *Labels* angezeigt wird, klicken Sie auf **Startseite** > **Labels** > **Smart Labels** oder **Label-Verwaltung**.

   Das neue Label ist zunächst leer. Wenn Geräte inventarisiert werden, wird ihnen das Label zugewiesen, sofern sie den Smart Label-Kriterien entsprechen.
8. Testen Sie das Smart Label:
   a. Klicken Sie auf **Inventar** > **Geräte**, um die Seite *Geräte* anzuzeigen.
   b. Klicken Sie auf den Namen eines Geräts, das den Kriterien entspricht, dem das Label jedoch noch nicht zugewiesen wurde.
   c. Klicken Sie auf der Seite *Gerätedetail* auf **Inventar erzwingen**.

      Wenn das Smart Label ordnungsgemäß funktioniert, wird das Gerät angemeldet und das Label dem Gerät zugewiesen.

   Die Option **Inventar erzwingen** ist nur verfügbar, wenn die Verbindung über das Agenten-Messaging-Protokoll zu einem von einem Agenten verwalteten Gerät aktiv ist oder wenn bei Geräten ohne Agenten das Gerät erreichbar ist.

Ausführungsreihenfolge von Smart Labels zuweisen

Sie können Smart Labels nacheinander ausführen, indem Sie in den Smart Label-Eigenschaften die Ausführungsreihenfolge festlegen.

Die Zuweisung von Ausführungsreihenfolgen für Smart Labels kann zweckmäßig sein, wenn ein bestimmtes Smart Label vor anderen Smart Labels ausgeführt werden soll. Sie könnten beispielsweise ein Smart Label besitzen, das eine Gruppe von Geräten bezeichnet. Wenn Sie ein zweites Smart Label verwenden möchten, um die Gerätegruppe auf der Grundlage des zuerst zugewiesenen Labels weiter zu verfeinern, können Sie die Ausführungsreihenfolge so festlegen, dass das erste Smart Label vor dem zweiten ausgeführt wird. Smart Labels weisen den Standardreihenfolgenwert 100 auf. Smart Labels mit niedrigeren Werten werden vor Smart Labels mit höheren Werten ausgeführt.

1. Rufen Sie die Liste *Smart Label* auf:

a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
b. Klicken Sie in der linken Navigationsleiste im Abschnitt **Startseite** auf **Label-Verwaltung**.
c. Klicken Sie im Bereich für die Label-Verwaltung auf **Smart Labels**.

2. Wählen Sie im Abschnitt *Reihenfolge* im Menü *Aktion auswählen* den Labeltyp aus, dessen Ausführungsreihenfolge Sie ändern möchten.

   Die Seite *Reihenfolge* wird mit allen Smart Labels des ausgewählten Typs angezeigt.
3. So ändern Sie den Reihenfolgenwert eines Smart Labels
   a. Klicken Sie rechts neben der Spalte *Reihenfolge* auf die Schaltfläche **Bearbeiten**. .
   b. Geben Sie den entsprechenden Reihenfolgenwert ein und klicken Sie auf **Speichern**.
4. Klicken Sie auf **Speichern**.

Smart Labels löschen

Das Löschen von Smart Labels ist hilfreich, falls Sie umfangreiche Änderungen an Smart Label-Kriterien vornehmen und gleichzeitig Labels beibehalten müssen, die in Aufgaben wie verwalteten Installationen verwendet werden.

Sie können z. B. alle Kriterien eines Smart Labels löschen und anschließend dem Containerlabel neue Kriterien zuweisen. Dadurch würden Sie praktisch ein neues Smart Label mithilfe des bestehenden Containerlabels, das für verwaltete Installationen benötigt wird, erstellen.

Durch das Löschen eines Smart Labels werden die Kriterien, die dem Smart Label zugeordnet sind, entfernt, es werden jedoch keine anderen Labels gelöscht, die dem Smart Label zugewiesen sind.

1. Rufen Sie die Liste *Smart Label* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste im Abschnitt **Startseite** auf **Label-Verwaltung**.
   c. Klicken Sie im Bereich für die Label-Verwaltung auf **Smart Labels**.
2. Aktivieren Sie das Kontrollkästchen neben mindestens einem Smart Label.
3. Wählen Sie **Aktion auswählen** > **Löschen** und klicken Sie dann zum Bestätigen auf **Ja**.

Verwalten von Labelgruppen

Sie verwalten Labelgruppen im Abschnitt *Labels*.

Labelgruppen hinzufügen, anzeigen oder bearbeiten

Sie können Labelgruppen nach Bedarf hinzufügen, anzeigen und bearbeiten.

1. Rufen Sie die Seite *Labelgruppen-Detail* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.

b. Klicken Sie in der linken Navigationsleiste im Abschnitt **Startseite** auf **Label-Verwaltung**.
c. Klicken Sie im Bereich für die Label-Verwaltung auf **Labels**.
d. Führen Sie einen der folgenden Schritte aus, um die Seite *Labelgruppen-Detail* anzuzeigen:

- Klicken Sie auf den Namen einer Labelgruppe.
- Klicken Sie auf **Aktion auswählen** > **Neue Labelgruppe**.

2. Geben Sie die folgenden Informationen an:

Option	Beschreibung
Name	Der Name der Labelgruppe
Beschreibung	Geben Sie nach Bedarf beliebige weitere Informationen ein.
Labelgruppen-Nutzung beschränken auf	(Optional) Die Kategorien der Elemente, auf die das Label oder die Labelgruppe angewendet werden können. Wenn Sie die Labelnutzung nicht beschränken, können das Label bzw. die Labelgruppe auf jedes beliebige Element angewendet werden. Wenn Sie jedoch das Label oder die Labelgruppe auf Kategorien wie Anwendungen und Patches beschränken, kann dieses Label bzw. diese Labelgruppe nur auf Anwendungen und Patches angewendet werden, und nicht auf andere Elemente wie beispielsweise Geräte.
Erfassung der Softwarenutzung	Aktivieren oder deaktivieren Sie dieses Kontrollkästchen zur Aktivierung bzw. Deaktivierung der Nutzungserfassung für Gerätelabels.
Anwendungssteuerung zulassen	Aktivieren Sie die Anwendungssteuerung auf Geräten. Software, die als "Nicht zulässig" gekennzeichnet wurde, kann nicht auf den Geräten ausgeführt werden, auf die das Label angewendet wurde.
Labelgruppe	(Optional) Die Labelgruppe, der das Label zugeordnet ist. Um das Label einer Labelgruppe zuzuordnen, klicken Sie auf **Bearbeiten** neben dem Feld *Labelgruppe* und wählen dann eine Labelgruppe aus. Dies ist nützlich, wenn Sie über eine große Zahl von Labels verfügen, die Sie in Unter-Labels gruppieren möchten. Sie können beispielsweise die Labels Ihrer lizenzierten Anwendungen in einer Labelgruppe namens *Lizenzen* zusammenfassen. Labels erben außerdem sämtliche Einschränkungen der Gruppen, denen sie angehören.

3. Klicken Sie auf **Speichern**.

Verwandte Themen

Anwendungssteuerungslabel zu Geräten zuweisen

Label Labelgruppen zuweisen bzw. Labels von Labelgruppen entfernen

Labels können Gruppen zugewiesen und mit mehr als einer Labelgruppe verknüpft werden. Labels erben die Einschränkungen der Gruppen, denen sie angehören.

1. Rufen Sie die Liste *Labels* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste im Abschnitt **Startseite** auf **Label-Verwaltung**.
   c. Klicken Sie im Bereich für die Label-Verwaltung auf **Labels**.
2. Aktivieren Sie die Kontrollkästchen neben den Labels, die Sie einer Gruppe zuweisen möchten.
3. Klicken Sie auf **Aktion auswählen** > **Labelgruppen übernehmen** und wählen Sie dann die Labelgruppe aus, der Sie das Label zuweisen möchten.

   Labelgruppen übernehmen wird nur angezeigt, wenn sich in Ihrer Appliance Labelgruppen befinden.

   Der Name der Labelgruppe wird neben dem Namen des bzw. der ausgewählten Labels angezeigt.
4. Aktivieren Sie das Kontrollkästchen neben den Labels, die Sie aus einer Gruppe entfernen möchten.
5. Klicken Sie auf **Aktion auswählen** > **Labelgruppen entfernen** und wählen Sie dann die Labelgruppe aus, aus der Sie die Labels entfernen möchten.

   Labelgruppen entfernen wird nur angezeigt, wenn sich in Ihrer Appliance Labelgruppen befinden.

   Der Name der Labelgruppe wird nicht mehr neben dem Namen des bzw. der ausgewählten Labels angezeigt.

Labelgruppen löschen

Sie können Labelgruppen nur löschen, wenn diese keine Labels oder Untergruppen enthalten.

Wenn eine Labelgruppe Labels oder Untergruppen enthält, müssen Sie diese entfernen, bevor Sie die Gruppe löschen können.

1. Rufen Sie die Liste *Labels* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste im Abschnitt **Startseite** auf **Label-Verwaltung**.
   c. Klicken Sie im Bereich für die Label-Verwaltung auf **Labels**.
2. Wenn die Labelgruppe keine Labels oder Untergruppen enthält:
   a. Aktivieren Sie das Kontrollkästchen neben dem Namen der Gruppe.
   b. Wählen Sie **Aktion auswählen** > **Löschen** und klicken Sie dann zum Bestätigen auf **Ja**.

      Die Labelgruppe wird entfernt.
3. Wenn die Gruppe Labels oder Untergruppen enthält:
   a. Klicken Sie auf den Namen der Labelgruppe, um die Seite*Labelgruppen-Detail* anzuzeigen.
   b. Klicken Sie unten auf der Seite im Abschnitt *Elemente mit Label* auf die Schaltfläche **Hinzufügen**, um den Abschnitt *Labels* zu erweitern. +.

c. Klicken Sie auf den Namen eines Labels oder einer Labelgruppe, um die zugehörige Detailseite anzuzeigen.
d. Klicken Sie im Feld *Labelgruppe* auf **Bearbeiten**.
e. Klicken Sie im Fenster *Labelgruppe zuweisen* auf die Schaltfläche **Löschen** neben dem Label, das Sie entfernen möchten: 🗑.
f. Klicken Sie auf **OK** und anschließend auf **Speichern**.
g. Wenn Sie alle Labels und Untergruppen aus der Labelgruppe entfernt haben, aktivieren Sie auf der Seite *Labels* das Kontrollkästchen neben dem Namen der Labelgruppe.
h. Wählen Sie **Aktion auswählen** > **Löschen** und klicken Sie dann zum Bestätigen auf **Ja**.

Verwalten von LDAP-Labels

Sie verwalten LDAP-Labels im Abschnitt *Labels*.

LDAP-Label hinzufügen oder bearbeiten

Sie können LDAP-Labels nach Bedarf hinzufügen oder bearbeiten. Testen Sie LDAP-Labels, bevor Sie sie aktivieren.

1. Rufen Sie die Seite *LDAP-Labeldetail* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste im Abschnitt **Startseite** auf **Label-Verwaltung**.
   c. Klicken Sie im Bereich für die Label-Verwaltung auf **LDAP-Labels**.
   d. Führen Sie einen der folgenden Schritte aus, um die Seite *LDAP-Labeldetail* anzuzeigen:
   - Klicken Sie auf den Namen eines LDAP-Labels.
   - Wählen Sie **Aktion auswählen** > **Neu**.
2. Geben Sie die folgenden Informationen an:

Option	Beschreibung
Aktiviert	Aktivieren Sie die Ausführung des LDAP-Labels durch die Appliance. **HINWEIS:** Aktivieren Sie das Kontrollkästchen *Aktiviert* erst, nachdem Sie das LDAP-Label gestestet und sichergestellt haben, dass die LDAP-Kriterien korrekt sind und Labels wie erwartet angewendet werden.
Typ	Der Typ des LDAP-Labels. Es gibt zwei Arten von LDAP-Labels: • **Gerät**: Labels, die Gerätedatensätzen zugewiesen werden. Sie sind hilfreich, falls Sie Geräte automatisch nach Name, Beschreibung oder anderen LDAP-Kriterien gruppieren möchten. Wenn Geräte inventarisiert werden, wird diese Abfrage an den LDAP-Server gesendet, um festzustellen, ob Geräte LDAP-Attribute mit Werten

Option	Beschreibung
	enthalten, die den Filterkriterien der LDAP-Suche entsprechen. Wenn ein Ergebnis zurückgegeben wird, wird dem Gerät das im Feld *Verknüpfter Labelname* angegebene Label zugewiesen. Sie müssen in Gerätelabeln mindestens eine Variable für die Appliance angeben, z. B. `KBOX_COMPUTER_NAME`, damit das LDAP-Label einem Gerät zugewiesen werden kann. Während der LDAP-Labelverarbeitung wird die Variable zum Vergleich des Werts eines Attributs im LDAP-Verzeichnis verwendet, um festzustellen, ob zwischen dem LDAP-Objekt und einem Appliance-Objekt Beziehungen bestehen. Siehe LDAP-Variable. • **Benutzer**: Labels, die Benutzerdatensätzen zugewiesen werden. Sie sind hilfreich, falls Sie Benutzer automatisch nach Domäne, Standort, Budgetcode oder anderen LDAP-Kriterien gruppieren möchten. LDAP-Labels werden auf Benutzerdatensätze angewendet oder aus diesen entfernt, wenn Benutzer manuell oder nach einem Zeitplan in die Appliance importiert werden. Sie können Benutzervariablen, z. B. `KBOX_USER_NAME`, in Benutzerlabels verwenden. Während der LDAP-Labelverarbeitung wird die Variable zum Vergleich des Werts eines Attributs im LDAP-Verzeichnis verwendet, um festzustellen, ob zwischen dem LDAP-Objekt und einem Appliance-Objekt Beziehungen bestehen. Siehe LDAP-Variable. **TIPP:** Um ein Label zu testen, ersetzen Sie die `KBOX_`-Variablen durch entsprechende Werte für Ihre Umgebung und wählen dann **Testen**.
Verknüpftes Label	Das mit diesem LDAP-Label zu verknüpfende manuelle Label oder Containerlabel. Jedes LDAP-Label muss über ein verknüpftes Label verfügen.
Beschreibung des verknüpften Labels	Hinweise vom gewählten Label im Feld *Verknüpfter Labelname*
Server	Die IP-Adresse oder der Hostname des LDAP-Servers. Wenn die IP-Adresse ungültig ist, wartet die Appliance auf ein Timeout, sodass bei der Verwendung der LDAP-Authentifizierung Verzögerungen bei der Anmeldung entstehen. **HINWEIS:** Wenn die Verbindung über SSL hergestellt wird, verwenden Sie die IP-Adresse oder den Hostnamen. Beispiel: ldaps://hostname.

Option	Beschreibung
Port	Die LDAP-Port-Nummer, in der Regel 389 (LDAP) oder 636 (sicheres LDAP).

Basis-DN	Die Kriterien für die Suche nach Konten.
	Diese Kriterien legen einen Standort oder Container in der LDAP- oder Active Directory-Struktur fest und sollten alle Benutzer umfassen, die authentifiziert werden sollen. Geben Sie eine genaue Kombination aus OUs, DCs oder CNs an, die Ihren Kriterien entsprechen, die von links (sehr genau) bis rechts (sehr allgemein) reichen. Dieser Pfad führt beispielsweise zum Container mit den Benutzern, die Sie authentifizieren müssen:
	`OU=end_users,`
	`DC=Unternehmen, DC=com.`

Erweiterte Suche	Der Suchfilter. Beispiel: `(&(sAMAccountName=KBOX_USERNAME)(memberOf=CN=financial,DC=example,DC=com))`
Anmeldeinformationen	Die LDAP-Anmeldeinformationen, die erforderlich sind, damit die Appliance sich beim LDAP-Server anmelden und Konten lesen kann. Wählen Sie aus der Liste aus, oder erstellen Sie neue LDAP-Anmeldeinformationen. Weitere Informationen zu LDAP-Anmeldeinformationen finden Sie unter Hinzufügen und Bearbeiten von LDAP-Benutzer-/Kennwort-Anmeldeinformationen.

Wenn Sie nicht genau wissen, welche Informationen Sie für den *Basis-DN* und die *Erweiterte Suche* bereitstellen müssen, verwenden Sie den LDAP-Browser. Siehe LDAP-Browser verwenden.

HINWEIS: Ausschlussfilter weisen folgendes Format auf: `(!(sAMAccountName=David))`. Anders formatierte Ausschlusswerte verursachen einen Fehler.

3. Klicken Sie auf die Schaltfläche **Testen**, um das neue Label zu testen. Ändern Sie ggf. die Parameter des Labels und testen Sie es erneut.
4. Wenn das LDAP-Label zur Verwendung bereit ist, aktivieren Sie das Kontrollkästchen *Aktiviert*. Speichern Sie andernfalls das Label, ohne es zu aktivieren.
5. Klicken Sie auf **Speichern**.

Verwandte Themen

LDAP-Browser verwenden

LDAP-Label aktivieren

Nachdem Sie ein LDAP-Label hinzugefügt und getestet haben, können Sie es aktivieren. Aktivierte Geräte-LDAP-Labels werden an den LDAP-Server gesendet, wenn sich Geräte bei der Appliance anmelden. Aktivierte Benutzer-LDAP-Labels werden an den LDAP-Server gesendet, wenn Benutzer manuell oder nach einem Zeitplan importiert werden.

Sie wollen ein LDAP-Label hinzufügen und testen. Siehe LDAP-Label hinzufügen oder bearbeiten.

1. Rufen Sie die Seite *LDAP-Labeldetail* auf:

a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
b. Klicken Sie in der linken Navigationsleiste im Abschnitt **Startseite** auf **Label-Verwaltung**.
c. Klicken Sie im Bereich für die Label-Verwaltung auf **LDAP-Labels**.
d. Klicken Sie auf den Namen eines LDAP-Labels.

2. Aktivieren Sie das Kontrollkästchen *Aktiviert*.
3. Klicken Sie auf **Speichern**.

LDAP-Label löschen

Durch das Löschen eines LDAP-Labels werden die Kriterien, die dem LDAP-Label zugeordnet sind, entfernt, es werden jedoch keine anderen Labels gelöscht, die dem LDAP-Label zugewiesen sind.

1. Rufen Sie die Seite *LDAP-Labeldetail* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste im Abschnitt **Startseite** auf **Label-Verwaltung**.
   c. Klicken Sie im Bereich für die Label-Verwaltung auf **LDAP-Labels**.
2. Aktivieren Sie das Kontrollkästchen neben den gewünschten LDAP-Labels.
3. Wählen Sie **Aktion auswählen > Löschen** und klicken Sie dann zum Bestätigen auf **Ja**.

LDAP-Browser verwenden

Der LDAP-Browser ermöglicht es Ihnen, die Daten auf einem LDAP-Server zu suchen und zu durchsuchen, wie zum Beispiel die eines Active Directory Servers.

Zur Verwendung des LDAP-Browsers benötigen Sie den Bindungs-DN und das PDAP-Kennwort, um sich beim LDAP-Server anmelden zu können.

Der LDAP-Browser kann nützlich sein, wenn Sie für LDAP-Abfragen Informationen in die Felder *Suchbasis-DN* und *Suchfilter* eingeben müssen.

1. Rufen Sie den *LDAP-Browser* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste im Abschnitt **Startseite** auf **Label-Verwaltung**.
   c. Klicken Sie im Bereich für die Label-Verwaltung auf **LDAP-Browser**.
2. Geben Sie Einstellungen für den *LDAP-Server* an:

Option	Beschreibung
IP-Adresse oder Hostname	Die IP-Adresse oder der Hostname des LDAP-Servers. Wenn die IP-Adresse ungültig ist, wartet die Appliance auf ein Timeout, sodass bei der Verwendung der LDAP-Authentifizierung Verzögerungen bei der Anmeldung entstehen.

Option	Beschreibung
	HINWEIS: Wenn die Verbindung über SSL hergestellt wird, verwenden Sie die IP-Adresse oder den Hostnamen. Beispiel: ldaps://hostname.
Port	Die LDAP-Port-Nummer, in der Regel 389 (LDAP) oder 636 (sicheres LDAP).
Anmeldung	Die Anmeldeinformationen, die erforderlich sind, damit die Appliance sich beim LDAP-Server anmelden und Konten lesen kann. Beispiel: `LDAP Login:CN=service_account,CN=Users, DC=Unternehmen, DC=com`. Wenn Benutzername und Kennwort nicht angegeben werden, wird der Struktur-Lookup nicht ausgeführt. Jedes LDAP-Label kann eine Verbindung zu einem anderen LDAP- oder Active Directory-Server herstellen.
Kennwort	Das Kennwort des Kontos, mit dem sich die Appliance beim LDAP-Server anmeldet.

3. Klicken Sie auf **Testen**.

   Nach erfolgreicher Verbindung mit einem LDAP-Server wird die Schaltfläche **Weiter** aktiviert.

   Überprüfen Sie im Falle eines Fehlers Folgendes:

   - Die IP-Adresse bzw. der Hostname sind korrekt.
   - Der LDAP-Server wird ausgeführt.
   - Die Anmeldeinformationen sind korrekt.
4. Klicken Sie auf **Weiter**.

   Das Fenster *Suche einengen* wird angezeigt.
5. Geben Sie einen Suchfilter an, um die Anzahl der angezeigten Ergebnisse am unteren Rand des Bildschirms einzuschränken.

Option	Beschreibung
LDAP - einfache Suche	Geben Sie die Zeichenfolge ein, nach der Sie suchen möchten.
Suche in	Geben Sie an, ob Sie nach indizierten oder nicht indizierten Feldern suchen möchten, indem Sie die entsprechende Option nach Bedarf wählen.
Andere Attribute	Geben Sie eine durch Kommas getrennte Liste der Active-Directory-Felder ein, nach denen Sie suchen möchten.

Option	Beschreibung
	HINWEIS: Die Suche wird nicht prüfen, ob die angegebenen Felder tatsächlich im Active Directory vorhanden sind.

6. Klicken Sie auf **Start**.

   Die Suchergebnisse werden im unteren Bereich des Bildschirms auf der linken Seite angezeigt.
7. Klicken Sie auf einen untergeordneten Knoten, um dessen Attribute anzuzeigen.

   Die Attribute werden im rechten Bereich angezeigt.

Konfigurieren von Benutzerkonten, LDAP-Authentifizierung und SSO

Sie können Benutzerkonten konfigurieren und verwalten, Benutzer mithilfe von LDAP-Informationen authentifizieren und die einmalige Anmeldung (SSO, Single Sign-On) für Benutzer aktivieren.

Informationen zu Benutzerkonten und Benutzerauthentifizierung

Benutzerkonten können in der Appliance erstellt und verwaltet werden. Benutzer, die mit diesen Konten auf die **Administratorkonsole** und **Benutzerkonsole** zugreifen, werden als **lokal authentifiziert** bezeichnet.

Alternativ zur lokalen Authentifizierung können Sie eine externe Authentifizierung über einen externen LDAP-Server einrichten. Siehe Verwenden eines LDAP-Servers zur Benutzerauthentifizierung.

Es gibt folgende lokal authentifizierte Benutzerkontotypen:

- **Benutzerkonten auf Systemebene**. Konten, die es Benutzern ermöglichen, sich bei der **Systemverwaltungskonsole** anzumelden, um Appliance-Einstellungen wie den Hostnamen oder die Netzwerkeinstellungen zu verwalten. Benutzerkonten auf Systemebene beinhalten das standardmäßige **admin**-Konto für die Appliance. Diese Konten ermöglichen darüber hinaus den Zugriff auf Komponenten auf Organisationsebene (adminui) und die **Benutzerkonsole**. Siehe Verwalten von Benutzerkonten auf Systemebene.
- **Organisationsbenutzerkonten**. Konten, die es Benutzern ermöglichen, sich bei der Organisationsebene der **Administratorkonsole** (Administratorkonsole) anzumelden, um organisationsspezifische Komponenten zu verwalten. Diese Komponenten können je nach Benutzerrolle Inventar, Assets, Verteilung, Skripterstellung, Sicherheit, Service Desk und **Benutzerkonsole** umfassen. Siehe Verwalten von Organisationsbenutzerkonten.

Informationen zu Gebietsschema-Einstellungen

Gebietsschema-Einstellungen legen die Sprache für den Text der Benutzeroberflächen fest. Sie können die Gebietsschema-Einstellungen für die **Befehlszeilenkonsole**, **Administratorkonsole** und **Benutzerkonsole** auswählen.

Siehe Konfigurieren der Gebietsschema-Einstellungen.

Verwalten von Benutzerkonten auf Systemebene

Benutzerkonten auf Systemebene ermöglichen es Benutzern, sich bei der **Systemverwaltungskonsole** anzumelden, um Appliance-Einstellungen wie den Appliance-Hostnamen oder die -Netzwerkeinstellungen zu verwalten. Benutzerkonten auf Systemebene authentifizieren Benutzer lokal auf der Appliance.

Informationen zur Verwendung eines LDAP-Servers für die Benutzerauthentifizierung finden Sie unter Verwenden eines LDAP-Servers zur Benutzerauthentifizierung.

HINWEIS: Das Standard-**Administratorkonto** kann nicht gelöscht werden. Sie können den Benutzernamen des **Administratorkontos** ändern oder auf der Appliance deaktivieren (LDAP- oder SAML-Konfiguration erforderlich). Sie können auch das Kennwort für das **Administratorkonto** ändern. Siehe Benutzerkonten auf Systemebene hinzufügen oder bearbeiten. Wenn auf Ihrer Appliance die Organisationskomponente aktiviert ist oder wenn Sie mehrere Appliances der K Serie verknüpfen möchten, gehen Sie beim Ändern der Anmeldedaten und des Kennworts für das **Administratorkonto** vorsichtig vor. Die Anmeldenamen und Kennwörter für das **Administratorkonto** müssen für alle verknüpften Appliances und Organisationen gleich sein, wenn Sie über die Dropdown-Liste oben rechts in der **Systemverwaltungskonsole** zwischen diesen wechseln möchten. In der Dropdown-Liste werden nur die Appliances und Organisationen angezeigt, deren Anmeldenamen und Kennwörter für das **Administratorkonto** gleich sind.

HINWEIS: Siehe Schnellen Wechsel von Organisationen und verknüpften Appliance aktivieren.

Benutzerkonten auf Systemebene hinzufügen oder bearbeiten

Sie können Benutzerkonten auf Systemebene nach Bedarf hinzufügen oder bearbeiten. Diese Konten ermöglichen es Benutzern, sich an der **Systemverwaltungskonsole** anzumelden, um Appliance-Einstellungen zu verwalten.

Wenn auf der Appliance die Organisationskomponente aktiviert wurde, können Sie auch organisationsspezifische Benutzerkonten hinzufügen oder bearbeiten. Siehe Verwalten von Organisationsbenutzerkonten.

HINWEIS: Das Standard-**Administratorkonto** kann nicht gelöscht werden. Sie können den Benutzernamen des **Administratorkontos** ändern oder auf der Appliance deaktivieren (LDAP- oder SAML-Konfiguration erforderlich). Sie können auch das Kennwort für das **Administratorkonto** ändern. Wenn auf Ihrer Appliance die Organisationskomponente aktiviert ist oder wenn Sie mehrere Appliances der K Serie verknüpfen möchten, gehen Sie beim Ändern der Anmeldedaten und des Kennworts für das **Administratorkonto** vorsichtig vor. Die Anmeldenamen und Kennwörter für das **Administratorkonto** müssen für alle verknüpften Appliances und Organisationen gleich sein, wenn Sie über die Dropdown-Liste oben rechts in der **Systemverwaltungskonsole** zwischen diesen wechseln möchten. In der Dropdown-Liste werden nur die Appliances und Organisationen angezeigt, deren Anmeldenamen und Kennwörter für das **Administratorkonto** gleich sind.

HINWEIS: Siehe Schnellen Wechsel von Organisationen und verknüpften Appliance aktivieren.

1. Rufen Sie die Seite *Administratordetail* auf.
   a. Melden Sie sich bei der Systemadministratorkonsole der Appliance an: `http://`**appliance_hostname**`/system`. Oder wählen Sie in der Dropdown-Liste rechts oben auf der Seite den Eintrag **System** aus.
   b. Klicken Sie auf der linken Navigationsleiste auf **Einstellungen** und anschließend auf **Administratoren**.

c. Führen Sie eine der folgenden Aktionen aus, um die Seite *Administratordetail* anzuzeigen:

- Auf den Namen eines Administrators klicken
- Wählen Sie **Aktion auswählen** > **Neu**.

2. Geben Sie die Benutzerinformationen ein oder ändern Sie sie.

Option	Beschreibung
Anmeldung	(Erforderlich) Der Name, den der Benutzer auf der Anmeldeseite ins Feld *Anmelde-ID* eingibt. Wenn Sie das Standard-*Administratorkonto* bearbeiten, können Sie den Anmeldenamen ändern. Gehen Sie jedoch vorsichtig vor, wenn Sie den Anmeldenamen und das Kennwort des *Administratorkontos* ändern. Die Anmeldenamen und Kennwörter für das *Administratorkonto* müssen für alle verknüpften Appliances und Organisationen gleich sein, wenn Sie über die Dropdown-Liste oben rechts in der **Systemverwaltungskonsole** zwischen diesen wechseln möchten. In der Dropdown-Liste werden nur die Appliances und Organisationen angezeigt, deren Anmeldenamen und Kennwörter für das *Administratorkonto* gleich sind.
Name	Der vollständige Name des Benutzers.
Primäre E-Mail-Adresse	Die primäre E-Mail-Adresse des Benutzers.
Zusätzliche E-Mail-Adressen	Alle weiteren E-Mail-Adressen, die dem Benutzer zugeordnet sind.
Domain	Die Active Directory-Domäne, die dem Benutzer zugewiesen wurde.
Budgetcode	Der Code der Finanzabteilung, der dem Benutzer zugewiesen wurde.
Standort	Der Name des Standorts oder Gebäudes, an/in dem sich der Benutzer befindet.
Telefon (geschäftlich), Telefon (privat), Mobiltelefon und Pager	Die Telefonnummern des Benutzers.
Benutzerdefiniert 1-4	Alle zusätzlichen Informationen über den Benutzer oder sein Konto.
„Kennwort“ und „Kennwort bestätigen“	(Erforderlich) Das Kennwort, das der Benutzer zur Anmeldung eingibt Wenn auf Ihrer Appliance die Organisationskomponente aktiviert ist oder Sie mehrere Appliances der K-Serie verknüpfen möchten, sollten Sie beim Ändern des Kennworts für das **admin**-Konto vorsichtig vorgehen. Die **admin**-Kennwörter für die Systemebene, für Organisationen und für verknüpfte Appliances müssen gleich sein, wenn Sie über die Dropdown-Liste oben rechts

Option	Beschreibung
	in der **Administratorkonsole** zwischen diesen wechseln möchten. In der Dropdown-Liste werden nur die Organisationen und Appliances angezeigt, deren Kennwörter für das Administratorkonto gleich sind.
Rolle	(Erforderlich) Rollen werden Benutzerkonten zugewiesen, um den Zugriff auf die **Administratorkonsole** und **Benutzerkonsole** zu steuern. Standardadministratorrollen sind: • **Administrator**: Dieser Benutzer kann sich bei der **Administratorkonsole** anmelden und auf alle Funktionen zugreifen. • **Administrator mit Leseberechtigung**: Dieser Benutzer kann sich bei der **Administratorkonsole** anmelden, jedoch keine Einstellungen ändern. Die Rolle des Standard-Administratorkontos kann nicht geändert werden.
Als Standard festlegen	Wählen Sie diese Option, wenn Sie möchten, dass die ausgewählten Rolle die Standardrolle für neue Benutzer wird.
Gebietsschema	Das Gebietsschema, das für die **Administratorkonsole** und **Benutzerkonsole** für den Benutzer verwendet werden soll. Das Gebietsschema des Standard-Administratorkontos kann nicht geändert werden.
KACE Sicherheitsbenachrichtigungen aktivieren	Aktivieren Sie Quest, um Sicherheitsbenachrichtigungen an die E-Mail-Adresse des Administrators zu senden. Diese Funktion ist nur für Administratorkonten auf Systemebene verfügbar. Sie steht nicht für Administratorkonten auf Verwaltungsebene oder Benutzerkonten ohne Administratorberechtigungen zur Verfügung.
KACE Vertriebs- und Marketingbenachrichtigungen aktivieren	Aktivieren Sie Quest, um Vertriebs- und Marketingbenachrichtigungen an die E-Mail-Adresse des Administrators zu senden. Diese Funktion ist nur für Administratorkonten auf Systemebene, aber nicht für Administratorkonten auf Verwaltungsebene oder Benutzerkonten ohne Administratorberechtigungen verfügbar.

3. Klicken Sie auf **Speichern**.

E-Mail-Benachrichtigungen des Appliance-Administrators verwalten

Quest benachrichtigt Appliance-Administratoren per E-Mail über Sicherheitsprobleme und über Vertriebs- und Marketingmöglichkeiten. Sie können die E-Mail-Benachrichtigungen für Administratorkonten auf Systemebene (Appliance) aktivieren oder deaktivieren.

E-Mail-Benachrichtigungen sind nur für Appliance-Administratorkonten verfügbar. Für Benutzer ohne Administratorberechtigungen sind keine Benachrichtigungen verfügbar. Wenn die Organisationskomponente auf Ihrer Appliance aktiviert ist, sind für Administratorkonten in Organisationen auf Verwaltungsebene keine Benachrichtigungen verfügbar.

1. Rufen Sie die Seite *Benutzerdetails* oder *Administratordetail* auf:

   So rufen Sie die Seite *Benutzerdetails* auf:

   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.

   b. Klicken Sie auf der linken Navigationsleiste auf **Einstellungen** und anschließend auf **Benutzer**.

   c. Führen Sie eine der folgenden Aktionen aus, um die Seite *Benutzerdetails* anzuzeigen:

   - Klicken Sie auf den Namen eines Benutzers.
   - Wählen Sie **Aktion auswählen** > **Neu**.

   So rufen Sie die Seite *Administratordetail* auf:

   a. Melden Sie sich bei der Systemadministratorkonsole der Appliance an: `http://`**appliance_hostname**`/system`. Oder wählen Sie in der Dropdown-Liste rechts oben auf der Seite den Eintrag **System** aus.

   b. Klicken Sie auf der linken Navigationsleiste auf **Einstellungen** und anschließend auf **Administratoren**.

   c. Führen Sie eine der folgenden Aktionen aus, um die Seite *Administratordetail* anzuzeigen:

   - Auf den Namen eines Administrators klicken
   - Wählen Sie **Aktion auswählen** > **Neu**.

2. Überprüfen Sie die Benutzerinformationen, die E-Mail-Adresse und die Rolle.

   HINWEIS: Zum Aktivieren von Benachrichtigungen muss der Benutzer über eine Appliance-Administratorrolle verfügen.

3. Aktivieren bzw. deaktivieren Sie unten im Formular die Kontrollkästchen neben den Benachrichtigungsfeldern, um E-Mail-Benachrichtigungen für den Administrator ein- bzw. auszuschalten.

Option	Beschreibung
KACE Sicherheitsbenachrichtigungen aktivieren	Aktivieren Sie Quest, um Sicherheitsbenachrichtigungen an die E-Mail-Adresse des Administrators zu senden. Diese Funktion ist nur für Administratorkonten auf Systemebene verfügbar. Sie steht nicht für Administratorkonten auf Verwaltungsebene oder Benutzerkonten ohne Administratorberechtigungen zur Verfügung.
KACE Vertriebs- und Marketingbenachrichtigungen aktivieren	Aktivieren Sie Quest, um Vertriebs- und Marketingbenachrichtigungen an die E-Mail-Adresse

Option	Beschreibung
	des Administrators zu senden. Diese Funktion ist nur für Administratorkonten auf Systemebene, aber nicht für Administratorkonten auf Verwaltungsebene oder Benutzerkonten ohne Administratorberechtigungen verfügbar.

4. Klicken Sie auf **Speichern**.

Benutzerkonten auf Systemebene löschen

Wenn die Organisationskomponente in Ihrer Appliance aktiviert ist, können Sie Benutzerkonten auf Systemebene löschen. Diese Option ist nur dann verfügbar, wenn in der Appliance die Organisationskomponente aktiviert ist.

Wenn die Organisationskomponente auf Ihrer Appliance nicht aktiviert ist, befolgen Sie die Anweisungen in Verwalten von Organisationsbenutzerkonten.

HINWEIS: Das Standard-*Administratorkonto* kann nicht gelöscht werden.

1. Rufen Sie die Liste *Administratoren* auf:
   a. Melden Sie sich bei der Systemadministratorkonsole der Appliance an: `http://`**appliance_hostname**`/system`. Oder wählen Sie in der Dropdown-Liste rechts oben auf der Seite den Eintrag **System** aus.
   b. Klicken Sie auf der linken Navigationsleiste auf **Einstellungen** und anschließend auf **Administratoren**.
2. Aktivieren Sie das Kontrollkästchen neben einem oder mehreren Konten.
3. Wählen Sie **Aktion auswählen** > **Löschen** und klicken Sie dann zum Bestätigen auf **Ja**.

Verwalten von Organisationsbenutzerkonten

Organisationsbenutzerkonten stellen die Anmeldeinformationen bereit, mit denen sich Benutzer auf Grundlage der ihrem Konto zugewiesenen Benutzerrolle bei Komponenten wie der **Administratorkonsole** oder der **Benutzerkonsole** anmelden oder auf diese zugreifen können. Sie können Benutzerrollen und -konten nach Bedarf hinzufügen oder bearbeiten.

Organisationsbenutzerkonten authentifizieren Benutzer lokal auf der Appliance. Informationen zur Verwendung eines LDAP-Servers für die Benutzerauthentifizierung finden Sie unter Verwenden eines LDAP-Servers zur Benutzerauthentifizierung.

Benutzerrollen hinzufügen oder bearbeiten

Benutzerrollen werden Benutzerkonten zugewiesen, um den Zugriff auf die **Administratorkonsole** und **Benutzerkonsole** zu steuern. Sie können Benutzerrollen nach Bedarf hinzufügen oder bearbeiten.

Sie können jedoch nicht die vordefinierten Rollen ändern: Administrator, Kein Zugriff, Administrator mit Leseberechtigung und Benutzer.

Wenn die Organisationskomponente auf Ihrer Appliance aktiviert ist, hängen die für Benutzerrollen verfügbaren Berechtigungen von der Organisationsrolle ab, die der Organisation zugewiesen ist. Siehe Verwalten von Organisationsrollen und Benutzerrollen.

1. Rufen Sie die Seite *Rollendetail* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen*

aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.

b. Klicken Sie auf der linken Navigationsleiste auf **Einstellungen** und anschließend auf **Rollen**.

c. Führen Sie eine der folgenden Aktionen aus, um die Seite *Rollendetail* anzuzeigen:

- Klicken Sie auf den Namen einer Rolle.
- Wählen Sie **Aktion auswählen** > **Neu**.

2. Geben Sie im Feld *Name* einen Namen ein, beispielsweise Service Desk-Mitarbeiter.

   Sie können den Namen von vordefinierten Rollen nicht ändern.

3. Wenn diese Rolle eine Standardrolle für neue Rolle sein soll, wählen Sie das Kontrollkästchen **Standardrolle für neue Benutzer** aus.

4. Geben Sie im Feld *Beschreibung* eine Kurzbeschreibung der Rolle ein, beispielsweise Wird verwendet für Service Desk-Administratoren.

   Diese Beschreibung wird in der Liste *Rollen* angezeigt. Sie können die Beschreibung von vordefinierten Rollen nicht ändern.

5. Legen Sie Berechtigungen für die Administratorkonsole fest.

   a. Klicken Sie unter *Berechtigungen für Administratorkonsole* auf die Schaltfläche **Alle erweitern**.

   b. Legen Sie Berechtigungen für jede Komponente wie zutreffend fest.

6. Legen Sie Berechtigungen für die Benutzerkonsole fest.

   a. Klicken Sie unter *Endbenutzer-Konsolenberechtigungen* auf **Benutzerkonsole**, um die Liste der Berechtigungen zu erweitern.

   b. Legen Sie Berechtigungen für jede Komponente wie zutreffend fest.

7. Geben Sie unter *Gerätebereich* die Geräte an, zu denen Sie Vollzugriff mit dieser Rolle erteilen möchten.

   Rollenbasierter Zugriff ermöglicht Administratoren basierend auf den Geräten, die mit ihrer Benutzerrolle verknüpft sind, die Aktionen von Benutzern zu beschränken. Sie können einem Benutzer (*Benutzer mit eingeschränkten Zugriffsrechten*) den Zugriff auf alle Geräte mit dieser bestimmten Rolle gestatten oder nur auf ausgewählte Geräte, die mit einem Label verknüpft sind.

   TIPP: Labels sind Container zum Organisieren und Kategorisieren von Elementen wie etwa Geräten, sodass diese als Gruppe verwaltet werden können. Weitere Informationen zu Labels finden Sie unter Informationen zu den Labels.

   TIPP: Wenn ein Smart Label mit einer Rolle verknüpft ist, wird dies auf der Liste *Smart Labels* in der Spalte *Name* angegeben.

   - Zum Gewähren von Zugriff auf alle Geräte in der Appliance oder Organisation (sofern zutreffend) wählen Sie **Alle Geräte**.
   - Zum Gewähren von Zugriff nur auf Geräte, die mit einem bestimmten Label verknüpft sind, klicken Sie auf **Verknüpfte Labels verwalten** und wählen Sie ein Label nach Bedarf.

8. Klicken Sie auf **Speichern**.

Die Seite *Rollen* wird angezeigt. Wenn sich ein Benutzer anmeldet, der dieser Rolle zugeordnet ist, werden in der Leiste für Appliance-Komponenten die verfügbaren Funktionen angezeigt.

Benutzerrollen löschen

Sie können Benutzerrollen löschen, sofern diese nicht Benutzern zugewiesen sind und es sich bei den Rollen nicht um vordefinierte Benutzerrollen handelt. Wenn die Organisationskomponente auf Ihrer Appliance aktiviert ist, löschen Sie Benutzerrollen separat für jede Organisation.

HINWEIS: Sie können Benutzerrollen löschen, die einem oder mehreren Labels zugeordnet sind.

1. Rufen Sie die Liste *Rollen* auf:

a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.

b. Klicken Sie auf der linken Navigationsleiste auf **Einstellungen** und anschließend auf **Rollen**.

2. Aktivieren Sie das Kontrollkästchen neben mindestens einer Rolle.
3. Wählen Sie **Aktion auswählen** > **Löschen** und klicken Sie dann zum Bestätigen auf **Ja**.

Organisationsbenutzerkonten hinzufügen oder bearbeiten

Sie können Benutzerkonten auf Organisationsebene hinzufügen oder bearbeiten. Wenn die Organisationskomponente auf Ihrer Appliance aktiviert ist, können Sie Benutzerkonten für jede Organisation separat hinzufügen und bearbeiten.

1. Rufen Sie die Seite *Benutzerdetails* auf.

   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.

   b. Klicken Sie auf der linken Navigationsleiste auf **Einstellungen** und anschließend auf **Benutzer**.

   c. Führen Sie eine der folgenden Aktionen aus, um die Seite *Benutzerdetails* anzuzeigen:

   - Klicken Sie auf den Namen eines Benutzers.
   - Wählen Sie **Aktion auswählen** > **Neu**.

   HINWEIS: Es darf maximal 50 Organisation in Ihrem System geben. Jeder Versuch weitere Organisationen zu erstellen, resultiert in einer Fehlermeldung.

2. Fügen Sie die folgenden Informationen hinzu oder bearbeiten diese:

Option	Beschreibung
Anmeldung	(Erforderlich) Der Name, den der Benutzer auf der Anmeldeseite ins Feld *Anmelde-ID* eingibt. Wenn Sie das Standard-*Administratorkonto* bearbeiten, können Sie den Anmeldenamen ändern. Gehen Sie jedoch vorsichtig vor, wenn Sie den Anmeldenamen und das Kennwort des *Administratorkontos* ändern. Die Anmeldenamen und Kennwörter für das *Administratorkonto* müssen für alle verknüpften Appliances und Organisationen gleich sein, wenn Sie über die Dropdown-Liste oben rechts in der **Administratorkonsole** zwischen diesen wechseln möchten. In der Dropdown-Liste werden nur die Appliances und Organisationen angezeigt, deren Anmeldenamen und Kennwörter für das *Administratorkonto* gleich sind.
Name	Der vollständige Name des Benutzers.
E-Mail	Die primäre E-Mail-Adresse des Benutzers.
Zusätzliche E-Mail-Adressen	Ein oder mehrere zusätzliche E-Mail-Adressen auf die der Benutzer Zugriff hat. Trennen Sie mehrere Einträge durch Kommata.

Option	Beschreibung
Domain	Die Active Directory-Domäne, die dem Benutzer zugewiesen wurde.
Budgetcode	Der Code der Finanzabteilung, der dem Benutzer zugewiesen wurde.
Standort	Der Name des Standorts oder Gebäudes, an/in dem sich der Benutzer befindet. Klicken Sie auf einen in der Drop-Down-Liste angezeigten Standort und wählen Sie diesen aus.
Telefon (geschäftlich), Telefon (privat), Mobiltelefon und Pager	Die Telefonnummern des Benutzers.
Benutzerdefiniert 1-4	Alle zusätzlichen Informationen über den Benutzer oder sein Konto.
„Kennwort“ und „Kennwort bestätigen“	(Erforderlich) Das Kennwort, das der Benutzer zur Anmeldung eingibt
Rolle	(Erforderlich) Die Rolle, die dem Benutzer zugewiesen wurde. Rollen werden Benutzerkonten zugewiesen, um den Zugriff auf die **Administratorkonsole** und **Benutzerkonsole** zu steuern. Standardsystemrollen sind: • **Administrator**: Dieser Benutzer kann sich bei der **Administratorkonsole** anmelden und auf alle Funktionen zugreifen. • **Administrator mit Leseberechtigung**: Dieser Benutzer kann sich bei der **Administratorkonsole** anmelden, jedoch keine Einstellungen ändern. • **Nur Administratorkonsole**: Dieser Benutzer kann sich nur bei der **Administratorkonsole** anmelden. • **Kein Zugriff**: Der Benutzer kann sich nicht bei der **Administratorkonsole** oder **Benutzerkonsole** anmelden. Die Rolle des Standard-Administratorkontos kann nicht geändert werden.
Gebietsschema	Gebietsschema, das angezeigt wird, wenn sich der Benutzer bei der **Administratorkonsole** oder der **Benutzerkonsole** anmeldet.
Zuweisen zu Label	Das Label, das dem Benutzer zugewiesen wurde.
Standardwarteschlange	Die Warteschlange, die standardmäßig für von dem Benutzer gesendete Service-Desk-Tickets verwendet wird.

Option	Beschreibung
Mobilgerätezugriff	Aktiviert bzw. deaktiviert den Mobilgerätezugriff des Benutzers. Der Mobilgerätezugriff ermöglicht die Interaktion mit der Appliance mithilfe der KACE GO-App für Smartphones und Tablets mit iOS und Android. Administratoren können mithilfe der App auf Service Desk-, Inventar- und Anwendungsbereitstellungsfunktionen zugreifen. **HINWEIS:** Dieses Feld ist verfügbar, wenn der Mobilgerätezugriff auf der Appliance aktiviert ist. Siehe Konfigurieren des Mobilgerätezugriffs.
Service-Desk-Tickets	(Schreibgeschützt) Links zu vom Benutzer erstellten Tickets.
Zugehörige Assets	(Schreibgeschützt) Assets, die dem Benutzer zugewiesen sind. Die liste zeigt für jeden Benutzer den Asset-Name, seinen Typ (beispielsweise Software oder Gerät) und (gegebenenfalls) den Asset-Subtyp. Sie können die Liste wie gewünscht nach Spaltenüberschriften sortieren.
Zugewiesene Geräte	Geräte, die dem Benutzer zugewiesen sind. Die Liste zeigt für jeden Benutzer den Gerätenamen und Subtyp (sofern zutreffend) an und gibt an, ob das Gerät das primäre Gerät des Benutzers ist. Sie können die Liste wie gewünscht nach Spaltenüberschriften sortieren. Weisen Sie einem Benutzer ein Gerät zu, indem Sie auf + klicken und ein Asset wählen. Wenn Sie ein Gerät auswählen, das bereits einem anderen Benutzer zugewiesen, verschiebt sich das Besitzrecht an dem Gerät auf diesen Benutzer. Das erste dem Benutzer zugewiesene Gerät wird standardmäßig das primäre Gerät. Wenn einem Benutzer mehrere Geräte zugewiesen werden, kann ein beliebiges Gerät als primäres Gerät festgelegt werden.

3. Klicken Sie auf **Speichern**.

Verwandte Themen

Benutzerrollen hinzufügen oder bearbeiten

Konfigurieren der Gebietsschema-Einstellungen

Informationen zu den Labels

Konfigurieren des Mobilgerätezugriffs

Benutzerinformationen anpassen

Sie können die in Benutzerkonten zur Verfügung stehenden benutzerdefinierten Felder nach Bedarf ändern.

Jedes Benutzerkonto verfügt über einen Satz benutzerdefinierter Felder. Sie können diese Felder bearbeiten, sodass diese enthalten sinnvolle benutzerspezifische Daten enthalten, z. B. ihre Badge-Nummer.

1. Rufen Sie die Seite *Benutzerdetails* auf.
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie auf der linken Navigationsleiste auf **Einstellungen** und anschließend auf **Benutzer**.
   c. Wählen Sie **Aktion auswählen** > **Neu**, um die Seite *Benutzerdetail* zu öffnen.
2. Klicken Sie auf der Seite *Benutzerdetail* auf *Zusätzliche Felder anpassen*.

   Die Seite *Benutzerdefinierte Felder* wird angezeigt.
3. Für jedes benutzerdefinierte Feld, können Sie Folgendes festlegen:

Option	Beschreibung
Feldname	Name des benutzerdefinierten Felds.
Erforderlich	Anzeige, ob das Feld erforderlich ist.
Standardwert	Der Standardwert.

4. Die Erfassung von benutzerdefinierten Feldern nach Bedarf, unter Verwendung der zur Verfügung stehenden Steuerelemente, verwalten.
5. Klicken Sie auf **Speichern**.

Benutzerkonten archivieren

Wenn Benutzer von Ihrem System entfernt werden, haben Sie die Option, ihre Konten vor der Löschung zu archivieren.

Um Benutzerkonten zu archivieren, muss die Archivierung auf der Seite *Allgemeine Einstellungen* aktiviert sein. Weitere Informationen hierzu finden Sie unter Allgemeine Einstellungen auf Verwaltungs- oder organisationsspezifischer Ebene konfigurieren.

Archivierte Benutzerkonten werden auf der Appliance als schreibgeschützt gespeichert. Sie können sie nach Bedarf löschen. Wenn Sie ein Benutzerkonto archivieren und wieder zur Appliance hinzufügen, wird ein neues Benutzerkonto erstellt und das archivierte Konto gespeichert, bis es entfernt wird. Wenn beispielsweise ein Mitarbeiter das Unternehmen verlässt und sein Benutzerkonto archiviert wird, wird ein neues Benutzerkonto ohne jede Verknüpfung mit dem archivierten Konto erstellt, wenn er ins Unternehmen zurückkommt. Ähnlich führt ein LDAP-Import bei der Archivierung eines Benutzerkontos auf der Appliance ohne Aktualisierung des Active Directory des Unternehmens zu einem neuen Benutzerkonto, das nicht mit dem zuvor archivierten Benutzer verknüpft ist.

HINWEIS: Wenn die Benutzerarchivierung aktiviert ist, können Benutzerkonten nur gelöscht werden, wenn sie als archiviert gekennzeichnet sind.

1. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in*

Verwaltungskopfzeile anzeigen aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.

2. Klicken Sie in der linken Navigationsleiste auf **Systemsteuerung > Service Desk**.
3. Führen Sie einen der folgenden Schritte aus:
   - **Klicken Sie in der Liste** *Benutzer* **auf ein oder mehrere Benutzerkonten, die Sie archivieren möchten, und wählen Sie Aktion auswählen > Archivieren.**
   - **Klicken Sie in der Liste** *Benutzer* **auf den Namen des Benutzers, den Sie archivieren möchten. Klicken Sie auf der angezeigten Seite** *Benutzerdetail* **auf Archivieren.**
4. Klicken Sie im angezeigten Dialogfeld auf **Bestätigen**.

   Das Dialogfeld wird geschlossen und die Liste der *Benutzer* wird aktualisiert und zeigt an, dass der Benutzer den Status „Archiviert“ aufweist ( ).
5. Wenn Sie die Details für einen archivierten Benutzer überprüfen möchten, klicken Sie in der Liste *Benutzer* in der Spalte *Name* auf den Benutzernamen.

   Die Seite *Benutzerdetails* mit den Benutzerdetails im schreibgeschützten Modus wird angezeigt.

Als Nächstes können Sie Benutzerkonten löschen, falls erforderlich.

Anzeigen oder Bearbeiten von Benutzerprofilen

Sie können,, falls erforderlich, allgemeine Informationen zu Ihrem Benutzerprofil anzeigen und bestimmte Einstellungen bearbeiten.

Das Dialogfeld *Benutzerprofil* ermöglicht es jedem Benutzer schnell das Kennwort zu ändern, Geräte und Assets, die zugewiesen werden, und alle Service Desk Tickets, die sie erstellt haben, zu überprüfen. Benutzer mit Administratorberechtigungen können auch einige zusätzliche Parameter bearbeiten, wie Name, E-Mail, Manager und Gebietsschema. Sie können auch schnell auf die Seite *Benutzerdetails* wechseln und zusätzliche Informationen über ihr Konto überprüfen und gegebenenfalls Änderungen vornehmen.

Für weitere Informationen über das Bearbeiten von Benutzerkonten mithilfe der Seite *Benutzerdetails*, lesen Sie die folgenden Themen:

- Organisationsbenutzerkonten hinzufügen oder bearbeiten
- Benutzerkonten auf Systemebene hinzufügen oder bearbeiten

1. Führen Sie einen der folgenden Schritte aus:
   - **Melden Sie sich an der Administratorkonsole der Appliance unter `https://appliance_hostname/admin` an, wobei appliance_hostname der Hostname Ihrer Appliance ist. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option** *Organisationsmenü in Verwaltungskopfzeile anzeigen* **aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.**
   - **Melden Sie sich an der Systemverwaltungskonsole der Appliance unter `https://appliance_hostname/system` an, wobei appliance_hostname der Hostname Ihrer Appliance ist. Oder wählen Sie System in der Dropdownliste oben rechts auf der Seite aus.**
   - **Melden Sie sich an der Benutzerkonsole der Appliance unter `https://appliance_hostname/user` an, wobei appliance_hostname der Hostname Ihrer Appliance ist. Oder wählen Sie in der Dropdownliste oben rechts auf der Seite Benutzerkonsole aus.**
2. Wählen Sie rechts oben auf der Seite aus der Dropdown-Liste **Mein Profil**.

   Das Dialogfeld *Benutzerprofil* wird angezeigt.
3. Überprüfen und bearbeiten Sie die Informationen im Dialogfeld *Benutzerprofil* nach Bedarf.

HINWEIS: Benutzer ohne Administratorrechte können nur ihre Kennwörter aktualisieren und eine begrenzte Auswahl der Informationen in diesem Dialogfeld anzeigen ohne zusätzliche Änderungen ausführen zu können oder Zugriff auf die Seite *Benutzerdetail*.

Registerkarte	Option	Beschreibung
Profil	**Anmeldung**	Der Name, den der Benutzer auf der Anmeldeseite ins Feld *Anmelde-ID* eingibt. **HINWEIS:** Der Anmeldename des Standard-Administratorkontos kann nicht geändert werden.
	Name	Der vollständige Name des Benutzers.
	Primäre E-Mail-Adresse	Die E-Mail-Adresse des Benutzers.
	Manager	Der Manager des Benutzers.
	Gebietsschema	Das Gebietsschema, das für die **Administratorkonsole** und **Benutzerkonsole** für den Benutzer verwendet werden soll.
	Kennwort aktualisieren	Das Kennwort, das der Benutzer zur Anmeldung eingibt Wenn auf Ihrer Appliance die Organisationskomponente aktiviert ist oder Sie mehrere Appliances der K-Serie verknüpfen möchten, sollten Sie beim Ändern des Kennworts für das **admin**-Konto vorsichtig vorgehen. Die **admin**-Kennwörter für die Systemebene, für Organisationen und für verknüpfte Appliances müssen gleich sein, wenn Sie sie über die Dropdown-Liste oben rechts verwenden möchten. In der Dropdown-Liste werden nur die Organisationen und Appliances angezeigt, deren Kennwörter für das Administratorkonto gleich sind.
Geräte	**Name**	Der Gerätename.
	Untertyp	Der Asset-Untertyp für dieses Gerät, sofern einer zugewiesen wurde.

Registerkarte	Option	Beschreibung
	Primäres Gerät	Gibt an, ob das Gerät ist das primäre Gerät für den ausgewählten Benutzer ist.
Assets	**Name**	Der Asset-Name.
	Typ	Der Asset-Typ
	Untertyp	Der Asset-Untertyp für dieses Gerät, sofern einer zugewiesen wurde.
Service-Desk-Tickets	**Nummer**	Die Nummer des Service Desk Tickets, das der Benutzer angemeldet hat.
	Titel	Der Titel des Service Desk Ticket der Benutzer angemeldet hat.
	Status	Der Status des Service Desk Ticket der Benutzer angemeldet hat.

4. **Optional**. Für Zugriff auf die Seite *Benutzerdetails* klicken Sie in der oberen linken Ecke auf **Vollständiges Profil anzeigen**, und fahren fort, das Benutzerprofil auf dieser Seite zu überprüfen und zu bearbeiten.

   HINWEIS: Dieser Link wird nur angezeigt, wenn Ihr Konto über Administratorrechte verfügt.

5. Klicken Sie auf **Aktualisieren**, um Ihre Änderungen zu speichern.

Verwenden eines LDAP-Servers zur Benutzerauthentifizierung

Die Benutzerauthentifizierung kann lokal mit den auf der Appliance erstellten Konten oder extern mithilfe eines LDAP-Servers erfolgen.

Wenn Sie die externe LDAP-Serverauthentifizierung verwenden, greift die Appliance zur Authentifizierung von Benutzern auf einen Verzeichnisdienst zu. Dies ermöglicht Benutzern die Anmeldung an der **Benutzerkonsole**, der **Systemverwaltungskonsole** oder **Systemverwaltungskonsole** der Appliance mithilfe ihres Domainbenutzernamens und des -kennworts.

Informationen zum Hinzufügen von Benutzerkonten in der Appliance für die lokale Benutzerauthentifizierung finden Sie unter:

- Informationen zu Benutzerkonten und Benutzerauthentifizierung
- Verwalten von Benutzerkonten für Organisationen

Informationen zum Anmeldekonto für Ihren LDAP-Server

Zur Einrichtung der LDAP-Benutzerauthentifizierung müssen Sie auf dem LDAP-Server ein Anmeldekonto für die Appliance erstellen. Dieses Konto dient zum Lesen und Importieren von Benutzerinformationen des LDAP-Servers durch die Appliance.

Das Konto erfordert nur Lesezugriff auf das Feld *Suchbasis-DN* auf dem LDAP-Server. Das Konto benötigt keinen Schreibzugriff, da die Appliance nicht auf den LDAP-Server schreibt.

Außerdem muss das Konto ein nie ablaufendes Kennwort besitzen. Da das Kennwort nie abläuft, muss es sehr sicher sein. Der Benutzer kann das Kennwort ändern (das den entsprechenden Sicherheitsanforderungen entspricht), das Kennwort muss jedoch in der Appliance aktualisiert werden. Sie können einen Benutzernamen für das Konto vergeben, beispielsweise KACE_Login, oder versuchen, mit einer anonymen Bindung eine Verbindung zum LDAP-Server herzustellen.

LDAP-Benutzerauthentifizierung einrichten und testen

Sie können Verbindungen von der Appliance zu einem externen LDAP-Server konfigurieren und testen.

1. Führen Sie einen der folgenden Schritte aus:
   - **Melden Sie sich bei der Administratorkonsole der Appliance an: `https://appliance_hostname/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option** *Organisationsmenü in Verwaltungskopfzeile anzeigen* **aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.**
   - **Melden Sie sich bei der Systemadministratorkonsole der Appliance an: `https://appliance_hostname/system`. Oder wählen Sie in der Dropdown-Liste rechts oben auf der Seite den Eintrag System aus.**

   Die Seite *Dashboard* oder *System-Dashboard* wird angezeigt.
2. Rufen Sie die Seite *Authentifizierungseinstellungen* auf System- oder Verwaltungsebene auf:
   a. Klicken Sie in der linken Navigationsleiste auf **Einstellungen** und anschließend auf **Systemsteuerung**.
   b. Klicken Sie in der *Systemsteuerung* auf **Benutzerauthentifizierung** (nur Administratorkonsole) oder **System User Authentication (Systembenutzerauthentifizierung)** (nur Systemverwaltungskonsole).
3. Wenn Sie das lokale Administratorkonto deaktivieren möchten und als Benutzer auf Administratorebene über LDAP oder SAML angemeldet sind, wählen Sie **Disable Local Built-In Administrator (LDAP or SAML configuration required) (Lokal integriertes Administratorkonto deaktivieren (LDAP- oder SAML-Konfiguration erforderlich))**.

   Die Deaktivierung des integrierten Administratorkontos wirkt sich nicht auf einen vom KACE Support verwendeten Tether aus. Weitere Informationen zu dieser Funktion finden Sie unter .
4. Wählen Sie die Option **LDAP-Authentifizierung** aus:

Option	Beschreibung
Lokale Authentifizierung	Lokale Authentifizierung aktivieren (Standard). Wenn die lokale Authentifizierung aktiviert ist, wird das Kennwort anhand der vorhandenen Einträge in der lokalen Datenbank unter **Einstellungen** > **Benutzer** authentifiziert.
LDAP-Authentifizierung	Aktivierung der externen Benutzerauthentifizierung über einen LDAP- oder Active Directory-Server. Wenn **LDAP-Authentifizierung** aktiviert ist, wird das Kennwort über den externen LDAP-Server authentifiziert. Hilfe zur Authentifizierung erhalten Sie vom **Quest Support** unter https://support.quest.com/contact-support.

5. Klicken Sie auf die Schaltflächen neben den Servernamen, um die folgenden Aktionen auszuführen:

Schaltfläche	Aktion
	Planung eines Benutzerimports für den Server
	Änderung der Serverdefinition. Weitere Informationen zu den Feldern in diesem Abschnitt finden Sie unter Table 5.
	Entfernen des Servers
	Änderung der Reihenfolge der Server in der Serverliste

6. **Optional**: Klicken Sie auf **Neu**, um einen LDAP-Server hinzuzufügen. Es kann mehr als ein LDAP-Server konfiguriert werden.

   HINWEIS: Alle Server müssen über eine gültige IP-Adresse oder einen gültigen Hostnamen verfügen. Anderenfalls tritt bei diesem Vorgang ein Timeout auf, sodass bei der Verwendung der LDAP-Authentifizierung Verzögerungen bei der Anmeldung entstehen.

7. Geben Sie die folgenden Informationen an, um einen Server hinzuzufügen:

Serverinformationen

Option	Beschreibung
Name	Der Name für die Identifizierung des Servers.
Hostname oder IP-Adresse	Die IP-Adresse oder der Hostname des LDAP-Servers. Wenn die IP-Adresse ungültig ist, wartet die Appliance auf ein Timeout, sodass bei der Verwendung der LDAP-Authentifizierung Verzögerungen bei der Anmeldung entstehen. **HINWEIS:** Wenn die Verbindung über SSL hergestellt wird, verwenden Sie die IP-Adresse oder den Hostnamen. Beispiel: ldaps://hostname.
Port	Die LDAP-Port-Nummer, in der Regel 389 (LDAP) oder 636 (sicheres LDAP).
Basis-DN	Die Kriterien für die Suche nach Konten. Diese Kriterien legen einen Standort oder Container in der LDAP- oder Active Directory-Struktur fest und sollten alle Benutzer umfassen, die authentifiziert werden sollen. Geben Sie eine genaue Kombination aus OUs, DCs oder CNs an, die Ihren Kriterien entsprechen, die von links (sehr genau) bis rechts (sehr allgemein) reichen. Dieser Pfad führt beispielsweise zum Container mit den Benutzern, die Sie authentifizieren müssen: `OU=end_users,DC=company,DC=com`.

Option	Beschreibung
	HINWEIS: Domainbenutzer ist eine spezielle Gruppe, die nicht zu den `memberof`-Attributwerten hinzugefügt wird. Verwenden Sie für Benutzer der Gruppe "Domainbenutzer" das folgende Format: (primaryGroupId=513).
Erweiterte Suche	Der Suchfilter. Beispiel: `(&(sAMAccountName=KBOX_USERNAME) (memberOf=CN=financial,DC=example,DC=com))`

Anmeldung	Die Anmeldeinformationen, die erforderlich sind, damit die Appliance sich beim LDAP-Server anmelden und Konten lesen kann. Beispiel:
	`LDAP Login:CN=service_account,CN=Users,`
	`DC=Unternehmen, DC=com.`
	Wenn Benutzername und Kennwort nicht angegeben werden, wird der Struktur-Lookup nicht ausgeführt.
	Jedes LDAP-Label kann eine Verbindung zu einem anderen LDAP- oder Active Directory-Server herstellen.

Kennwort	Das Kennwort des Kontos, mit dem sich die Appliance beim LDAP-Server anmeldet.
Rolle	(Erforderlich) Die Rolle des Benutzers: • **Globaler Administrator**: Der Benutzer kann als Administrator mit vollständigen Lese-/Schreibberechtigungen auf die **Systemverwaltungskonsole** und jede **Administratorkonsole** der Organisation zugreifen. Er muss sich zuerst bei der **Systemverwaltungskonsole** und dann über die Dropdown-Liste oben rechts beim entsprechenden Konto der Organisation anmelden. • **Administrator**: Der Benutzer kann sich sowohl bei der **Administratorkonsole** als auch bei der **Benutzerkonsole** sowie der **Systemverwaltungskonsole** anmelden und auf alle Funktionen zugreifen. • **Administrator mit Leseberechtigung**: Der Benutzer kann sich bei der **Administratorkonsole**, der **Benutzerkonsole** oder bei der **Systemverwaltungskonsole** anmelden, jedoch keine Einstellungen ändern. • **Nur Benutzerkonsole**: Der Benutzer kann sich nur bei der **Benutzerkonsole**

Option	Beschreibung
	anmelden. Diese Rolle ist nur in der **Administratorkonsole** verfügbar. • **Kein Zugriff**: Der Benutzer kann sich nicht bei der **Administratorkonsole**, der **Systemverwaltungskonsole** oder der **Benutzerkonsole** anmelden. **Kein Zugriff** ist die Standardrolle. **HINWEIS:** Diese Rollen sind vordefiniert und können nicht bearbeitet werden. Sie können jedoch nach Bedarf benutzerdefinierte Rollen erstellen und bearbeiten.

HINWEIS: Halten Sie die Such- und Filterkriterien fest, die Sie für das Ausfüllen des Formulars verwenden. Sie benötigen dieselben Daten zum Importieren von Benutzerdaten und später für die Planung des regelmäßigen Benutzerimports.

8. Klicken Sie auf **Speichern**.
9. Testen Sie die Authentifizierung auf einem externen LDAP-Server wie folgt:
   a. Wählen Sie **LDAP-Authentifizierung** aus.
   b. Klicken Sie auf die Schaltfläche **Bearbeiten** neben dem Server, auf dem sich das zu testende Benutzerkonto befindet .
   c. Ersetzen Sie zu Testzwecken im Feld *Erweiterte Suche:* den Eintrag **KBOX_USER** durch den Benutzernamen. Die Syntax lautet `sAMAccountName=username`.
   d. Geben Sie das Kennwort des Benutzers in das Feld *Kennwort für Test* ein.
   e. Klicken Sie auf **Testen**.

   Wenn der Test erfolgreich war, ist die Authentifizierung für diesen und andere Benutzer im selben LDAP-Kontainer abgeschlossen.

Importieren von Benutzern aus einem LDAP-Server

Sie können Benutzerinformationen von LDAP-Servern importieren, um Benutzerkonten auf der Appliance zu erstellen. Dadurch können Administratoren, beispielsweise Service Desk-Mitarbeiter, bei der Arbeit mit Benutzern auf umfassendere Daten zurückgreifen.

Es gibt zwei Möglichkeiten, Benutzerinformationen zu importieren:

- **Manuell:** Siehe Benutzerinformationen manuell importieren
- **Nach einem Zeitplan:** Siehe Benutzerinformationen nach einem Zeitplan importieren

HINWEIS: Bei jedem Import von Benutzern in die Appliance werden Benutzerinformationen überschrieben. Kennwortinformationen werden jedoch nicht importiert. Benutzer müssen bei jeder Anmeldung an der **Administratorkonsole** oder **Benutzerkonsole** ihre Kennwörter eingeben.

Benutzerinformationen manuell importieren

Sie können Benutzerinformationen manuell importieren, indem Sie die zu importierenden Benutzer mithilfe von Kriterien angeben.

1. Rufen Sie die Seite *Benutzer* auf:

a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://appliance_hostname/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.

b. Klicken Sie auf der linken Navigationsleiste auf **Einstellungen** und anschließend auf **Benutzer**.

c. Wählen Sie **Aktion auswählen > Benutzer importieren**.

2. Geben Sie die folgenden Informationen an:

HINWEIS: Geben Sie im LDAP-Browser den *Suchbasis-DN* und den *Suchfilter* an. Siehe LDAP-Browser verwenden.

Option	Beschreibung
Server	Die IP-Adresse oder der Hostname des LDAP-Servers. Wenn die IP-Adresse ungültig ist, wartet die Appliance auf ein Timeout, sodass bei der Verwendung der LDAP-Authentifizierung Verzögerungen bei der Anmeldung entstehen. **HINWEIS:** Wenn die Verbindung über SSL hergestellt wird, verwenden Sie die IP-Adresse oder den Hostnamen. Beispiel: ldaps://hostname.
Port	Die LDAP-Port-Nummer, in der Regel 389 (LDAP) oder 636 (sicheres LDAP).
Basis-DN	Die Kriterien für die Suche nach Konten. Diese Kriterien legen einen Standort oder Container in der LDAP- oder Active Directory-Struktur fest und sollten alle Benutzer umfassen, die authentifiziert werden sollen. Geben Sie eine genaue Kombination aus OUs, DCs oder CNs an, die Ihren Kriterien entsprechen, die von links (sehr genau) bis rechts (sehr allgemein) reichen. Dieser Pfad führt beispielsweise zum Container mit den Benutzern, die Sie authentifizieren müssen: `OU=end_users,DC=company,DC=com`. **HINWEIS:** Geben Sie im LDAP-Browser den Suchbasis-DN und den Suchfilter an. LDAP-Browser verwenden.
Erweiterte Suche	Der Suchfilter. Beispiel: `(&(sAMAccountName=KBOX_USERNAME) (memberOf=CN=financial,DC=example,DC=com))`
Anmeldung	Die Anmeldeinformationen, die erforderlich sind, damit die Appliance sich beim LDAP-Server anmelden und Konten lesen kann. Beispiel: `LDAP Login:CN=service_account,CN=Users,` `DC=Unternehmen, DC=com`. Wenn Benutzername und Kennwort nicht angegeben werden, wird der Struktur-Lookup nicht ausgeführt. Jedes LDAP-Label kann eine

Option	Beschreibung
	Verbindung zu einem anderen LDAP- oder Active Directory-Server herstellen.
Kennwort	Das Kennwort des Kontos, mit dem sich die Appliance beim LDAP-Server anmeldet.

3. Geben Sie die LDAP-Attribute an, die importiert werden sollen.

Option	Beschreibung
Abzurufende Attribute	Geben Sie die LDAP-Attribute an, die abgerufen werden sollen. Beispiel: `sAMAccountName, objectguid, mail, memberof, displayname, sn, cn, userPrincipalName, name, description, manager` Die LDAP-Attribute in diesem Feld können den Benutzerattributen der Appliance auf der nächsten Seite zugewiesen werden. Wenn dieses Feld leer ist, ruft die Appliance alle LDAP-Attribute ab. Es wird nicht empfohlen, dieses Feld leer zu lassen, da ansonsten das Importieren von Attributen länger dauert. **WICHTIG: Um das Manager-Objekt abzurufen, das dem Benutzer zugewiesen wurde, müssen Sie das Attribut `manager` der Liste hinzufügen und diese Zuordnung später angeben.**
Labelattribut	Geben Sie ein Labelattribut ein. Beispiel: `memberof`. Diese Einstellung gibt eine Liste von Gruppen zurück, in denen dieser Benutzer Mitglied ist. Alle Labelattribute zusammen bilden die Labelliste, die Sie importieren können. Wenn der Suchfilter sowohl die Labelnamen als auch die Benutzernamen enthält, ist das Labelattribut nicht erforderlich.
Labelpräfix	Geben Sie das Labelpräfix ein. Beispiel: `ldap_` Das Labelpräfix ist eine Zeichenfolge, die allen Labels vorangestellt wird.
Binäre Attribute	Geben Sie die binären Attribute ein. Beispiel: `objectsid`. Hiermit wird angegeben, welche Attribute zu Speicherzwecken binär verarbeitet werden sollten.
Maximale Zeilenanzahl	Geben Sie die maximale Anzahl der abzurufenden Zeilen an. Hierdurch werden die im nächsten Schritt zurückgegeben Ergebnisse begrenzt.

Option	Beschreibung
Debug-Ausgabe	Aktivieren Sie das Kontrollkästchen, um die Debug-Ausgabe anzuzeigen.

4. Klicken Sie auf **Weiter**.

   Die Seite *Zuordnung zwischen Benutzerattributen und LDAP-Attributen definieren* wird angezeigt.
5. Wählen Sie in der Dropdown-Liste neben jedem Attribut den Wert aus, der für die Appliance-Benutzerattribute beim Import verwendet werden soll. Die Werte in der Dropdown-Liste sind die Werte, die im Feld *Abzurufende Attribute* auf der vorhergehenden Seite angegeben sind.

   Folgende Attribut-Zuordnungen sind erforderlich:

Option	Beschreibung
LDAP-UID	Der Bezeichner für den Benutzer. Empfohlener Wert: `objectguid`.
Benutzername	Der Name des Benutzers. Empfohlener Wert: `name`.
E-Mail	Die E-Mail-Adresse des Benutzers. Empfohlener Wert: `mail`.
Manager	Der Manager des Benutzers. Diese Zuordnung ist nur obligatorisch, wenn Sie Manager-Informationen abrufen möchten. Empfohlener Wert: `manager`. **WICHTIG: Um das Manager-Objekt abzurufen, das dem Benutzer zugewiesen wurde, müssen Sie das Attribut `manager` auch dem Feld *Abzurufende Attribute* zuordnen.**

   Die folgenden Attribut-Zuordnungen sind zwar nicht erforderlich, werden aber empfohlen:

Option	Beschreibung
API aktiviert	Ob Benutzer mit der KACE GO-App auf die Appliance zugreifen dürfen. Der Zugriff ist aktiviert, wenn das Feld einen numerischen Wert enthält. Der Zugriff ist deaktiviert, wenn das Feld keinen Wert enthält. Wenn Sie also den Zugriff gewähren wollen, müssen Sie ein Attribut auswählen, das einen numerischen Wert zurück gibt. Zum Deaktivieren des Zugriffs wählen Sie **Kein Wert** aus.
Ams Id	Nicht verwendet. Empfohlener Wert: **Kein Wert**.

6. **Optional**: Wählen Sie in der Dropdown-Liste *Rolle* die Rolle für importierte Benutzer aus. Siehe Benutzerrollen hinzufügen oder bearbeiten.
7. **Optional**: Wählen Sie in der Dropdown-Liste *Labels* das Label aus, das importierten Benutzern zugewiesen werden soll. Siehe Informationen zu den Labels.
8. Überprüfen Sie im Abschnitt *Suchergebnisse* unter der Liste mit den Attribut-Zuordnungen, dass die Liste der zu importierenden Benutzer korrekt ist und die für jeden Benutzer gezeigten Informationen Ihren Erwartungen entsprechen. Um die Suche zu verfeinern, klicken Sie auf die Schaltfläche **Zurück** und überarbeiten Sie die Suchparameter und Attribute.

Um beispielsweise die Anzahl der *Suchergebnisse* zu ändern, passen Sie die *Maximale Zeilenzahl* auf der Seite *Zu importierende Attribute auswählen* an.

9. Klicken Sie auf **Weiter**, um die Seite *Import Data into the appliance (Daten in die Appliance importieren)* anzuzeigen.
10. Überprüfen Sie die Tabellen mit Benutzern, um sicherzustellen, dass die Daten gültig sind und dass sie die erwarteten Daten enthalten.

    Es werden nur Benutzer importiert, die die erforderlichen Attribute *LDAP-UID*, *Benutzername*, *E-Mail* und *Manager* haben. Datensätze, die nicht über diese Werte verfügen, werden im Abschnitt *Benutzer mit ungültigen Daten* aufgeführt.
11. Klicken Sie auf **Jetzt importieren**, um den Import zu starten.

Die Seite *Benutzer* wird mit den importierten Benutzern in der Liste angezeigt. Die importierten Benutzer können je nach zugewiesener Rolle auf die Funktionen der **Administratorkonsole** und **Benutzerkonsole** zugreifen.

Benutzerinformationen nach einem Zeitplan importieren

Damit die Benutzerdaten stets aktuell sind, sollten Sie diese regelmäßig von Ihrem LDAP-Server importieren.

1. Rufen Sie die Seite *Authentifizierungseinstellungen* auf der Verwaltungsebene auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Einstellungen** und anschließend auf **Systemsteuerung**.
   c. Klicken Sie in der *Systemsteuerung* auf **Benutzerauthentifizierung** (nur Administratorkonsole) oder **System User Authentication (Systembenutzerauthentifizierung)** (nur Systemverwaltungskonsole).
2. Wählen Sie **LDAP-Authentifizierung** aus und klicken Sie dann auf die Schaltfläche **Zeitplan** neben dem Servernamen in der Serverliste, um einen Benutzerimport zu planen:

   Die Seite *Benutzerimport: Planen – Zu importierende Attribute auswählen* wird angezeigt.

   Die folgenden *schreibgeschützten Serverdetails für Administratoren* werden angezeigt:

Option	Beschreibung
Server	Die IP-Adresse oder der Hostname des LDAP-Servers. Wenn die IP-Adresse ungültig ist, wartet die Appliance auf ein Timeout, sodass bei der Verwendung der LDAP-Authentifizierung Verzögerungen bei der Anmeldung entstehen. **HINWEIS:** Wenn die Verbindung über SSL hergestellt wird, verwenden Sie die IP-Adresse oder den Hostnamen. Beispiel: ldaps://hostname.
Port	Die LDAP-Port-Nummer, in der Regel 389 (LDAP) oder 636 (sicheres LDAP).
Basis-DN	Die Kriterien für die Suche nach Konten. Diese Kriterien legen einen Standort oder Container in der LDAP- oder Active Directory-Struktur fest und sollten alle Benutzer umfassen, die authentifiziert werden sollen. Geben Sie eine genaue Kombination

Option	Beschreibung
	aus OUs, DCs oder CNs an, die Ihren Kriterien entsprechen, die von links (sehr genau) bis rechts (sehr allgemein) reichen. Dieser Pfad führt beispielsweise zum Container mit den Benutzern, die Sie authentifizieren müssen: `OU=end_users,DC=company,DC=com`. **HINWEIS:** Geben Sie im LDAP-Browser den Suchbasis-DN und den Suchfilter an. LDAP-Browser verwenden.
Erweiterte Suche	Der Suchfilter. Beispiel: `(&(sAMAccountName=KBOX_USERNAME) (memberOf=CN=financial,DC=example,DC=com))`
Anmeldung	Die Anmeldeinformationen, die erforderlich sind, damit die Appliance sich beim LDAP-Server anmelden und Konten lesen kann. Beispiel: `LDAP Login:CN=service_account,CN=Users,` `DC=Unternehmen, DC=com`. Wenn Benutzername und Kennwort nicht angegeben werden, wird der Struktur-Lookup nicht ausgeführt. Jedes LDAP-Label kann eine Verbindung zu einem anderen LDAP- oder Active Directory-Server herstellen.
Kennwort	Das Kennwort des Kontos, mit dem sich die Appliance beim LDAP-Server anmeldet.

3. Geben Sie die LDAP-Attribute an, die importiert werden sollen.

Option	Beschreibung
Abzurufende Attribute	Geben Sie die LDAP-Attribute an, die abgerufen werden sollen. Beispiel: `sAMAccountName, objectguid, mail, memberof, displayname, sn, cn, userPrincipalName, name, description, manager` Die LDAP-Attribute in diesem Feld können den Benutzerattributen der Appliance auf der nächsten Seite zugewiesen werden. Wenn dieses Feld leer ist, ruft die Appliance alle LDAP-Attribute ab. Es wird nicht empfohlen, dieses Feld leer zu lassen, da ansonsten das Importieren von Attributen länger dauert. **WICHTIG: Um das Manager-Objekt abzurufen, das dem Benutzer zugewiesen wurde, müssen Sie das Attribut `manager` der Liste hinzufügen und diese Zuordnung später angeben.**

Option	Beschreibung
Labelattribut	Geben Sie ein Labelattribut ein. Beispiel: `memberof`. Diese Einstellung gibt eine Liste von Gruppen zurück, in denen dieser Benutzer Mitglied ist. Alle Labelattribute zusammen bilden die Labelliste, die Sie importieren können. Wenn der Suchfilter sowohl die Labelnamen als auch die Benutzernamen enthält, ist das Labelattribut nicht erforderlich.
Labelpräfix	Geben Sie das Labelpräfix ein. Beispiel: `ldap_` Das Labelpräfix ist eine Zeichenfolge, die allen Labels vorangestellt wird.
Binäre Attribute	Geben Sie die binären Attribute ein. Beispiel: `objectsid`. Hiermit wird angegeben, welche Attribute zu Speicherzwecken binär verarbeitet werden sollten.
Maximale Zeilenanzahl	Geben Sie die maximale Anzahl der abzurufenden Zeilen an. Hierdurch werden die im nächsten Schritt zurückgegeben Ergebnisse begrenzt.
Debug-Ausgabe	Aktivieren Sie das Kontrollkästchen, um die Debug-Ausgabe anzuzeigen.

4. Klicken Sie im Abschnitt *E-Mail-Empfänger* auf die Schaltfläche **Bearbeiten**, um die E-Mail-Adresse der Empfänger einzugeben .
5. Wählen Sie in der Dropdown-Liste *Empfänger* Benutzer aus.
6. Geben Sie im Abschnitt *Zeitplan* die Zeitplanungsoptionen an:

Option	Beschreibung
Kein(e)	Die Ausführung erfolgt im Zusammenhang mit einem Ereignis anstatt zu einem bestimmten Datum oder zu einem bestimmten Zeitpunkt. Diese Option ist nützlich, wenn Sie Patches manuell auf Server anwenden oder Patch-Aktionen ausführen möchten, die nicht nach einem Zeitplan ausgeführt werden sollen.
Alle _ Stunden	Der Vorgang wird im angegebenen Intervall durchgeführt.
Täglich/an einem bestimmten Tag um HH:MM	Die Erfassung wird täglich zu einem bestimmten Zeitpunkt oder an einem bestimmten Wochentag um eine bestimmte Uhrzeit ausgeführt.
Ausführen am n-ten jedes Monats/eines bestimmten Monats um HH:MM	Am **n**. Tag jedes Monats ausführen (beispielsweise am ersten oder zweiten) Tag des Monats oder in einem bestimmten Monat zu einer bestimmten Zeit.

Option	Beschreibung
Ausführen am n-ten Wochentag **jedes Monats/ eines bestimmten Monats um HH:MM**	Die Erfassung wird jeden Monat oder in einem bestimmten Monat an einem festgelegten Wochentag zu einer festgelegten Uhrzeit ausgeführt.

Benutzerdefiniert	Ausführung nach einem benutzerdefinierten Zeitplan.
	Verwenden Sie das Standard-5-Feld-Cron-Format (das erweiterte Cron-Format wird nicht unterstützt):
	`* * * * *`
	`| | | | +————Wochentag (0-6) (Sonntag=0)`
	`| | | +————Monat (1-12)`
	`| | +————Monatstag (1-31)`
	`| +————Stunde (0-23)`
	`+————Minute (0-59)`
	Verwenden Sie bei der Angabe von Werten die folgenden Zeichen:
	• **Leerzeichen( )**: Die einzelnen Felder mit einem Leerzeichen trennen.
	• **Sternchen (*)**: Ein Sternchen repräsentiert den gesamten Wertebereich in einem Feld. Zum Beispiel repräsentiert ein Sternchen im Stundenfeld eine beliebige Stunde.
	• **Kommas (,)**: Mehrere Werte in einem Feld werden mit einem Komma getrennt. Zum Beispiel werden mit `0,6` im Feld „Wochentag“ Sonntag und Samstag angegeben.
	• **Bindestriche (-)**: Mit einem Bindestrich wird ein Wertebereich in einem Feld angegeben. Zum Beispiel entspricht `1-5` im Feld „Wochentag“ `1,2,3,4,5`, d. h. Montag bis Freitag.
	• **Schrägstriche (/)**: Die Angabe der Zeitabstände, mit denen eine Aktion wiederholt werden soll, erfolgt mit einem Schrägstrich. Zum Beispiel entspricht `*/3` im Feld Stunde `0,3,6,9,12,15,18,21`. Das Sternchen (`*`) gibt jede Stunde an, mit `/3` erfolgt aber eine Einschränkung auf durch drei teilbare Stunden.

Option	Beschreibung
	Beispiele: • `15 * * * *` Jeden Tag 15 Minuten nach jeder vollen Stunde ausführen • `0 22 * * *` Jeden Tag um 22:00 Uhr ausführen • `0 0 1 1,6 *` Am 1. Januar und 1. Juni um 00:00 Uhr ausführen • `30 8,12 * * 1-5` An Wochentagen um 08:30 Uhr und 12:30 Uhr ausführen • `0 2 */2 * *` Jeden zweiten Tag um 02:00 Uhr ausführen
Aufgabenplan anzeigen	Klicken Sie, um den Aufgabenplan anzuzeigen. Im Dialogfeld *Taskplan* wird eine Liste der geplanten Ziele angezeigt. Klicken Sie auf eine Aufgabe, um die Aufgabendetails anzuzeigen. Weitere Informationen hierzu finden Sie unter Aufgabenpläne anzeigen.

7. Klicken Sie auf **Weiter**, um die Seite *Benutzerimport: Planen – Zuordnung zwischen Benutzerattributen und LDAP-Attributen definieren* anzuzeigen.
8. Wählen Sie in der Dropdown-Liste neben jedem Attribut den Wert aus, der für die Appliance-Benutzerattribute beim Import verwendet werden soll. Die Werte in der Dropdown-Liste sind die Werte, die im Feld *Abzurufende Attribute* auf der vorhergehenden Seite angegeben sind.

   Folgende Attribut-Zuordnungen sind erforderlich:

Option	Beschreibung
LDAP-UID	Der Bezeichner für den Benutzer. Empfohlener Wert: `objectguid`.
Benutzername	Der Name des Benutzers. Empfohlener Wert: `name`.
E-Mail	Die E-Mail-Adresse des Benutzers. Empfohlener Wert: `mail`.
Manager	Der Manager des Benutzers. Diese Zuordnung ist nur obligatorisch, wenn Sie Manager-Informationen abrufen möchten. Empfohlener Wert: `manager`. **WICHTIG: Um das Manager-Objekt abzurufen, das dem Benutzer zugewiesen wurde, müssen Sie das Attribut `manager` auch dem Feld *Abzurufende Attribute* zuordnen.**

   Die folgenden Attribut-Zuordnungen sind zwar nicht erforderlich, werden aber empfohlen:

Option	Beschreibung
API aktiviert	Ob Benutzer mit der KACE GO-App auf die Appliance zugreifen dürfen. Der Zugriff ist aktiviert, wenn das Feld einen numerischen Wert enthält. Der

Option	Beschreibung
	Zugriff ist deaktiviert, wenn das Feld keinen Wert enthält. Wenn Sie also den Zugriff gewähren wollen, müssen Sie ein Attribut auswählen, das einen numerischen Wert zurück gibt. Zum Deaktivieren des Zugriffs wählen Sie **Kein Wert** aus.
Ams Id	Nicht verwendet. Empfohlener Wert: **Kein Wert**.

9. **Optional**: Wählen Sie in der Dropdown-Liste *Rolle* die Rolle für importierte Benutzer aus. Siehe Benutzerrollen hinzufügen oder bearbeiten.
10. Wenn die gewählte Rolle eine Standardrolle für neue Rollen sein soll, wählen Sie das Kontrollkästchen **Als Standard festlegen** aus.
11. **Optional**: Wählen Sie in der Dropdown-Liste *Labels* das Label aus, das importierten Benutzern zugewiesen werden soll. Siehe Informationen zu den Labels.
12. Überprüfen Sie im Abschnitt *Suchergebnisse* unter der Liste mit den Attribut-Zuordnungen, dass die Liste der zu importierenden Benutzer korrekt ist und die für jeden Benutzer gezeigten Informationen Ihren Erwartungen entsprechen. Um die Suche zu verfeinern, klicken Sie auf die Schaltfläche **Zurück** und überarbeiten Sie die Suchparameter und Attribute.

    Um beispielsweise die Anzahl der *Suchergebnisse* zu ändern, passen Sie die *Maximale Zeilenzahl* auf der Seite *Zu importierende Attribute auswählen* an.
13. Klicken Sie auf **Weiter**, um die Seite *Import Data into the appliance (Daten in die Appliance importieren)* anzuzeigen.
14. Überprüfen Sie die Tabellen mit Benutzern, um sicherzustellen, dass die Daten gültig sind und dass sie die erwarteten Daten enthalten.

    Es werden nur Benutzer importiert, die die erforderlichen Attribute *LDAP-UID*, *Benutzername*, *E-Mail* und *Manager* haben. Datensätze, die nicht über diese Werte verfügen, werden im Abschnitt *Benutzer mit ungültigen Daten* aufgeführt.
15. Führen Sie einen der folgenden Schritte aus:
    - **Klicken Sie auf Zurück, um die Einstellungen zu ändern.**
    - **Klicken Sie auf Importieren, um den Zeitplan zu speichern und die Benutzerinformationen sofort zu importieren. Das Importieren beginnt und der Zeitplan wird entsprechend der Optionen im Abschnitt *Planen* zur Ausführung ausgewählt.**
    - **Klicken Sie auf Fertig stellen, um den Zeitplan zu speichern, ohne die Benutzerinformationen zu importieren. Der Zeitplan wird entsprechend der Optionen im Abschnitt *Planen* zur Ausführung ausgewählt.**

    Die Benutzerinformationen werden im Einklang mit dem angegebenen Zeitplan importiert.

Informationen zur einmaligen Anmeldung (SSO)

Dank der einmaligen Anmeldung können Benutzer, die sich bei der Domäne angemeldet haben oder über einen Drittanbieter authentifiziert sind, auf die **Administratorkonsole** und die **Benutzerkonsole** der Appliance zugreifen, ohne die Anmeldeinformationen erneut auf der Anmeldeseite der Appliance eingeben zu müssen.

Sie können für die einmalige Anmeldung Active Directory verwenden.

Die einmalige Anmeldung ist verfügbar für:

- **Nur eine Domäne**: Wenn Sie über mehrere Domänen verfügen, ist die einmalige Anmeldung nur für eine Domäne möglich. Dies gilt auch dann, wenn in der Appliance die Organisationskomponente aktiviert wurde und Sie über mehrere Organisationen in unterschiedlichen Domänen verfügen. Die einmalige Anmeldung

ist eine Konfiguration auf Systemebene und Organisationen können nicht unabhängig voneinander für die einmalige Anmeldung konfiguriert werden.

- **Microsoft Active Directory-Server**: Sie können die einmalige Anmeldung über Microsoft Active Directory-Server mit 2003 R2 oder höheren Schemaversionen aktivieren. Ältere Schema-Versionen können nicht genutzt werden. Wenn die Organisationskomponente auf Ihrer Appliance aktiviert ist, kann die Active Directory-Methode zur einmaligen Anmeldung mit mehreren Organisationen verwendet werden.

Externe LDAP- oder Active Directory-Server für die einmalige Anmeldung verwenden

Bei Verwendung von Active Directory für die Authentifizierung zur einmaligen Anmeldung muss der externe LDAP- oder Active Directory-Server dieselben Einträge aufweisen wie der für die einmalige Anmeldung angegebene Active Directory-Server. Die Appliance gleicht die Benutzeranmeldeinformationen der hinzugefügten Domäne ab und ermittelt dann mithilfe der Konfiguration des externen LDAP die Benutzerrollen und Rechte.

Zur Authentifizierung von Benutzern mithilfe lokaler Konten auf der Appliance müssen Sie entweder Konten von einem LDAP- oder Active Directory-Server auf die Appliance importieren oder die Konten manuell in der Appliance anlegen. Siehe:

- Importieren von Benutzern aus einem LDAP-Server
- Verwalten von Benutzerkonten auf Systemebene
- Verwalten von Organisationsbenutzerkonten

Aktivieren und Deaktivieren der einmaligen Anmeldung

Sie können die einmalige Anmeldung in den Sicherheitseinstellungen der Appliance aktivieren bzw. deaktivieren.

Einmalige Anmeldung aktivieren

Zur Aktivierung der einmaligen Anmeldung müssen Sie die Sicherheitseinstellungen der Appliance für das Herstellen einer Verbindung zwischen einem Active Directory Server und der Appliance konfigurieren.

- Informationen zum Konfigurieren der einmaligen Anmeldung für Active Directory finden Sie unter Active Directory als Methode für das einmalige Anmelden konfigurieren

1. Navigieren Sie zur *Systemsteuerung* der Appliance:
   - **Wenn die Organisationskomponente nicht für die Appliance aktiviert ist, melden Sie sich bei der Administratorkonsole an: `https://appliance_hostname/admin`, und wählen Sie dann Einstellungen > Systemsteuerung aus.**
   - **Wenn die Organisationskomponente für die Appliance aktiviert ist, melden Sie sich bei der Systemverwaltungskonsole der Appliance an: `https://appliance_hostname/system`. Oder wählen Sie in der Dropdown-Liste rechts oben auf der Seite den Eintrag System aus, und klicken Sie dann auf Einstellungen > Systemsteuerung.**
2. Klicken Sie auf **Sicherheitseinstellungen**, um die Seite *Sicherheitseinstellungen* anzuzeigen.
3. Wählen Sie im Abschnitt *Einmalige Anmeldung* eine Methode für die einmalige Anmeldung aus.

- Active Directory als Methode für das einmalige Anmelden konfigurieren

Einmalige Anmeldung deaktivieren

Sie können die einmalige Anmeldung deaktivieren, ohne die Appliance aus der Domäne zu entfernen.

1. Navigieren Sie zur *Systemsteuerung* der Appliance:
   - **Wenn die Organisationskomponente nicht für die Appliance aktiviert ist, melden Sie sich bei der Administratorkonsole an: `https://appliance_hostname/admin`, und wählen Sie dann Einstellungen > Systemsteuerung aus.**
   - **Wenn die Organisationskomponente für die Appliance aktiviert ist, melden Sie sich bei der Systemverwaltungskonsole der Appliance an: `https://appliance_hostname/system`. Oder wählen Sie in der Dropdown-Liste rechts oben auf der Seite den Eintrag System aus, und klicken Sie dann auf Einstellungen > Systemsteuerung.**
2. Klicken Sie auf **Sicherheitseinstellungen**, um die Seite *Sicherheitseinstellungen* anzuzeigen.
3. Klicken Sie im Abschnitt *Einmalige Anmeldung* auf **Deaktivieren**.

   Die einmalige Anmeldung ist deaktiviert. Benutzer, die derzeit bei der **Administratorkonsole** oder **Benutzerkonsole** angemeldet sind, bleiben bis zum Ende ihrer Sitzung angemeldet. Wenn sie das nächste Mal auf die **Administratorkonsole** oder **Benutzerkonsole** zugreifen, müssen sie ihre Anmeldeinformationen jedoch eingeben.

Verwenden von Active Directory für die einmalige Anmeldung

Wenn Active Directory für die einmalige Anmeldung konfiguriert ist, können authentifizierte Benutzer auf die **Administratorkonsole** oder die **Benutzerkonsole** zugreifen, ohne Anmeldeinformationen eingeben zu müssen.

Benutzer müssen hierzu den Hostnamen der Appliance im Adressfeld des Browsers eingeben. Wenn Benutzer eine IP-Adresse eingeben, werden sie nicht automatisch angemeldet. Sie gelangen zur Anmeldeseite der Appliance, auf der sie ihre Anmeldeinformationen eingeben müssen, um sich anzumelden.

Wenn Sie Active Directory für die einmalige Anmeldung verwenden, müssen Sie die Browser Microsoft Edge und Mozilla Firefox so konfigurieren, dass sie die korrekten Sicherheitseinstellungen verwenden.

Active Directory als Methode für das einmalige Anmelden konfigurieren

Die einmalige Active Directory Anmeldung ermöglicht Benutzern, die sich bei der Domain angemeldet haben, auf die **Administratorkonsole** und die **Benutzerkonsole** der Appliance zuzugreifen, ohne die Anmeldeinformationen bei jeder Anmeldung erneut eingeben zu müssen.

Vergewissern Sie sich vor der Verbindung der Appliance mit einem Active Directory-Server folgender Punkte:

- Netzwerk- und DNS-Einstellungen sind so konfiguriert, dass die Appliance auf den Active Directory-Server zugreifen kann. Siehe Netzwerkeinstellungen der Appliance ändern.
- Die Zeiteinstellungen des Active Directory-Servers stimmen mit den Zeiteinstellungen der Appliance überein. Weitere Informationen zur Einstellung der Zeit auf der Appliance finden Sie unter Konfigurieren der Datum- und Uhrzeiteinstellungen der Appliance.

1. Navigieren Sie zur *Systemsteuerung* der Appliance:
   - **Wenn die Organisationskomponente nicht für die Appliance aktiviert ist, melden Sie sich bei der Administratorkonsole an: `https://appliance_hostname/admin`, und wählen Sie dann Einstellungen > Systemsteuerung aus.**
   - **Wenn die Organisationskomponente für die Appliance aktiviert ist, melden Sie sich bei der Systemverwaltungskonsole der Appliance an: `https://appliance_hostname/system`. Oder wählen Sie in der Dropdown-Liste rechts oben auf der Seite den Eintrag System aus, und klicken Sie dann auf Einstellungen > Systemsteuerung.**
2. Wählen Sie im Abschnitt *Einmalige Anmeldung* der Seite *Sicherheitseinstellungen* die Option **Active Directory** aus und geben Sie die folgenden Informationen an:

Option	Beschreibung
Domain	Der Hostname der Domain Ihres Active Directory® Servers, z.B. beispiel.com.
Benutzername	Der Benutzername des Administratorkontos auf dem Active Directory-Server. Beispiel: benutzername@beispiel.com.
Kennwort	Das Kennwort des Administratorkontos auf dem Active Directory-Server.
Computerobjektcontainer	Der Name des Computerobjektcontainers des Administratorkontos auf dem Active Directory-Server.
Computerobjektname	Der Name des Computerobjektcontainers des Administratorkontos auf dem Active Directory-Server.
Servicekontocontainer	Der Name des Servicekontocontainers des Administratorkontos auf dem Active Directory-Server.

3. Klicken Sie auf **Beitreten**.

Die Appliance führt die folgenden Tests aus (Leseberechtigung erforderlich), um festzustellen, ob die Domäne korrekt für den Beitritt der Appliance konfiguriert ist:

- Prüfung auf unterstützte Betriebssysteme und korrekte Betriebssystem-Patches
- Prüfung auf ausreichenden Speicherplatz zur Installation von QAS
- Prüfung, dass der Hostname des Systems nicht 'localhost' ist
- Prüfung, ob der Namensdienst für die Verwendung von DNS konfiguriert ist
- Prüfung, ob die Namensdiensteinträge in resolv.conf richtig formatiert sind und ob der Host aufgelöst werden kann
- Prüfung auf einen Namensserver, der über die entsprechenden DNS SRV-Datensätze für Active Directory verfügt
- Erkennung eines beschreibbaren Domänencontrollers mit offenem UDP-Port 389
- Erkennung der Active Directory-Site, falls verfügbar
- Prüfung, ob TCP-Port 464 für Kerberos kpasswd geöffnet ist
- Prüfung, ob UDP-Port 88 und TCP-Port 88 für Kerberos-Datenverkehr geöffnet sind
- Prüfung, ob TCP-Port 389 für LDAP geöffnet ist
- Prüfung auf einen globalen Katalogserver und ob TCP-Port 3268 für die Kommunikation mit globalen Katalogservern geöffnet ist
- Prüfung auf einen gültigen Zeitversatz über Active Directory
- Prüfung auf die QAS-Anwendungskonfiguration in Active Directory
- Prüfung, ob TCP-Port 445 für Microsoft CIFS-Datenverkehr geöffnet ist

Diese Tests erfordern keinen Schreibzugriff. Auch für einzelne Verzeichnisse werden keine Schreibberechtigungen benötigt. Zudem werden bei diesen Tests keine Benutzernamen und Kennwörter überprüft. Wenn die Anmeldeinformationen nicht korrekt sind, kann die Appliance selbst bei erfolgreich verlaufenen Tests möglicherweise nicht der Domäne beitreten.

Eine Meldung mit den Ergebnissen des Tests wird angezeigt. Klicken Sie zum Anzeigen von Fehlern auf **Protokolle** und wählen Sie aus der Dropdown-Liste *Protokoll* das Protokoll **Serverfehler** aus.

4. **Optional**: Damit der Server Fehler ignoriert und der Domäne beitritt, wählen Sie **Beitritt erzwingen** aus.
5. Klicken Sie auf **Dienste speichern und neu starten**.

Wenn Benutzer an Geräten angemeldet sind, die zur Active Directory Domain hinzugefügt wurden, können Sie auf die **Benutzerkonsole** der Appliance zugreifen, ohne die Anmeldeinformationen erneut eingeben zu müssen. Wenn Benutzer an Geräten angemeldet sind, die nicht zur Active Directory-Domäne hinzugefügt wurden, wird das Anmeldefenster angezeigt, mit dem sich die Benutzer mit einem lokalen Appliance-Benutzerkonto anmelden können. Siehe Benutzerkonten auf Systemebene hinzufügen oder bearbeiten.

HINWEIS: Zur Verwendung der einmaligen Anmeldung mit den Browsern Microsoft Edge und Firefox müssen die Benutzer ihre Browsereinstellungen für die richtige Authentifizierung konfigurieren. Siehe Browsereinstellungen für die einmalige Anmeldung konfigurieren.

Browsereinstellungen für die einmalige Anmeldung konfigurieren

Zur Verwendung der einmaligen Anmeldung für Active Directory mit den Browsern Microsoft Edge™ und Firefox® müssen Benutzer ihre Browsereinstellungen für die richtige Authentifizierung konfigurieren. Für den Chrome™-Browser wird keine besondere Konfiguration benötigt.

Einstellungen des Microsoft Edge-Browsers konfigurieren

Zur Verwendung der einmaligen Anmeldung für Active Directory mit Microsoft Edge müssen Sie die Windows-Sicherheitseinstellungen konfigurieren.

1. Klicken Sie in der Windows-Systemsteuerung auf **InternetoptionenExtras** > **Internetoptionen** > **Sicherheit**.
2. Wählen Sie im daraufhin angezeigten Dialogfeld *Eigenschaften von Internet* auf der Registerkarte *Sicherheit* die entsprechende Sicherheitsrichtlinie aus:
   - **Wenn die Appliance mit dem Internet verbunden ist, wählen Sie Vertrauenswürdige Sites aus.**
   - **Wenn die Appliance nicht mit dem Internet verbunden ist, wählen Sie Lokales Intranet.**
3. Klicken Sie auf **Stufe anpassen** und scrollen Sie zum Ende der Liste.
4. Wählen Sie **Automatische Anmeldung mit aktuellem Benutzernamen und Kennwort** aus. Wenn diese Option nicht gewählt wird, kann sich Microsoft Edge nicht automatisch bei der Administratorkonsole oder Benutzerkonsole anmelden, selbst wenn die einmalige Anmeldung auf der Appliance aktiviert ist.

Browsereinstellungen für Firefox konfigurieren

Zur Verwendung der einmaligen Anmeldung für Active Directory mit Firefox müssen Sie die Authentifizierungseinstellungen des Browsers konfigurieren.

1. Geben Sie in Firefox in der Adressleiste about:config ein.
2. Geben Sie im *Suchfeld* folgende Zeichenfolge ein: network.negotiate-auth.trusted-uris.
3. Doppelklicken Sie in den Suchergebnissen auf den Namen der Einstellung.
4. Geben Sie im Zeichenfolgenwert-Feld die URL der Appliance ein, Zum Beispiel http://kace_sma.beispiel.com. Klicken Sie anschließend auf **OK**.

Active Directory zur einmaligen Anmeldung für die Administratorkonsole oder Benutzerkonsole verwenden

Wenn die einmalige Anmeldung mit Active Directory auf der Appliance aktiviert ist, können bei der Domäne angemeldete Benutzer auf die **Administratorkonsole** oder **Benutzerkonsole** zugreifen, ohne zuerst ihre Anmeldeinformationen auf der Anmeldeseite der Appliance anzugeben.

Die einmalige Anmeldung mit Active Directory muss aktiviert sein. Siehe Einmalige Anmeldung aktivieren.

1. Melden Sie sich bei der Domäne an.
2. Geben Sie im Webbrowser den Hostnamen der Appliance im Adressfeld des Browsers ein. Zur Ermittlung des Hostnamens siehe Netzwerkeinstellungen der Appliance ändern.

   TIPP: Wenn Sie die Appliance-IP-Adresse eingeben, gelangen Sie zur Anmeldeseite der Appliance, statt automatisch angemeldet zu werden.

   Je nach den Berechtigungen des Benutzerkontos wird die **Administratorkonsole** oder **Benutzerkonsole** angezeigt.

Domänenbeitritt rückgängig machen und einmalige Anmeldung für Active Directory deaktivieren

Sie können die Appliance aus der Active Directory-Domäne entfernen. Das Entfernen der Appliance aus der Domäne deaktiviert automatisch die einmalige Anmeldung.

1. Navigieren Sie zur *Systemsteuerung* der Appliance:
   - **Wenn die Organisationskomponente nicht für die Appliance aktiviert ist, melden Sie sich bei der Administratorkonsole an: `https://appliance_hostname/admin`, und wählen Sie dann Einstellungen > Systemsteuerung aus.**
   - **Wenn die Organisationskomponente für die Appliance aktiviert ist, melden Sie sich bei der Systemverwaltungskonsole der Appliance an: `https://appliance_hostname/system`. Oder wählen Sie in der Dropdown-Liste rechts oben auf der Seite den Eintrag System aus, und klicken Sie dann auf Einstellungen > Systemsteuerung.**
2. Klicken Sie auf **Sicherheitseinstellungen**, um die Seite *Sicherheitseinstellungen* anzuzeigen.
3. Klicken Sie im Abschnitt *Einmalige Anmeldung* auf **Domänenbeitritt rückgängig machen**.

> **HINWEIS:** Benutzer, die derzeit bei der **Benutzerkonsole** oder **Administratorkonsole** angemeldet sind, bleiben bis zum Ende ihrer Sitzung angemeldet. Wenn sie das nächste Mal auf die **Benutzerkonsole** oder **Administratorkonsole** zugreifen, müssen sie ihre Anmeldeinformationen jedoch eingeben.

SAML für die einmalige Anmeldung konfigurieren

Sie können die Appliance so konfigurieren, dass Benutzer ohne Angabe ihrer Anmeldeinformationen auf der *Willkommensseite* mit einem Authentifizierungstool eines Drittanbieters authentifiziert werden.

Security Assertion Markup Language (SAML) ist ein XML-basiertes Protokoll, das Sicherheitstoken zwischen Identitäts- und Dienstanbietern verwendet. Die Sicherheitstoken enthalten Assertionselemente, die Informationen über die Identität des Benutzers bereitstellen.

Wenn SAML auf der Appliance aktiviert und konfiguriert ist und sich der Benutzer mit dieser Methode für die einmalige Anmeldung anmeldet, sendet die Appliance eine Autorisierungsanfrage an Ihren Identitätsanbieter (IdP). Der Identitätsanbieter bestätigt dann die Identität des Benutzers und sendet eine Authentifizierungsantwort an die Appliance. Als nächstes meldet das Gerät den Benutzer an der **Administratorkonsole** (oder **Benutzerkonsole**) an und startet die Benutzersitzung. Wenn sich ein SAML-Benutzer von der Appliance abmeldet, wird er bei seinem IdP-Konto abgemeldet. Wenn Sie nach der Verwendung der Appliance weiterhin bei Ihrem IdP-Konto angemeldet sein möchten, schließen Sie einfach das **Administratorkonsole** Browserfenster, ohne sich abzumelden. Wenn die Sitzung eines SAML-Benutzers abläuft und dieser immer noch bei seinem IdP-Konto angemeldet ist, startet die Appliance automatisch eine neue Sitzung für diesen Benutzer.

Wenn Sie über mehrere Organisationen verfügen, können Sie SAML in jeder Organisation konfigurieren, die diese Authentifizierungsmethode verwendet, und die lokale Anmeldemethode für andere Organisationen beibehalten.

1. Stellen Sie sicher, dass Ihr IdP über gültige Identitätsinformationen für die Anmeldung bei der Appliance verfügt.
2. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
3. Rufen Sie die Seite *SAML-Einstellungen* auf:

a. Klicken Sie in der linken Navigationsleiste auf **Einstellungen** und anschließend auf **SAML-Konfiguration**.

b. Aktivieren Sie auf der Seite *SAML-Einstellungen* unter *Security Assertion Markup Language (SAML)* das Kontrollkästchen **SAML-Service-Provider aktivieren**.

4. Wenn Benutzer nur SAML für den Zugriff auf diese Appliance verwenden sollen, wählen Sie **Require SAML login (SAML-Anmeldung erforderlich)**.

   Diese Option bewirkt, dass alle lokalen Anmeldungen bei der Appliance deaktiviert werden, mit Ausnahme des lokalen Administratorbenutzers und des KACE Support-Kontos (nur mit aktivem Support-Tether verfügbar).

5. Geben Sie im Abschnitt *Einstellungen für Remote Identity Provider (IdP)* Ihre IdP-Metadaten an, um Benutzer zu authentifizieren, indem Sie einen der folgenden Schritte ausführen.

   - **Empfohlen. Wenn Ihr IdP eine URL zur XML-Seite mit den IdP-Metadaten (vorgeschlagene Option) bereitstellt, klicken Sie auf Metadaten aus IdP abrufen. Geben Sie im angezeigten Feld** *IdP-Metadaten-URL* **diese URL ein und klicken Sie auf IdP-Metadaten importieren.**
   - **Wenn Sie Ihre IdP-Metadaten-XML-Datei verwenden möchten, klicken Sie auf XML-Metadaten eingeben und kopieren Sie den Inhalt der XML-Datei in das angezeigte Feld** *IdP-Metadaten-XML***. Klicken Sie dann auf IdP-Metadaten importieren. Die Appliance analysiert den bereitgestellten XML-Inhalt und füllt die Einstellungen aus, die zum Herstellen einer Verbindung mit dem IdP erforderlich sind.**

   Der Abschnitt *Einstellungen des Remote Identity Providers (IdP)* wird aktualisiert und zeigt die Details Ihrer IdP-Konfiguration an. Die aufgeführten Optionen geben die Weiterleitungen der Appliance-Seite während der SAML-Authentifizierung an. Weitere Informationen finden Sie unter https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security.

   HINWEIS: Um diese Informationen während der SAML-Konfiguration jederzeit zu überprüfen, klicken Sie in diesem Abschnitt auf **Metadaten anzeigen**.

6. Wählen Sie im Abschnitt *IdP-Attributzuordnungen* die Option aus, die Sie verwenden möchten, um dem SAML-Benutzer Zugriff auf die Appliance zu gewähren.

   - **Lokale Benutzertabelle verwenden: Basiert auf der Benutzerliste, die lokal auf der Appliance gespeichert ist.**
   - **LDAP-Suche verwenden: Importiert Benutzerinformationen von einem externen LDAP-Server. Weitere Informationen hierzu finden Sie unter Verwenden eines LDAP-Servers zur Benutzerauthentifizierung.**
   - **SAML verwenden: Verwendet die auf dieser Seite angegebenen Werte, um die von Ihrem IdP verwendeten Felder den Benutzerdatensätzen der Appliance zuzuordnen, z. B. Name, E-Mail-Adresse usw. Wenn der IdP beispielsweise LDAP zur Authentifizierung von Benutzern verwendet, können Sie** *UID* **und** *Anmeldung* **auf `objectGUID` bzw. `cn` einstellen. Weitere Informationen finden Sie in der IdP-Dokumentation.**

7. Wenn Sie **SAML verwenden** ausgewählt haben, geben Sie an, ob Sie auf der Appliance für authentifizierte SAML-Benutzer, die nicht über Konten auf der Appliance verfügen, einen neuen Benutzer erstellen möchten. Wählen Sie dazu **Create new SMA user if authenticated SAML user does not exist on SMA (Neuen SMA-Benutzer erstellen, wenn über SAML authentifizierter Benutzer auf SMA nicht vorhanden)**.

8. Wenn Sie **SAML verwenden** ausgewählt haben, geben Sie die Rollen an, die Sie dem über SAML authentifizierten Benutzer gewähren möchten. Geben Sie unter *Rollenzuordnung* die Bedingungen an, die beim Gewähren der Rollen überprüft werden sollen.

   Sie können beispielsweise den Mitgliedern einer LDAP-Gruppe, deren Name eine bestimmte Textzeichenfolge enthält (z. B. `admin`), die Rolle *Administrator* wie folgt verleihen:

   Administrator `memberOf` *enthält* `admin`

   Die Rollen werden in der Reihenfolge ihrer Priorität aufgelistet. Sie können die Rollenpriorität nach Bedarf durch Ziehen und Ablegen ändern. Wenn mehrere Übereinstimmungen vorhanden sind, gewährt die Appliance dem SAML-Benutzer die Rolle mit der höchsten Priorität.

Die Rollenzuordnung ist optional. Wenn keine Übereinstimmungen gefunden werden, weist die Appliance die Standardrolle zu. Um die Standardrolle festzulegen, klicken Sie auf **Standardrolle für nicht übereinstimmende Benutzer**, und wählen Sie eine entsprechende Rolle aus den verfügbaren Optionen aus: *Administrator*, *Kein Zugriff*, *Administrator mit Leseberechtigung* oder *Nur Benutzerkonsole*.

9. **Optional**. Um die Appliance-spezifischen SAML-Einstellungen auf der Appliance anzuzeigen, klicken Sie im Abschnitt *Lokale Einstellungen für Service Provider (SP)* auf **Metadaten anzeigen** und überprüfen Sie die angezeigten Optionen.

   Diese Felder enthalten Standardwerte und in den meisten Fällen müssen Sie keine Änderungen vornehmen.

10. Klicken Sie auf **Speichern**.
11. Testen Sie Ihre SAML-Konfiguration.
    a. Melden Sie sich von der Appliance ab.
    b. Stellen Sie sicher, dass Sie bei Ihrem IdP-Konto angemeldet sind.
    c. Öffnen Sie die Willkommensseite von Administratorkonsole oder Benutzerkonsole.
    d. Klicken Sie auf **Anmelden**, ohne Ihre Benutzeranmeldedaten anzugeben.

    TIPP: Wenn SAML auf der Appliance aktiviert ist, klicken Sie auf **Lokale Anmeldung**, und geben Sie Ihre Benutzeranmeldedaten an.

    Die Seite **Administratorkonsole** oder **Benutzerkonsole** wird angezeigt.

Beispiel: Verwenden von Microsoft Active Directory in Azure als SAML Identity Provider

Wenn Sie Active Directory in Azure als SAML Identity Provider (IdP, Identitätsanbieter) verwenden, sind einige zusätzliche Schritte erforderlich. In diesem Thema wird beschrieben, wie SAML mit Active Directory als IdP konfiguriert wird.

1. Stellen Sie sicher, dass Ihr IdP über gültige Identitätsinformationen für die Anmeldung bei der Appliance verfügt.
2. Führen Sie folgende Schritte durch:
   a. Aktivieren Sie SSL für die Appliance. Dieser Schritt ist erforderlich, da Microsoft Azure nur mit SSL-Clients erfolgreich kommunizieren kann. Anleitungen dazu finden Sie unter Sicherheitseinstellungen für die Appliance konfigurieren.
   b. Melden Sie sich bei https://portal.azure.com an, und wählen Sie **Azure Active Directory** aus.
   c. Erstellen Sie unter **App-Registrierungen** eine neue Registrierung, und lassen Sie die *Umleitungs-URI*-Einstellungen deaktiviert.
   d. Kopieren Sie in der neu erstellten Anwendungsregistrierung auf der Seite *Endpunkte* den Inhalt des Felds *Verbundmetadaten-Dokument*.
3. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
4. Rufen Sie die Seite *SAML-Einstellungen* auf:
   a. Klicken Sie in der linken Navigationsleiste auf **Einstellungen** und anschließend auf **SAML-Konfiguration**.
   b. Aktivieren Sie auf der Seite *SAML-Einstellungen* unter *Security Assertion Markup Language (SAML)* das Kontrollkästchen **SAML-Service-Provider aktivieren**.
5. Geben Sie im Abschnitt *Einstellungen für Remote Identity Provider (IdP)* Ihre IdP-Metadaten an, um Benutzer zu authentifizieren, indem Sie einen der folgenden Schritte ausführen.
   a. Klicken Sie auf **Metadaten aus IdP abrufen**.

b. Geben Sie im angezeigten Feld *IdP-Metadaten-URL* den Inhalt aus dem Feld *Verbundmetadaten-Dokument* ein, das Sie in 2.d aufgezeichnet haben, und klicken Sie auf **IdP-Metadaten importieren**.

Der Abschnitt *Einstellungen des Remote Identity Providers (IdP)* wird aktualisiert und zeigt die Details Ihrer IdP-Konfiguration an. Die aufgeführten Optionen geben die Weiterleitungen der Appliance-Seite während der SAML-Authentifizierung an. Weitere Informationen finden Sie unter https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security.

HINWEIS: Um diese Informationen während der SAML-Konfiguration jederzeit zu überprüfen, klicken Sie in diesem Abschnitt auf **Metadaten anzeigen**.

6. Stellen Sie im Abschnitt *Security Assertion Markup Language (SAML)* sicher, dass das Kontrollkästchen **IdP unterstützt keine passive Authentifizierung** aktiviert ist.
7. Wählen Sie im Abschnitt *IdP-Attributzuordnungen* die Option aus, die Sie verwenden möchten, um dem SAML-Benutzer Zugriff auf die Appliance zu gewähren.
   - **Lokale Benutzertabelle verwenden: Basiert auf der Benutzerliste, die lokal auf der Appliance gespeichert ist.**
   - **LDAP-Suche verwenden: Importiert Benutzerinformationen von einem externen LDAP-Server. Weitere Informationen hierzu finden Sie unter Verwenden eines LDAP-Servers zur Benutzerauthentifizierung.**
   - **Wählen Sie SAML verwenden aus, und legen Sie die folgenden Optionen fest:**
     - **UID**: http://schemas.microsoft.com/identity/claims/objectidentifier
     - **Anmeldung**: http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name
     - **Name**: http://schemas.microsoft.com/identity/claims/displayname
     - **Primäre E-Mail-Adresse**: http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name
8. Wenn Sie die Option **SAML verwenden** unter *Rollenzuordnung* ausgewählt haben, geben Sie die folgende Bedingung für die Rolle an, die Sie SAML-authentifizierten Benutzern gewähren möchten (z. B. die Rolle *Administrator*):

   `http://schemas.microsoft.com/ws/2008/06/identity/claims/groups` *entspricht* `<Objekt-ID>`

   Wobei `<Objekt-ID>` die Objekt-ID der Gruppe ist.
9. **Optional**. Um die Appliance-spezifischen SAML-Einstellungen auf der Appliance anzuzeigen, klicken Sie im Abschnitt *Lokale Einstellungen für Service Provider (SP)* auf **Metadaten anzeigen** und überprüfen Sie die angezeigten Optionen.

   Diese Felder enthalten Standardwerte und in den meisten Fällen müssen Sie keine Änderungen vornehmen.
10. Führen Sie folgende Schritte durch:
    a. Klicken Sie im Abschnitt *Einstellungen für lokalen Serviceprovider (SP)* auf **Metadaten anzeigen**.
    b. Suchen Sie im Microsoft Azure-Portal die neu erstellte Anwendungsregistrierung.
    c. Klicken Sie auf der Seite „App-Registrierung“ auf **Umleitungs-URL hinzufügen**.
    d. Wählen Sie im Abschnitt *Umleitungs-URIs* die Option **Web** aus, und legen Sie den Wert für *Verbrauchsdienst-URL für SP-Assertionen* auf der Seite *SAML-Einstellungen* unter *Lokale Einstellungen für Service Provider (SP)* fest.
    e. Legen Sie unter *Erweiterte Einstellungen* im Feld *URL abmelden* den Wert für *SP-SLO-Endpunkt (url)* im Abschnitt *Einstellungen für lokalen Serviceprovider (SP)* fest.
    f. Klicken Sie in Azure auf **Eine API verfügbar machen** und dann auf **Festlegen** neben *Anwendungs-ID-URI*. Legen Sie in diesem Feld den *SP-Entitäts-ID (uri)*-Wert aus dem Abschnitt *Lokale Einstellungen für Service Provider (SP)* fest.

g. Klicken Sie in Azure auf **Manifest**, und fügen Sie im rechts angezeigten Editor das Attribut `"groupMembershipClaims"` hinzu oder aktualisieren Sie dessen Wert auf `"SecurityGroup"` oder `"All"`.

Beispiel: `"groupMembershipClaims": "SecurityGroup",`

11. Klicken Sie auf **Speichern**.
12. Testen Sie Ihre SAML-Konfiguration.
    a. Melden Sie sich von der Appliance ab.
    b. Stellen Sie sicher, dass Sie bei Ihrem IdP-Konto angemeldet sind.
    c. Öffnen Sie die Willkommensseite von Administratorkonsole oder Benutzerkonsole.
    d. Klicken Sie auf **Anmelden**, ohne Ihre Benutzeranmeldedaten anzugeben.

    TIPP: Wenn SAML auf der Appliance aktiviert ist, klicken Sie auf **Lokale Anmeldung**, und geben Sie Ihre Benutzeranmeldedaten an.

    Die Seite **Administratorkonsole** oder **Benutzerkonsole** wird angezeigt.

Bereitstellen des KACE Agent auf verwalteten Geräten

Der KACE Agent ist eine Anwendung, die auf Geräten installiert werden kann, um Inventarberichte und andere Geräteverwaltungsfunktionen nutzen zu können. Auf verwalteten Geräten installierte KACE Agenten kommunizieren über das Agenten-Messaging-Protokoll mit der Appliance. Agenten führen geplante Aufgaben durch, beispielsweise das Erfassen von Inventarinformationen auf verwalteten Geräten und das Verteilen von Software an verwaltete Geräte.

Sie können den KACE Agent mithilfe einer der folgenden Methoden für verwaltete Geräte bereitstellen.

TIPP: Nur authentifizierte KACE Agenten können eine erfolgreiche Verbindung mit der Appliance herstellen. Weitere Informationen hierzu finden Sie unter Registrieren des KACE Agent bei der Appliance.

- **Bereitstellung des KACE Agent**: Mit dem Assistenten für die Agenten-Provisionierung können Sie den Agenten auf Geräten unter Windows, Mac OS X und Linux provisionieren. Im Assistenten können Sie wählen, ob Sie den Agenten mithilfe des Tools für die Gruppenrichtlinienobjekt-Provisionierung auf Windows-Geräten bereitstellen oder ob Sie die integrierte Provisionierung verwenden möchten, um den Agenten auf Geräten unter Windows, Mac OS X oder Linux bereitzustellen. Siehe Provisionierung des KACE Agent.
- **Manuelle Bereitstellung des KACE Agent**: Die manuelle Bereitstellung ist hilfreich, wenn die automatisierte Agenten-Provisionierung nicht praktikabel ist oder Sie die KACE Agent-Software per E-Mail oder mithilfe von Anmeldeskripten, einem Gruppenrichtlinienobjekt oder Active Directory bereitstellen möchten. Die Appliance enthält KACE Agent-Installationsprogramme für verschiedene Betriebssystemplattformen. Jede Plattform bietet eine oder mehrere Möglichkeiten zur Bereitstellung des KACE Agent. Die folgenden Abschnitte und ihre Unterthemen sind ein guter Einstieg:
    - KACE Agent auf Windows-Geräten manuell bereitstellen
    - KACE Agent auf Linux-Geräten manuell bereitstellen und aktualisieren
    - KACE Agent auf Mac-Geräten manuell bereitstellen und aktualisieren

Verwenden von Replikationsfreigaben

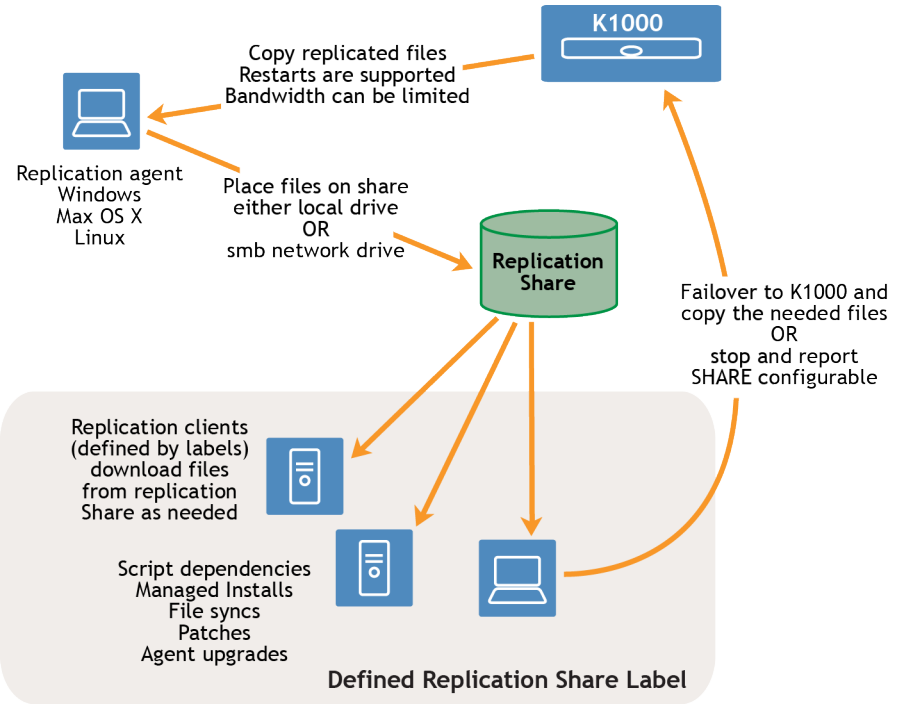
Replikationsfreigaben sind Geräte, die Kopien von Dateien zur Verteilung beibehalten. Sie sind insbesondere dann hilfreich, wenn Ihre verwalteten Geräte an mehreren geografischen Standorten bereitgestellt sind.

Mit Replikationsfreigaben kann beispielsweise ein Gerät in New York Dateien von einem anderen Gerät im selben Büro herunterladen anstatt von einer Appliance mit Standort in Los Angeles. Eine Replikationsfreigabe ist eine vollständige Replikation aller digitalen Assets und wird von der Appliance automatisch verwaltet. Sobald eine Replikationsfreigabe für ein Label angegeben wird, rufen Geräte in diesem Label Dateien von dieser Replikationsfreigabe ab.

Außerdem können Sie mithilfe von Replikationsfreigaben verwaltete Installationen, Patches oder Dell Aktualisierungen in Umgebungen bereitstellen, in denen Netzwerkbandbreite und Geschwindigkeit ein Problem sind. Replikationsfreigaben sind gute Alternativen zum direkten Herunterladen von einer Appliance.

Mithilfe von Replikationsfreigaben kann eine Appliance Anwendungs-Installationsprogramme, Patches, Upgrades und Skriptabhängigkeiten in einem freigegebenen Ordner auf einem Gerät replizieren. Wenn ein Replikationselement von der Appliance gelöscht wird, wird es in der Replikationsfreigabe zum Löschen markiert und im Replikationsaufgabenzyklus gelöscht. Die Abbildung zeigt die Konfiguration und Aufgabenablauf einer Replikationsfreigabe.

Replikationsfreigabenkonfiguration



Legen Sie zum Erstellen einer Replikationsfreigabe an jedem Remote-Standort ein Gerät als **Replikationsgerät** fest. Die Appliance kopiert alle Replikationselemente auf dem Replikationsgerät in das angegebene Zielverzeichnis. Der Replikationsprozess startet automatisch neu, wenn er aufgrund eines Netzwerkfehlers oder Replikationszeitplans angehalten wurde. Der Replikationsprozess startet dann an dem Punkt neu, an dem er angehalten wurde.

Sneakernet-Freigabe (Turnschuhnetzwerk): Sie können einen Ordner erstellen und den Inhalt eines vorhandenen Replikationsordners in diesen neuen Ordner kopieren. Anschließend können Sie diesen Ordner als neuen Replikationsordner in der Appliance festlegen. Die Appliance bestimmt, ob im neuen Ordner alle Replikationselemente vorhanden sind, und repliziert nur die neuen, um an Bandbreite zu sparen. Sie können

den Inhalt eines Replikationsordners manuell in einen neuen Ordner kopieren. Der auf einem Gerät erstellte Replikationsordner befolgt die folgende Hierarchie:

```
\\Computername\Ordnername\repl2\Ordner mit Replikationselementen
```

Gerätename und Ordnername werden vom Benutzer angegeben, während `repl2` automatisch von der Appliance erstellt wird. Der Ordner mit den Replikationselementen enthält den Ordner für Patches, kbots, Upgrade-Dateien und Anwendungen.

Alle Replikationselemente werden zunächst in der Replikationswarteschlange aufgeführt und dann nacheinander in das Zielverzeichnis kopiert. Jedes neue Replikationselement wird zuerst in der Replikationswarteschlange aufgeführt und nach einem Intervall von 10 Minuten kopiert.

Replikationselemente werden in der folgenden Reihenfolge kopiert:

1. Skriptabhängigkeiten
2. Anwendungen
3. Agenten-Upgrades
4. Patches

Replikationsfreigaben erstellen

Sie können Replikationsfreigaben auf verwalteten Geräten erstellen.

Um eine Replikationsfreigabe zu erstellen, müssen Sie:

- Zum Schreiben der Softwaredateien eine **Schreibberechtigung** für den Zielpfad besitzen.
- Den KACE Agent auf der Replikationsfreigabe installiert haben.
- Erstellen Sie ein Label für Ihre Geräte, bevor Sie mit dem Vorgang beginnen.

Replikationsfreigaben können nur auf Geräten erstellt werden, die im Inventar in der Liste *Geräte* angezeigt werden. Befindet sich das gewünschte Gerät nicht in der Liste *Geräte*, müssen Sie einen Inventardatensatz für das Gerät erstellen, bevor Sie es als Replikationsfreigabe verwenden können.

Siehe Verwalten von Inventarinformationen.

1. Rufen Sie die Seite *Detail zum Replikationszeitplan* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Verteilung** und anschließend auf **Replikation**.
   c. Wählen Sie **Aktion auswählen** > **Neu**.
2. Aktivieren Sie im Abschnitt *Konfigurieren* das Kontrollkästchen **Aktiviert**.
3. **Optional**: Klicken Sie auf **Failover zur Appliance**, um die Appliance zu verwenden, wenn die Replikationsfreigabe nicht verfügbar ist.

   HINWEIS: Aktivieren Sie **Failover zur Appliance** erst, nachdem Sie die Replikationsfreigabe getestet haben.
4. Wählen Sie in der Dropdown-Liste *Gerät* das Gerät aus, das Sie als Replikationsfreigabe verwenden möchten.

Es gibt zwei Möglichkeiten, die Replikationsfreigabe zu erstellen:

- **Lokal**
- **Auf einem freigegebenen Netzlaufwerk**

5. Wählen Sie das **Betriebssystem** und die **Gebietsschemata** der Patches aus, die repliziert werden sollen. Die Listen werden basierend auf den im Patch-Abonnement ausgewählten Betriebssystemen und Gebietsschemata ausgefüllt.
6. Aktivieren Sie die Kontrollkästchen **Anwendungs-Patches einschließen** und **Windows-Funktionsaktualisierungen einschließen** und **Dell-Aktualisierungen einschließen**, um die Patch- und Aktualisierungsdateien in die Replikationsfreigabe zu kopieren.
7. Geben Sie die Einstellungen *Zielfreigabe* an:

Option	Beschreibung
Pfad	Der Verzeichnispfad, den das Replikationsgerät für die Replikationsfreigabe verwendet. Anwendungen werden von der Appliance an diesen Speicherort kopiert. Verwenden Sie für ein lokales Laufwerk die Syntax für lokale Laufwerke, zum Beispiel: `C:\`**kace_sma_share** Verwenden Sie für ein Netzlaufwerk das UNC-Format, zum Beispiel: `\\`**kaceRep**`\`**kace_sma_share**`\` **HINWEIS:** Die Schreibweise mit **$**, z. B. `\\`**KaceRep**`\e$`, wird nicht unterstützt.
Lokale Freigabe oder **UNC**	Wählen Sie aus, ob eine lokale Freigabe oder UNC verwendet werden soll.
Anmeldeinformationen	Die Details des Dienstkontos, die erforderlich sind, um eine Verbindung zum Gerät herzustellen und Befehle auszuführen Wählen Sie vorhandene Anmeldeinformationen in der Dropdown-Liste aus oder wählen Sie **Neue Anmeldeinformationen hinzufügen** aus, um nicht bereits aufgeführte Anmeldeinformationen hinzuzufügen. Siehe Hinzufügen und Bearbeiten von Benutzer-/Kennwort-Anmeldeinformationen.
Label	Das Label der Geräte, die die Replikationsfreigabe verwenden. Prüfen Sie, ob für das ausgewählte Label die Zeichenfolge KACE_ALT_LOCATION nicht festgelegt wurde. KACE_ALT_LOCATION hat beim Herunterladen von Dateien auf Geräte Vorrang gegenüber der Replikationsfreigabe.

8. Geben Sie die Einstellungen für *Freigabe herunterladen* an:

Option	Beschreibung
Pfad	Der Pfad, der von Geräten im Replikationslabel verwendet wird, um Elemente vom Replikationslaufwerk zu kopieren. Geben Sie beispielsweise einen UNC-Pfad ein:

Option	Beschreibung
	`\\Dateiservername\Verzeichnis\kace_sma\` Andere Geräte benötigen zum Kopieren von Replikationselementen aus diesem freigegebenen Ordner eine **Leseberechtigung**.
Anmeldeinformationen	Die Details des Dienstkontos, die erforderlich sind, um eine Verbindung zum Gerät herzustellen und Befehle auszuführen Wählen Sie vorhandene Anmeldeinformationen in der Dropdown-Liste aus oder wählen Sie **Neue Anmeldeinformationen hinzufügen** aus, um nicht bereits aufgeführte Anmeldeinformationen hinzuzufügen. Siehe Hinzufügen und Bearbeiten von Benutzer-/Kennwort-Anmeldeinformationen.

9. Geben Sie im Abschnitt *Zeitplan* die folgenden Einstellungen an:

Option	Beschreibung
Hohe Bandbreite	Die maximale Bandbreite für die Verwendung bei der Replikation. Wenn Sie in dieses Feld keinen Wert eingeben, wird für die Replikation die maximal verfügbare Bandbreite verwendet. Dieses Feld wird in Byte pro Sekunde angegeben.
Niedrige Bandbreite	Die eingeschränkte Bandbreite für die Verwendung bei der Replikation. Wenn Sie in dieses Feld keinen Wert eingeben, wird für die Replikation die maximal verfügbare Bandbreite verwendet. Dieses Feld wird in Byte pro Sekunde angegeben.
Zeitplanübersicht	Die Bandbreite, die jeden Tag der Woche rund um die Uhr verwendet wird (24-Stunden-Format) • Um die Bandbreitenauswahl zu ändern, klicken Sie in ein Kästchen. • Um die Stunden (Spalten) auszuwählen, klicken Sie auf die Stundenzahl. • Um die Tage (Zeilen) auszuwählen, klicken Sie auf den Wochentag. Die Bandbreite ist farbcodiert: • **Weiß**: Replikation ist ausgeschaltet • **Hellblau**: Replikation ist mit niedriger Bandbreite aktiviert • **Blau**: Replikation ist mit hoher Bandbreite aktiviert
Zeitplan kopieren von	Wählen Sie in der Dropdown-Liste einen vorhandenen Replikationszeitplan aus, um Replikationselemente gemäß diesem Zeitplan zu replizieren.

Option	Beschreibung
Anmerkungen	Geben Sie nach Bedarf beliebige weitere Informationen ein.

10. Klicken Sie auf **Speichern**.

    Die Seite *Replikation* wird angezeigt.
11. **Optional**: Kehren Sie nach dem Testen der Replikationsfreigabe zu 3 zurück und aktivieren Sie **Failover zur Appliance**.

Verwandte Themen

Manuelle Labels hinzufügen oder bearbeiten

Informationen zur Patch-Verwaltung

Details zu Replikationsfreigaben anzeigen

Sie können Details zu den Geräten anzeigen, die als Replikationsfreigaben verwendet werden.

1. Rufen Sie die Liste *Replikation* auf:
    a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
    b. Klicken Sie in der linken Navigationsleiste auf **Verteilung** und anschließend auf **Replikation**.

    Auf dieser Seite wird eine Liste der Replikationsfreigaben angezeigt, die auf der Appliance zur Verfügung stehen. Für jede Replikationsfreigabe zeigt eine Standardansicht deren *Status*, die *Aufgabe* der Replikation, das zugehörige *Gerät*, den *Zielpfad*, die KACE *Agenten-Version*, das *Kennzeichen*, eine Angabe, ob die Replikationsfreigabe *aktiviert* ist, sowie die Anzahl der noch zu kopierenden Dateien und die Gesamtgröße der zu kopierenden Dateien (in der Spalte *ToDo*) an. Die Informationen, die in der Spalte *ToDo* angezeigt werden, ermöglichen Ihnen, den Status des Replikationsprozesses für jede Replikationsfreigabe in der Liste zu prüfen, statt dass Sie die einzelnen Freigaben überprüfen müssen, um festzustellen ob ihr Replikationsprozess abgeschlossen wurde.
2. Klicken Sie in der Spalte *Geräte* auf den Namen einer Replikationsfreigabe, um die Seite *Detail zum Replikationszeitplan* anzuzeigen.

    Auf dieser Seite können Sie folgende Aufgaben ausführen:

    - **Die Replikationswarteschlange anzeigen**: Wenn Sie Elemente in der Warteschlange für die Replikation anzeigen möchten, klicken Sie unterhalb der Konfigurationsinformationen auf **Replikationswarteschlange anzeigen**. Diese Ansicht wird beim Öffnen der Seite standardmäßig angezeigt.
    - **Das Replikationsinventar anzeigen**: Wenn Sie auf der Freigabe replizierte Elemente anzeigen möchten, klicken Sie unterhalb der Konfigurationsinformationen auf **Freigabe-Inventar anzeigen**.
    - **Die Replikationswarteschlange löschen**: Wenn Sie Replikationselemente anzeigen möchten, die zum Löschen gekennzeichnet sind, klicken Sie unterhalb der Konfigurationsinformationen auf **'Löschen der Warteschlange' anzeigen**.

Verwalten von Anmeldeinformationen

Die Appliance ermöglicht es Ihnen, Benutzernamen und Kennwörter, die für die Anmeldung bei anderen Systemen wie Computern und Servern oder für die Google- oder SNMP-Authentifizierung erforderlich sind, zentral zu verwalten.

Anmeldeinformationen, die zur Seite *Verwaltung der Anmeldeinformationen* hinzugefügt wurden, stehen über Dropdown-Listen in den Abschnitten *Inventar* (Suche, Bestand und Geräteverwaltung ohne Agenten-Software), *Verteilung* (verwaltete Installationen, Dateisynchronisierungen und Replikation) und *Skripterstellung* (Konfigurationsrichtlinien und Sicherheitsrichtlinien) zur Auswahl zur Verfügung.

Darüber hinaus werden Anmeldeinformationen, die auf der Seite *Verwaltung der Anmeldeinformationen* geändert werden, in allen Komponenten der Appliance aktualisiert, in denen sie verwendet werden. Sie müssen nicht jedes Element, das die Anmeldeinformationen verwendet, separat aktualisieren.

Die Anmeldeinformationen, die Sie zur Appliance hinzufügen, müssen mit denen auf den Zielsystemen übereinstimmen. Wenn Sie die Anmeldeinformationen auf den Zielsystemen ändern, müssen Sie sie auch auf der Seite *Verwaltung der Anmeldeinformationen* für die Appliance ändern.

Wenn auf der Appliance die Organisationskomponente aktiviert ist, können Sie Anmeldeinformationen für jede Organisation separat verwalten.

HINWEIS: Die Dropdown-Liste "Verwaltung der Anmeldeinformationen" ist nicht auf LDAP-Konfigurationsseiten verfügbar. Die Funktion wird nicht für die Verwaltung von Benutzeranmeldeinformationen für den Zugriff auf die **Administratorkonsole** oder **Benutzerkonsole** der Appliance verwendet, die eine einmalige Anmeldung und LDAP-Authentifizierung nutzen. Siehe Informationen zu Benutzerkonten und Benutzerauthentifizierung.

Verfolgen von Änderungen in der Verwaltung der Anmeldeinformationen

Wenn Verlaufsabonnements zur Aufbewahrung von Informationen konfiguriert wurden, können Sie Details zu den an Einstellungen, Assets und Objekten vorgenommenen Änderungen anzeigen. Diese Informationen beinhalten auch das Datum der Erstellung, Änderung oder Löschung sowie den Benutzer, der die Aktion durchgeführt hat. Dies kann beim Beheben von Störungen nützlich sein.

Siehe Informationen zu den Verlaufseinstellungen.

Geheimschlüssel-Anmeldeinformationen hinzufügen und bearbeiten

Fügen Sie die Geheimschlüssel-Anmeldeinformationen zur Seite *Verwaltung der Anmeldeinformationen* hinzu, um die Verwaltung der für das Inventar, die Verteilung und die Skripterstellung verwendeten SNMP-Anmeldeinformationen zu vereinfachen. Geheimschlüssel-Anmeldeinformationen können für Geräte erstellt werden, die mithilfe des KACE Cloud Mobile Device Managers verwaltet werden.

- Sie haben den Geheimschlüssel des KACE Cloud Mobile Device Manager.
- Sie verfügen über Administratorrechte in der **Administratorkonsole**.

Nach dem Hinzufügen von Anmeldeinformationen können Sie diese auf Konfigurationsseiten auswählen, statt sie jedes Mal manuell einzugeben. Außerdem können Sie von allen Konfigurationsseiten, auf denen

sie verwendet werden, Anmeldeinformationen hinzufügen. Auf Konfigurationsseiten hinzugefügte Anmeldeinformationen werden automatisch zur Seite *Verwaltung der Anmeldeinformationen* **hinzugefügt.**

1. Rufen Sie die Seite *Verwaltung der Anmeldeinformationen* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie auf der linken Navigationsleiste auf **Einstellungen** und anschließend auf **Anmeldeinformationen**.
2. Wählen Sie **Aktion auswählen > Neu**.
3. Geben Sie in dem Formular *Anmeldeinformationen hinzufügen* die Eigenschaften der Anmeldeinformationen an:

   HINWEIS: Auf dieses Formular können Sie auch von Seiten zugreifen, auf denen Anmeldeinformationen verwendet werden, z. B. von der Seite *Detail zum Erkennungszeitplan*. Auf diesen Seiten hinzugefügte Anmeldeinformationen werden automatisch zur Liste *Verwaltung der Anmeldeinformationen* hinzugefügt.

Option	Beschreibung
Name	Ein eindeutiger Name für die Anmeldeinformationen. Dieser Name wird in der Liste *Verwaltung der Anmeldeinformationen* und in den Dropdown-Listen für die Auswahl der Anmeldeinformationen in den Komponentenabschnitten angezeigt, z. B. bei der Skripterstellung. Dieser Name dient zur Identifikation in der **Administratorkonsole** und gehört nicht zu den eigentlichen Anmeldeinformationen auf dem Zielgerät.
Typ	Die Klassifizierung der Anmeldeinformationen. Wählen Sie **Geheimer Schlüssel** aus, um Anmeldeinformationen anzugeben, die geheime Schlüssel vom KACE Cloud Mobile Device Manager enthalten.
Geheim	Der geheime Schlüssel der KACE Cloud Mobile Device Manager-Umgebung.
Zeichen anzeigen	Anzeigen der Zeichen im Feld *Kennwort* in dem Formular *Anmeldeinformationen hinzufügen*. Diese Option ist nur verfügbar, wenn Sie Anmeldeinformationen hinzufügen. Wenn Sie vorhandene Anmeldeinformationen bearbeiten, können die Kennwortzeichen nicht angezeigt werden.
Anmerkungen	Weitere Informationen, die Sie zu den Anmeldeinformationen angeben möchten.

4. Klicken Sie auf **Speichern**.

   Die Anmeldeinformationen werden in der Liste *Verwaltung der Anmeldeinformationen* angezeigt und stehen für die Auswahl in Komponenten zur Verfügung, in denen Anmeldeinformationen verwendet werden.

Hinzufügen und Bearbeiten von Benutzer-/Kennwort-Anmeldeinformationen

Fügen Sie die folgenden Anmeldeinformationen zur Seite *Verwaltung der Anmeldeinformationen* hinzu, um die Verwaltung der für das Inventar, die Verteilung und die Skripterstellung verwendeten Benutzer- und Kennwort-Anmeldeinformationen zu vereinfachen. Benutzer-/Kennwort-Anmeldeinformationen können für Mac, Windows und Linux Betriebssysteme sowie für VMware ESXi-Hosts and vCenter-Server erstellt werden.

- Sie verfügen über die Benutzernamen und Kennwörter der Anmeldeinformationen, die Sie verwalten möchten.
- Sie verfügen über Administratorrechte in der **Administratorkonsole**.

Nach dem Hinzufügen von Anmeldeinformationen können Sie diese auf Konfigurationsseiten auswählen, statt sie jedes Mal manuell einzugeben. Außerdem können Sie von allen Konfigurationsseiten, auf denen sie verwendet werden, Anmeldeinformationen hinzufügen. Auf Konfigurationsseiten hinzugefügte Anmeldeinformationen werden automatisch zur Seite *Verwaltung der Anmeldeinformationen* **hinzugefügt.**

1. Rufen Sie die Seite *Verwaltung der Anmeldeinformationen* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie auf der linken Navigationsleiste auf **Einstellungen** und anschließend auf **Anmeldeinformationen**.
2. Wählen Sie **Aktion auswählen** > **Neu**.
3. Geben Sie in dem Formular *Anmeldeinformationen hinzufügen* die Eigenschaften der Anmeldeinformationen an:

   HINWEIS: Auf dieses Formular können Sie auch von Seiten zugreifen, auf denen Anmeldeinformationen verwendet werden, z. B. von der Seite *Detail zum Erkennungszeitplan*. Auf diesen Seiten hinzugefügte Anmeldeinformationen werden automatisch zur Liste *Verwaltung der Anmeldeinformationen* hinzugefügt.

Option	Beschreibung
Name	Ein eindeutiger Name für die Anmeldeinformationen. Dieser Name wird in der Liste *Verwaltung der Anmeldeinformationen* und in den Dropdown-Listen für die Auswahl der Anmeldeinformationen in den Komponentenabschnitten angezeigt, z. B. bei der Skripterstellung. Dieser Name dient zur Identifikation in der **Administratorkonsole** und gehört nicht zu den eigentlichen Anmeldeinformationen auf dem Zielgerät.
Typ	Die Klassifizierung der Anmeldeinformationen. Wählen Sie **Benutzer/Kennwort** aus, um Anmeldeinformationen mit Benutzernamen und Kennwörtern anzugeben.
Benutzer oder Domain\Benutzer	Der für die Anmeldeinformationen erforderliche Benutzername.

Option	Beschreibung
	TIPP: Für einige Windows Konfigurationen kann das Format `Domain\Benutzer` erforderlich sein.
Kennwort	Das für die Anmeldeinformationen erforderliche Kennwort.
Zeichen anzeigen	Anzeigen der Zeichen im Feld *Kennwort* in dem Formular *Anmeldeinformationen hinzufügen*. Diese Option ist nur verfügbar, wenn Sie Anmeldeinformationen hinzufügen. Wenn Sie vorhandene Anmeldeinformationen bearbeiten, können die Kennwortzeichen nicht angezeigt werden.
Ziele	Die Gerätetypen, bei denen die Anmeldeinformationen verwendet werden können. **TIPP:** Sie können mehrere Gerätetypen oder Betriebssysteme auswählen. Letzteres ist der Fall, wenn die angegebenen Anmeldeinformationen für die Authentifizierung auf mehreren Betriebssystemen verwendet werden können.
Anmerkungen	Weitere Informationen, die Sie zu den Anmeldeinformationen angeben möchten.

4. Klicken Sie auf **Speichern**.

   Die Anmeldeinformationen werden in der Liste *Verwaltung der Anmeldeinformationen* angezeigt und stehen für die Auswahl in Komponenten zur Verfügung, in denen Anmeldeinformationen verwendet werden.

Hinzufügen und Bearbeiten von LDAP-Benutzer-/Kennwort-Anmeldeinformationen

Um Kennwörter für LDAP-Anmeldeinformationen einfach zu verwalten, fügen Sie diese Anmeldeinformationen der Seite *Verwaltung der Anmeldeinformationen* hinzu. Benutzername und Kennwort für LDAP können für Mac-, Windows- und Linux-Betriebssysteme erstellt werden.

- Sie verfügen über die LDAP-Benutzernamen und -Kennwörter der Anmeldeinformationen, die Sie verwalten möchten.
- Sie verfügen über Administratorrechte in der **Administratorkonsole**.

Nach dem Hinzufügen von Anmeldeinformationen können Sie diese auf Konfigurationsseiten auswählen, statt sie jedes Mal manuell einzugeben. Außerdem können Sie von allen Konfigurationsseiten, auf denen sie verwendet werden, Anmeldeinformationen hinzufügen. Auf Konfigurationsseiten hinzugefügte Anmeldeinformationen werden automatisch zur Seite *Verwaltung der Anmeldeinformationen* **hinzugefügt.**

1. Rufen Sie die Seite *Verwaltung der Anmeldeinformationen* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.

b. Klicken Sie auf der linken Navigationsleiste auf **Einstellungen** und anschließend auf **Anmeldeinformationen**.

2. Wählen Sie **Aktion auswählen** > **Neu**.
3. Geben Sie in dem Formular *Anmeldeinformationen hinzufügen* die Eigenschaften der Anmeldeinformationen an:

> **HINWEIS:** Auf dieses Formular können Sie auch von Seiten zugreifen, auf denen Anmeldeinformationen verwendet werden, z. B. von der Seite *Detail zum Erkennungszeitplan*. Auf diesen Seiten hinzugefügte Anmeldeinformationen werden automatisch zur Liste *Verwaltung der Anmeldeinformationen* hinzugefügt.

Option	Beschreibung
Name	Ein eindeutiger Name für die Anmeldeinformationen. Dieser Name wird in der Liste *Verwaltung der Anmeldeinformationen* und in den Dropdown-Listen für die Auswahl der Anmeldeinformationen auf der Seite *LDAP-Labeldetail* angezeigt. Dieser Name dient zur Identifikation in der **Administratorkonsole** und gehört nicht zu den eigentlichen Anmeldeinformationen auf dem Zielgerät.
Typ	Die Klassifizierung der Anmeldeinformationen. Wählen Sie **LDAP User/Password (LDAP-Benutzer/Kennwort)** aus, um LDAP-Anmeldeinformationen anzugeben, die Benutzernamen und Kennwörter enthalten.
Benutzer oder Domain\Benutzer	Der für die Anmeldeinformationen Benutzername. **TIPP:** Für einige Windows Konfigurationen kann das Format `Domäne\Benutzer` erforderlich sein.
Kennwort	Das für die Anmeldeinformationen erforderliche Kennwort.
Zeichen anzeigen	Anzeigen der Zeichen im Feld *Kennwort* in dem Formular *Anmeldeinformationen hinzufügen*. Diese Option ist nur verfügbar, wenn Sie Anmeldeinformationen hinzufügen. Wenn Sie vorhandene Anmeldeinformationen bearbeiten, können die Kennwortzeichen nicht angezeigt werden.
Anmerkungen	Weitere Informationen, die Sie zu den Anmeldeinformationen angeben möchten.

4. Klicken Sie auf **Speichern**.

   Die Anmeldeinformationen werden in der Liste *Verwaltung der Anmeldeinformationen* angezeigt und stehen für die Auswahl in Komponenten zur Verfügung, in denen Anmeldeinformationen verwendet werden.

Hinzufügen und Bearbeiten von Google OAuth-Anmeldeinformationen

Fügen Sie die folgenden Anmeldeinformationen zur Seite *Verwaltung der Anmeldeinformationen* hinzu, um die Verwaltung der für das Inventar, die Verteilung, die Skripterstellung und den Service Desk verwendeten Google OAuth-Anmeldeinformationen zu vereinfachen.

- Sie verfügen über eine Domain vom Typ "Google Apps for Business" oder "Google Apps for Education" mit Unterstützung der Chrome-Geräteverwaltung.
- Sie verfügen über ein Google-Administratorkonto, das der Geschäfts- oder Bildungsdomain angehört. Dem Konto muss die Superuser-Rolle zugewiesen sein.
- Sie verfügen über ein als Entwicklerkonto verwendetes Google-Konto und haben eine Google-Anwendung mit einer Client-ID und einem geheimen Client-Schlüssel erstellt. Weitere Informationen finden Sie unter https://support.google.com/googleapi/answer/6158849?hl=en.
- Sie verfügen über Administratorrechte in der **Administratorkonsole**.

Nach dem Hinzufügen von Anmeldeinformationen können Sie diese auf Konfigurationsseiten auswählen, statt sie jedes Mal manuell einzugeben. Außerdem können Sie von allen Konfigurationsseiten, auf denen sie verwendet werden, Anmeldeinformationen hinzufügen. Auf Konfigurationsseiten hinzugefügte Anmeldeinformationen werden automatisch zur Seite *Verwaltung der Anmeldeinformationen* **hinzugefügt. Die Appliance validiert die gespeicherten Google OAuth-Anmeldeinformationen nicht während der Eingabe, aber der Versuch, Änderungen mit ungültigen Anmeldeinformationen zu speichern, führt zu einem Fehler.**

1. Rufen Sie die Seite *Verwaltung der Anmeldeinformationen* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie auf der linken Navigationsleiste auf **Einstellungen** und anschließend auf **Anmeldeinformationen**.
2. Wählen Sie **Aktion auswählen** > **Neu**.
3. Geben Sie in dem Formular *Anmeldeinformationen hinzufügen* die Eigenschaften der Anmeldeinformationen an:

Option	Beschreibung
Name	Ein eindeutiger Name für die Anmeldeinformationen. Dieser Name wird in der Liste *Verwaltung der Anmeldeinformationen* und in den Dropdown-Listen für die Auswahl der Anmeldeinformationen in den Komponentenabschnitten angezeigt, z. B. bei der Skripterstellung. Dieser Name dient zur Identifikation in der **Administratorkonsole** und gehört nicht zu den eigentlichen Anmeldeinformationen.
Typ	Die Klassifizierung der Anmeldeinformationen. Wählen Sie **Google OAuth** aus, um die Anmeldeinformationen für Chrome-Geräte anzugeben.
Client-ID	Ihre Google Developer API-Client-ID.

Option	Beschreibung
Geheimer Client-Schlüssel	Ihr geheimer Google Developer API-Clientschlüssel.
Zeichen anzeigen	Anzeigen der Zeichen im Feld *Geheimer Client-Schlüssel* in dem Formular *Anmeldeinformationen hinzufügen*. Diese Option ist nur verfügbar, wenn Sie Anmeldeinformationen hinzufügen. Wenn Sie vorhandene Anmeldeinformationen bearbeiten, können die Zeichen im Feld *Geheimer Client-Schlüssel* nicht angezeigt werden.
Genehmigungscode	Der Genehmigungscode für den Zugriff. Um diesen Code abzurufen, geben Sie Ihre *Client-ID* und Ihren *geheimen Client-Schlüssel* an und klicken dann auf **Neuen Code erstellen**.
Neuen Code erstellen	Ein Link zum Codegenerator. So erstellen Sie einen neuen Code: a. Klicken Sie auf **Neuen Code erstellen**. b. Melden Sie sich auf der Google-Anmeldeseite mit den Anmeldeinformationen Ihres Google-Administratorkontos an. Wenn die Google-Anmeldeseite nicht erscheint, sind die Anmeldeinformationen für Ihr Google-Konto bereits gespeichert. Handelt es sich bei dem gespeicherten Konto nicht um das bevorzugte Administratorkonto, melden Sie sich ab und mit dem bevorzugten Administratorkonto wieder an. **Nur Service Desk-E-Mail-Konfiguration.** Möglicherweise müssen Sie sicherstellen, dass die App, die auf Ihr Benutzerkonto zugreift, von Google überprüft wird, oder die App über die *Erweiterten Einstellungen* auf Ihr Konto zugreifen kann. Klicken Sie im angezeigten Dialogfeld *Mit Google anmelden* auf **Zulassen**, damit die App ungelesene E-Mail-Nachrichten abrufen, als gelesen markieren und die Ordnerstruktur ändern kann. c. Klicken Sie auf **Akzeptieren**, um einen Code zu generieren, mit dem die Appliance Zugriff erhält und Benutzer sowie Geräte mit Chrome-Betriebssystem in der Google-Domain anzeigen kann. d. Kopieren Sie den generierten Code und schließen Sie das Google-Fenster. e. Fügen Sie den Code in das Feld *Genehmigungscode* ein.
Anmerkungen	Weitere Informationen, die Sie zu den Anmeldeinformationen angeben möchten.

4. Klicken Sie auf **Speichern**.

   Die Anmeldeinformationen stehen für die Auswahl in Komponenten zur Verfügung, in denen Anmeldeinformationen verwendet werden.

Hinzufügen und Bearbeiten von SNMP-Anmeldeinformationen

Fügen Sie die folgenden Anmeldeinformationen zur Seite *Verwaltung der Anmeldeinformationen* hinzu, um die Verwaltung der für das Inventar, die Verteilung und die Skripterstellung verwendeten SNMP-Anmeldeinformationen zu vereinfachen.

- Sie verfügen über die für die SNMP-Authentifizierung erforderlichen Informationen.
- Sie verfügen über Administratorrechte in der **Administratorkonsole**.

Nach dem Hinzufügen von Anmeldeinformationen können Sie diese auf Konfigurationsseiten auswählen, statt sie jedes Mal manuell einzugeben. Außerdem können Sie von allen Konfigurationsseiten, auf denen sie verwendet werden, Anmeldeinformationen hinzufügen. Auf Konfigurationsseiten hinzugefügte Anmeldeinformationen werden automatisch zur Seite *Verwaltung der Anmeldeinformationen* **hinzugefügt.**

1. Rufen Sie die Seite *Verwaltung der Anmeldeinformationen* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie auf der linken Navigationsleiste auf **Einstellungen** und anschließend auf **Anmeldeinformationen**.
2. Wählen Sie **Aktion auswählen** > **Neu**.
3. Geben Sie in dem Formular *Anmeldeinformationen hinzufügen* die folgenden Informationen ein:

Option	Beschreibung
Name	Ein eindeutiger Name für die Anmeldeinformationen. Dieser Name wird in der Liste *Verwaltung der Anmeldeinformationen* und in den Dropdown-Listen für die Auswahl der Anmeldeinformationen in den Komponentenabschnitten angezeigt, z. B. bei der Skripterstellung. Dieser Name dient zur Identifikation in der **Administratorkonsole** und gehört nicht zu den eigentlichen Anmeldeinformationen.
Typ	Die Klassifizierung der Anmeldeinformationen. Wählen Sie **SNMP** aus, um die SNMP-Anmeldeinformationen anzugeben.

4. Geben Sie für SNMP v1 oder v2c die folgenden Informationen an:

Option	Beschreibung
SNMP v1 oder v2c	Für die SNMP-Anmeldeinformationen wird weder eine Authentifizierung noch eine Verschlüsselung verwendet.
Communityzeichenfolge	Für SNMP v1 oder v2c, die abzufragende Communityzeichenfolge. Der Standardwert ist **Öffentlich**. SNMP v1 bzw. v2c erfordern die öffentliche Zeichenfolge.

Option	Beschreibung
Anmerkungen	Weitere Informationen, die Sie zu den Anmeldeinformationen angeben möchten.

5. Geben Sie für SNMP v3 die folgenden Informationen an:

Option	Beschreibung
SNMP v3	SNMP-Anmeldeinformationen, die Authentifizierungs- und Verschlüsselungsalgorithmen zur Erhöhung der Sicherheit erfordern.
Sicherheitsname	Der Name des USM-Benutzerkontos (benutzerbasiertes Sicherheitsmodell) für SNMP v3. Dieses Konto und alle für die Authentifizierung und Verschlüsselung erforderlichen Kennwörter müssen auf den Zielgeräten eingerichtet werden.
Sicherheitsstufe	Die Sicherheitsstufe für SNMP v3. Mögliche Sicherheitsstufen: • **authPriv**: Die höchste SNMP v3-Sicherheitsstufe, die sowohl Authentifizierung als auch Verschlüsselung verwendet. Um diese Sicherheitsstufe zu verwenden, müssen Sie sämtliche SNMP v3-Authentifizierungs- und Datenschutzeinstellungen festlegen. • **authNoPriv**: Die mittlere SNMP v3-Sicherheitsstufe, die nur Authentifizierung verwendet. Datenübertragungen werden nicht verschlüsselt. Um diese Sicherheitsstufe zu verwenden, müssen Sie die Authentifizierungseinstellungen festlegen. • **noAuthNoPriv**: Die niedrigste SNMP v3-Sicherheitsstufe. Datenübertragungen werden nicht verschlüsselt.
Authentifizierungskennwort	Das Kennwort zum Authentifizieren von Datenübertragungen bei Auswahl der Sicherheitsstufen **authPriv** oder **authNoPriv** für SNMP v3. Dieses Kennwort ist mit dem USM-Benutzer verknüpft und muss auf den Zielgeräten eingerichtet werden.
Protokoll	Das für Datenübertragungen verwendete Protokoll für SNMP v3. Die Protokolle beinhalten: • **SHA**: Sicherer Hash-Algorithmus, SHA-1 • **MD5**: Message Digest 5. Schneller als SHA, gilt aber als nicht so sicher.
Datenschutzkennwort	Das Kennwort zum Authentifizieren von Datenübertragungen mit der Sicherheitsstufe **authPriv** für SNMP v3. Dieses Kennwort ist mit

Option	Beschreibung
	dem USM-Benutzer verknüpft und muss auf den Zielgeräten eingerichtet werden.
Protokoll	Das für das Datenschutzkennwort verwendete Protokoll für SNMP v3. Die Protokolle beinhalten: • **DES**: Data Encryption Standard (Datenverschlüsselungsstandard). Dieser Algorithmus verwendet eine Schlüssellänge von 56 Bit und gilt als nicht so sicher wie AES. • **AES**: Advanced Encryption Standard (Erweiterter Verschlüsselungsstandard). Die Appliance unterstützt eine Schlüssellänge von 128 Bit.
Anmerkungen	Weitere Informationen, die Sie zu den Anmeldeinformationen angeben möchten.

6. Klicken Sie auf **Speichern**.

   Die Anmeldeinformationen stehen für die Auswahl in Komponenten zur Verfügung, in denen Anmeldeinformationen verwendet werden.

Microsoft Office 365 OAuth-Anmeldeinformationen hinzufügen und bearbeiten

Zur einfachen Verwendung der Office 365-Anmeldeinformationen, die in der Service Desk-E-Mail-Kommunikation verwendet werden, fügen Sie sie auf der Seite *Verwaltung der Anmeldeinformationen* hinzu.

- Sie verfügen über ein Office 365-Konto und haben eine Microsoft Active Directory-Anwendung in Microsoft Azure mit einer Client-ID und einem geheimen Client-Schlüssel erstellt. Weitere Informationen finden Sie unter https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-create-service-principal-portal.
- Sie verfügen über Administratorrechte in der **Administratorkonsole**.

Nach dem Hinzufügen von Anmeldeinformationen können Sie diese auf Konfigurationsseiten auswählen, statt sie jedes Mal manuell einzugeben. Außerdem können Sie von allen Konfigurationsseiten, auf denen sie verwendet werden, Anmeldeinformationen hinzufügen. Auf Konfigurationsseiten hinzugefügte Anmeldeinformationen werden automatisch zur Seite *Verwaltung der Anmeldeinformationen* hinzugefügt. Die Appliance validiert die gespeicherten Office 365-Anmeldeinformationen nicht während der Eingabe, aber der Versuch, Änderungen mit ungültigen Anmeldeinformationen zu speichern, führt zu einem Fehler.

HINWEIS: Diese Funktion ist nur verfügbar, wenn sicherer SSL-Zugriff auf die Appliance aktiviert ist. Weitere Informationen hierzu finden Sie unter Sicherheitseinstellungen für die Appliance konfigurieren.

1. Rufen Sie die Seite *Verwaltung der Anmeldeinformationen* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.

b. Klicken Sie auf der linken Navigationsleiste auf **Einstellungen** und anschließend auf **Anmeldeinformationen**.

2. Wählen Sie **Aktion auswählen** > **Neu**.
3. Geben Sie in dem Formular *Anmeldeinformationen hinzufügen* die Eigenschaften der Anmeldeinformationen an:

Option	Beschreibung
Name	Ein eindeutiger Name für die Anmeldeinformationen. Dieser Name wird in der Liste *Verwaltung der Anmeldeinformationen* und in den Dropdown-Listen für die Auswahl der Anmeldeinformationen in den Komponentenabschnitten angezeigt, z. B. Service Desk-E-Mail-Einstellungen. Dieser Name dient zur Identifikation in der **Administratorkonsole** und gehört nicht zu den eigentlichen Anmeldeinformationen.
Typ	Die Klassifizierung der Anmeldeinformationen. Wählen Sie **Office365 OAuth (OAuth für Office 365)** aus, um die Anmeldeinformationen für Office 365 anzugeben.
Client-ID	Ihre Office 365-Client-ID.
Geheimer Client-Schlüssel	Ihr geheimer Office 365-Clientschlüssel.
Zeichen anzeigen	Anzeigen der Zeichen im Feld *Geheimer Client-Schlüssel* in dem Formular *Anmeldeinformationen hinzufügen*. Diese Option ist nur verfügbar, wenn Sie Anmeldeinformationen hinzufügen. Wenn Sie vorhandene Anmeldeinformationen bearbeiten, können die Zeichen im Feld *Geheimer Client-Schlüssel* nicht angezeigt werden.
Azure AD-Mandantentyp	Wählen Sie aus den verfügbaren Optionen Ihren Azure AD-Mandantentyp aus. Der Mandantentyp muss mit dem Typ übereinstimmen, der bei der Registrierung Ihrer Azure AD-Anwendung im Azure AD-Administratorportal ausgewählt wurde. • **Multitenant & Personal Microsoft Accounts - Default (Mandantenfähige und Persönliche Microsoft-Konten - Standard)**: Verwenden Sie diese Option, um Zugriff auf eine Vielzahl von Microsoft-Identitäten zu gewähren und die Mandantenfähigkeit zu aktivieren. Alle Benutzer mit einem Geschäfts-, Schul- oder persönlichen Microsoft-Konto können mit diesen Anmeldedaten auf Ihre Anwendung oder API zugreifen. Dies gilt für Schulen und Unternehmen, die Office 365 verwenden, sowie für persönliche Konten, die zur Anmeldung bei Diensten wie Xbox oder

Option	Beschreibung
	Skype verwendet werden. Dies ist die Standardeinstellung. • **Azure AD-Verzeichnis - Mehrinstanzenfähig**: Verwenden Sie diese Option, um Unternehmen oder Bildungseinrichtungen Zugriff zu gewähren und die Mehrmandantenfähigkeit zu aktivieren. Alle Benutzer mit einem Geschäfts- oder Schulkonto von Microsoft können Ihre Anwendung oder API verwenden. Dies gilt auch für Schulen und Unternehmen, die Office 365 verwenden. • **Nur persönliche Microsoft-Konten**: Verwenden Sie diese Option, um Zugriff auf persönliche Konten zu gewähren, die zur Anmeldung bei Diensten wie Xbox oder Skype verwendet werden. • **Organizational directory only (Single tenant) (Nur Organisationsverzeichnis (Einzelmandant))**: Verwenden Sie diese Option, um den Benutzern, die Ihrem Unternehmen zugeordnet sind, Zugriff zu gewähren.
Azure AD Endpoint URL (URL für Azure AD-Endpunkte)	Registrieren Sie Ihre Azure AD-Anwendung, und erwerben Sie Token für die nationale Cloud, die mit Ihrer Umgebung verbunden ist. Wählen Sie nach Bedarf eine der folgenden URLs aus: • **https://login.microsoftonline.com**: Wählen Sie diese Option aus, um Ihre Azure AD-Anwendung beim globalen Azure AD-Dienst zu registrieren. • **https://login.microsoftonline.us**: Wählen Sie diese Option, um Ihre Azure AD-Anwendung bei Azure AD für die US-Regierung zu registrieren. • **https://login.microsoftonline.de**: Wählen Sie diese Option, um Ihre Azure AD-Anwendung bei Azure AD Deutschland zu registrieren. • **https://login.chinacloudapi.cn**: Wählen Sie diese Option, um Ihre Azure AD-Anwendung bei Azure AD China zu registrieren, das von 21Vianet betrieben wird.
Genehmigungscode	Der Genehmigungscode für den Zugriff. Um diesen Code abzurufen, geben Sie Ihre *Client-ID* und Ihren *geheimen Client-Schlüssel* an und klicken dann auf **Neuen Code erstellen**.
Neuen Code erstellen	Ein Link zum Codegenerator. So erstellen Sie einen neuen Code: a. Klicken Sie auf **Neuen Code erstellen**.

Option	Beschreibung
	b. Wählen Sie im daraufhin angezeigten Dialogfeld *Anmeldeinformationen hinzufügen* Ihr Office 365-Konto aus. c. Melden Sie sich auf der Anmeldeseite mit Ihren Office 365-Anmeldeinformationen an. Wenn keine Office 365-Anmeldeseite angezeigt wird, sind die Anmeldeinformationen für Ihr Google-Konto bereits zwischengespeichert. Handelt es sich bei dem gespeicherten Konto nicht um das bevorzugte Konto, melden Sie sich ab und mit dem bevorzugten Konto wieder an. d. Klicken Sie auf **Akzeptieren**, um einen Code zu generieren, der dem Appliance Service Desk Zugriff auf Ihr Profil, Ihre E-Mail (einschließlich Lese- und Schreibzugriff) und den Offline-Zugriff auf heruntergeladene E-Mails gewährt. e. Die Anmeldeseite wird geschlossen, und das Dialogfeld *Anmeldeinformationen hinzufügen* wird aktualisiert und zeigt den neu generierten Code im Feld *Genehmigungscode* an.
Anmerkungen	Weitere Informationen, die Sie zu den Anmeldeinformationen angeben möchten.

4. Klicken Sie auf **Speichern**.

   Die Anmeldeinformationen stehen für die Auswahl in Komponenten zur Verfügung, in denen Anmeldeinformationen verwendet werden.

Anzeigen der Nutzung der Anmeldeinformationen

Sie können die Nutzung der Anmeldeinformationen auf der Seite *Verwaltung der Anmeldeinformationen* anzeigen.

- Zur Seite *Verwaltung der Anmeldeinformationen* sind Anmeldeinformationen hinzugefügt worden. Siehe Verwalten von Anmeldeinformationen.
- Sie verfügen über Administratorrechte in der **Administratorkonsole**.

1. Rufen Sie die Seite *Verwaltung der Anmeldeinformationen* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie auf der linken Navigationsleiste auf **Einstellungen** und anschließend auf **Anmeldeinformationen**.

   In der Spalte *In Gebrauch* werden die Komponenten angezeigt, die die Anmeldeinformationen verwenden.
2. Um die Liste zu sortieren, wählen Sie einen **Typ** aus der Dropdown-Liste *Anzeigen nach* oberhalb der Tabelle aus.

Erstellen von Berichten aus der Liste "Verwaltung der Anmeldeinformationen"

Wenn Verlaufsabonnements zur Aufbewahrung von Anmeldeinformationen konfiguriert werden, können Sie Berichte erstellen, die den Zeitpunkt der Erstellung, Bearbeitung und Löschung von Anmeldeinformationen enthalten.

- Zur Appliance hinzugefügte Anmeldeinformationen werden auf der Seite *Verwaltung der Anmeldeinformationen* angezeigt.
- Es sind Verlaufsabonnements zur Aufbewahrung von Anmeldeinformationen konfiguriert worden. Siehe Objektverlauf konfigurieren.

Bei der Erstellung von Berichten auf der Seite *Verwaltung der Anmeldeinformationen* können Sie Informationen über die Anmeldeinformationen wie Name, Typ, Erstellungsdatum und Nutzungsinformationen angeben. Authentifizierungsdetails wie das Kennwort oder der geheime Client-Schlüssel sind in den Berichten jedoch nicht enthalten.

HINWEIS: Wenn auf der Appliance die Organisationskomponente aktiviert ist, erstellen Sie Anmeldeinformationenberichte separat für jede Organisation.

1. Rufen Sie die Seite *Verwaltung der Anmeldeinformationen* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie auf der linken Navigationsleiste auf **Einstellungen** und anschließend auf **Anmeldeinformationen**.
2. Wählen Sie **Aktion auswählen** > **Bericht erstellen**.
3. Geben Sie auf der Seite *Berichtsdetail* einen Namen für den Bericht an.
4. Wählen Sie weitere Berichteinstellungen aus und klicken Sie dann auf **Speichern**. Siehe Berichte über Listenseiten erstellen.

   Der Bericht wird in der Liste **Berichte** angezeigt.
5. Wählen Sie in der Spalte *Bericht generieren* ein Format aus, um den Bericht zu generieren.

Exportieren von Anmeldeinformationen

Sie können die Liste der Anmeldeinformationen oder ausgewählte Anmeldeinformationen exportieren, die auf der Seite *Verwaltung der Anmeldeinformationen* angezeigt werden.

Zur Appliance hinzugefügte Anmeldeinformationen werden auf der Seite *Verwaltung der Anmeldeinformationen* angezeigt.

Sie können Informationen über die Anmeldeinformationen wie Name, Typ, Datum der letzten Änderung und Nutzungsinformationen exportieren. Authentifizierungsdetails wie das Kennwort oder der geheime Client-Schlüssel können nicht exportiert werden.

HINWEIS: Wenn auf der Appliance die Organisationskomponente aktiviert ist, exportieren Sie Anmeldeinformationen separat für jede Organisation.

1. Rufen Sie die Seite *Verwaltung der Anmeldeinformationen* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen*

aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.

b. Klicken Sie auf der linken Navigationsleiste auf **Einstellungen** und anschließend auf **Anmeldeinformationen**.

2. Wählen Sie **Aktion auswählen** > **Exportieren** aus und anschließend, ob alle Anmeldeinformationen oder nur die ausgewählten Anmeldeinformationen exportiert werden sollen. Wählen Sie dann das Format für die exportierten Informationen aus.
3. Öffnen oder speichern Sie die exportierte Datei.

Löschen von Anmeldeinformationen

Sie können Anmeldeinformationen löschen, wenn sie nicht in Komponenten wie Inventar, Verteilung oder Skripterstellung verwendet werden.

- Von allen Komponenten, die Anmeldeinformationen verwenden, sind die Anmeldeinformationen entfernt worden. Siehe Anzeigen der Nutzung der Anmeldeinformationen.
- Sie verfügen über Administratorrechte in der **Administratorkonsole**.

1. Rufen Sie die Seite *Verwaltung der Anmeldeinformationen* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie auf der linken Navigationsleiste auf **Einstellungen** und anschließend auf **Anmeldeinformationen**.
2. Aktivieren Sie das Kontrollkästchen neben den Anmeldeinformationen, die Sie löschen möchten.

   HINWEIS: Falls ausgewählte Anmeldeinformationen in Verwendung sind, wird eine Fehlermeldung angezeigt. Wenn ausgewählte Anmeldeinformationen in Verwendung sind, können keine Gruppen von Anmeldeinformationen gelöscht werden.
3. Wählen Sie **Aktion auswählen** > **Löschen** und klicken Sie dann zum Bestätigen auf **Ja**.

Konfigurieren von Assets

Sie können Assets und Asset-Typen nach Bedarf konfigurieren.

Informationen zur Komponente Asset Management

Die Asset Management-Komponente enthält Assets und Asset-Typen (Vorlagen). Sie ermöglicht die Verwaltung von Assets, die automatisch durch Inventarisierung oder manuell hinzugefügt wurden.

Zu den standardmäßigen Asset-Typen zählen folgende Elemente: Gerät, Kostenstelle, Abteilung, Lizenz, Standort, Software und Hersteller. Sie können bei Bedarf benutzerdefinierte Asset-Typen erstellen. Siehe Asset-Typen anpassen.

Die Asset Management-Komponente ermöglicht folgende Aktionen:

- **Verwalten von Elementen im Laufe ihres Lebenszyklus**. Verfolgen Sie Software und andere Elemente von der Beschaffung über die Bereitstellung und Nutzung bis zum Ende ihrer Lebensdauer. Dazu gehören

auch Peripheriegeräte wie Drucker, Netzwerkgeräte und Telefone. Siehe Nachzuverfolgende Assets festlegen.

- **Verwalten der Softwarelizenz-Compliance**. Sie können die von Ihnen erworbenen Softwarelizenzen sowie die Anzahl der auf den Geräten installierten Anwendungen verfolgen. Die Optionen für die Verwaltung der Lizenz-Compliance unterscheiden sich von den Elementen im Inventar des *Softwarekatalogs* und im Inventar der Seite *Software*. Siehe Einrichten der Lizenz-Compliance.
- **Verfolgen von Daten**. Sie haben die Möglichkeit, Bestellungen zu verfolgen, indem Sie die einzelnen Bestellungen als Asset eingeben und sie mit den erworbenen, erhaltenen und verteilten Artikeln verknüpfen. Siehe Hinzufügen von Lizenz-Assets für das Inventar der Seite "Software".
- **Verfolgen physischer Assets**. Die Komponente ermöglicht die Verfolgung physischer Assets wie beispielsweise Gerätehardware und Software sowie anderer physischer Assets wie Büromöbel. Sie haben die Möglichkeit, ihre Verwendung sowie den Status der Gewährleistung zu verfolgen. Siehe Verwalten physischer und logischer Assets.
- **Verfolgen logischer Assets**. Sie können logische Assets wie beispielsweise geografische Standorte, Kostenstellen, Abteilungen und Hersteller verfolgen. Logische Assets bilden normalerweise die Grundlage für Berichte. So können Sie Fragen beantworten wie "Wie viele Geräte befinden sich in dieser Abteilung?" oder "Wann laufen unsere Lizenzen des Softwareherstellers ab?". Siehe Verwalten physischer und logischer Assets.
- **Erstellen und Verfolgen von Beziehungen zwischen Assets**. Sie haben die Möglichkeit, Peer-to-Peer-Beziehungen und hierarchische Beziehungen zwischen Assets zu erstellen. Diese Beziehungen ermöglichen die Verfolgung von Assets nach Bestellung, Standort, Abteilung, Projekt oder anderen Kriterien. Siehe Beziehungen zwischen Asset-Feldern herstellen.

Das Asset Management-Dashboard verwenden

Das Asset Management-Dashboard bietet einen Überblick über verwaltete Assets für die ausgewählte Organisation (falls zutreffend) oder das Gerät.

Wenn auf der Appliance die Organisationskomponente aktiviert ist und Sie bei der Administratorkonsole angemeldet sind (`http://`**appliance_hostname**`/admin`), zeigt das Asset Management-Dashboard Informationen zur ausgewählten Organisation an. Wenn Sie an der Systemverwaltungskonsole angemeldet sind (`http://`**appliance_hostname**`/system`), zeigt das Asset Management-Dashboard Informationen zur Appliance an, einschließlich aller Organisationen.

TIPP: Die Appliance aktualisiert die Übersichtswidgets regelmäßig. Um die meisten Widgets zu aktualisieren, klicken Sie auf die Schaltfläche **Aktualisieren** in der oberen rechten Seite: . Um die meisten einzelne Widgets zu aktualisieren, zeigen Sie mit dem Mauszeiger auf das Widget und klicken Sie oberhalb des Widgets auf die Schaltfläche **Aktualisieren**. Einige Widgets erfordern möglicherweise zusätzliche Schritte.

Informationen zu den Asset Management-Widgets im Dashboard

Die Asset Management-Widgets im Dashboard bietet einen Überblick über verwaltete Assets für die ausgewählte Organisation oder Appliance.

In diesem Abschnitt werden die im *Asset Management Dashboard* verfügbaren Widgets beschrieben. Wenn die Organisationskomponente in Ihrer Appliance aktiviert ist, zeigen Widgets die Informationen für die ausgewählte Organisation auf Administratorebene und die Informationen für das Gerät auf Systemebene.

Dieses Dashboard bietet einen groben Überblick über Ihre Asset-Nutzung. Nutzen Sie es, um schnell den Status Ihrer Assets zu überprüfen und nach Indikatoren zu suchen, mit denen Sie Ihre Asset-Konfiguration verbessern können. Zum Beispiel, können Sie sich darauf konzentrieren, wie Ihre Softwarelizenzen verwendet werden, und ermitteln, für welche Softwaretitel die Lizenz erneuert werden muss.

Widget	Beschreibung
Assets nach Typ	Dieses Widget zeigt ein Ringdiagramm an, bei dem jeder Abschnitt des Diagramms den Prozentsatz Ihrer Assets nach Asset-Typ angibt, wie Gerät, Software, Standort, Lizenz und andere. Wenn Sie den Mauszeiger über die einzelnen Abschnitte des Diagramms bewegen, wird der Prozentsatz der Assets des ausgewählten Typs angezeigt.
Assets nach Status	Dieses Widget zeigt ein Ringdiagramm an, bei dem jeder Abschnitt des Diagramms den Prozentsatz Ihrer Assets nach Status angibt, wie z. B. aktiv, entsorgt, fehlt oder andere. Wenn Sie mit der Maus über die einzelnen Abschnitte des Diagramms fahren, wird der Prozentsatz an Assets mit dem ausgewählten Status angezeigt.
Kosten ($) von ungenutzten Lizenzen nach Produkt	Dieses Widget zeigt ein Balkendiagramm, wobei jeder Balken für die Kosten der jeweils ungenutzten Lizenzen für ein Produkt steht. Sie können diese Informationen verwenden, um ungenutzte Lizenzen neu zuzuweisen oder zu stornieren und zur Umleitung der Ressourcen an die Stellen, wo sie am meisten gebraucht werden.
Lizenz-Compliance	Wenn Sie Lizenz-Assets für Software erstellt haben, zeigt dieses Widget die Anzahl der vom Agenten verwalteten Geräte, auf denen eine bestimmte lizenzierte Software installiert ist, sowie die Anzahl verfügbarer Lizenzen an. Wenn für Ihre Appliance die Organisationskomponente aktiviert ist, zeigt das Widget Informationen für die jeweils ausgewählte Organisation an. Lizenz-Assets können für auf den Seiten *Software* oder *Softwarekatalog* aufgeführte Anwendungen erstellt werden. Der Lizenzmodus für Anwendungen muss *Lizenz für Einheit* oder *Unternehmen* lauten, damit Lizenzinformationen in diesem Widget angezeigt werden. Anwendungen mit anderen Lizenzmodi, wie z. B. *Shareware*, *Freeware* oder *Nicht angegeben*, werden in diesem Widget nicht angezeigt. Dieses Widget dient lediglich zu Informationszwecken. Bei der Appliance wird die Lizenz-Compliance nicht erzwungen. Sie verhindert beispielsweise nicht, dass Software auf vom Agenten verwalteten Geräten installiert wird, wenn eine Lizenz abgelaufen ist oder anderweitig gegen die Compliance-Vorgaben verstoßen wird. Diese Farben stehen für die folgenden Schwellenwerte: • **Rot**: Die Nutzung hat den kritischen Schwellenwert erreicht oder überschritten. • **Orange**: Die Nutzung hat den Warnungsschwellenwert erreicht oder

Widget	Beschreibung
	überschritten, liegt aber unter dem kritischen Schwellenwert. • **Grün**: Die Nutzung liegt unter dem Warnungsschwellenwert. Informationen zum Ändern der Schwellenwerte finden Sie unter Allgemeine Appliance-Einstellungen ohne aktivierte Organisationskomponente konfigurieren. Weitere Informationen zum Verwalten von Lizenz-Assets finden Sie unter Verwalten des Inventars.
Softwaretitel	Dieses Widget zeigt die im Softwarekatalog definierten Softwaretitel mit der höchsten Anzahl an Installationen auf verwalteten Geräten an. Wenn für Ihre Appliance die Organisationskomponente aktiviert ist, zeigt das Widget Informationen für die jeweils ausgewählte Organisation an.
Softwareherausgeber	Dieses Widget zeigt die im Softwarekatalog definierten Herausgeber mit der höchsten Anzahl an Softwaretiteln an, die auf verwalteten Geräten installiert sind. Wenn für Ihre Appliance die Organisationskomponente aktiviert ist, zeigt das Widget Informationen für die jeweils ausgewählte Organisation an.
Assets nach Standort	Dieses Widget zeigt ein Ringdiagramm an, in dem die Abschnitte des Diagramms den Prozentsatz der Assets nach Standort angeben. Wenn Sie mit der Maus über die einzelnen Abschnitte des Diagramms fahren, wird der Prozentsatz an Assets mit dem ausgewählten Standort angezeigt.
Installierte, aber in 60 Tagen nicht verwendete Software	Dieses Widget zeigt ein Balkendiagramm an, wobei jeder Balken einen Softwaretitel und die entsprechende Anzahl der Instanzen des jeweiligen Produkts darstellt, die in den letzten 60 Tagen nicht genutzt wurden. Sie können diese Informationen verwenden, um weiter zu untersuchen, ob diese Titel erforderlich sind, zum erneuten Zuweisen oder Deinstallieren nicht verwendeter Software und zur Umleitung der Ressourcen an die Stellen, wo sie am meisten gebraucht werden.
Wartung ablaufender Software-Lizenzen	Dieses Widget zeigt ein vertikales Balkendiagramm an, wobei jeder Balken für die Anzahl der Softwarelizenzen steht, die in einem bestimmten Zeitraum ablaufen werden.
Wartung abgelaufener Software-Lizenzen	Dieses Widget zeigt ein Ringdiagramm an, das das Verhältnis der abgelaufenen zu den aktuellen Lizenzen darstellt. Wenn Sie den Mauszeiger über die einzelnen Abschnitte des Diagramms bewegen, wird je nach Auswahl der Prozentsatz

Widget	Beschreibung
	der abgelaufenen oder aktuellen Softwarelizenzen angezeigt.
Ablaufende Verträge	Dieses Widget zeigt ein vertikales Balkendiagramm an, wobei jeder Balken für die Anzahl der Verträge steht, die in einem bestimmten Zeitraum ablaufen werden.
Abgelaufene Verträge	Dieses Widget zeigt ein Ringdiagramm an, das das Verhältnis der abgelaufenen zu den aktuellen Verträgen darstellt. Wenn Sie den Mauszeiger über die einzelnen Abschnitte des Diagramms bewegen, wird je nach Auswahl der Prozentsatz der abgelaufenen oder aktuellen Verträge angezeigt.
Softwarelizenz-Konfiguration	Wenn Sie Lizenz-Assets für Software einrichten und den Lizenztyp angeben, wie z. B. Standortlizenz, Abonnement oder Einheit, werden diese Informationen in diesem Widget angezeigt. Wenn für Ihre Appliance die Organisationskomponente aktiviert ist, zeigt das Widget Informationen für die jeweils ausgewählte Organisation an.

Das Asset Management-Dashboard anpassen

Sie können das Asset Management-Dashboard anpassen und Widgets nach Bedarf ein- oder ausblenden.

1. Rufen Sie das *Asset Management-Dashboard* auf.
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Asset Management** und anschließend auf **Dashboard**.
2. Fahren Sie mit dem Mauszeiger über das Widget und verwenden Sie anschließend die folgenden Schaltflächen:
   - : Die Informationen im Widget aktualisieren
   - : Die Informationen zum Widget anzeigen
   - : Das Widget ausblenden
   - : Die Größe des Widgets ändern
   - : Das Widget an eine andere Position auf der Seite ziehen.
3. Klicken Sie auf die Schaltfläche **Anpassen** in der oberen rechten Ecke der Seite, um die verfügbaren Widgets anzuzeigen.
4. Um ein Widget anzuzeigen, das derzeit ausgeblendet ist, klicken Sie auf **Installieren**.

Informationen zum Verwalten von Assets

Assets sind die Entitäten, die Informationen zu den Geräten, Softwarelizenzen und anderen Elementen enthalten, die Sie verwalten möchten. Assets basieren auf Asset-Typen. Dabei handelt es sich um Vorlagen für die Erstellung von Assets.

Unterschiede zwischen Asset- und Inventarinformationen

Asset- und Inventarinformationen werden auf unterschiedliche Weise erfasst und verwaltet.

In der folgenden Tabelle werden Asset- und Inventarinformationen verglichen:

Element	Asset-Komponente	Inventarkomponente
Anzeige von Informationen	Im Abschnitt *Assets*.	Im Abschnitt *Inventar*.
Typ der verwalteten Informationen	Asset-Informationen umfassen Details zu Geräten, Software, Lizenzen, physischen Assets, logischen Assets und die Beziehungen zwischen ihnen.	Inventarinformationen enthalten Details zu Geräten und den auf den verwalteten Geräten verwendeten Softwareanwendungen, Prozessen, Startprogrammen und Services. Der Softwarekatalog bietet zusätzliche Informationen zu Anwendungen, die als *Erkannt* oder *Nicht erkannt* kategorisiert sind.
Verwalten der Informationen	Asset-Informationen sind statisch und ändern sich nur, wenn Sie Daten importieren oder Daten manuell ändern. Geräte-Assets sind Ausnahmen dieser Regel, da Geräte-Assets immer dann aktualisiert werden, wenn verwaltete Geräte Inventar melden. Bei Lizenz-Assets wird die Anzahl der Installationen oder Arbeitsplätze jedoch aktualisiert, wenn verwaltete Geräte Daten an die Appliance melden. Der Asset-Verlauf wird in der Appliance gespeichert und in der **Administratorkonsole** angezeigt. Er bleibt beim Asset erhalten, bis das Asset gelöscht wird.	Inventarinformationen werden automatisch generiert und überschrieben, sobald verwaltete Geräte Daten an die Appliance melden.
Verfolgung von Lizenzen	Die Komponente "Asset Management" bietet Ihnen die Möglichkeit, die Softwarelizenz-Compliance sowie physische und logische Assets zu verwalten.	Auf der Seite *Software* umfassen Inventarinformationen die Anzahl der Software-Assets, jedoch nicht die Anzahl der Lizenzen. Auf der Seite *Softwarekatalog* werden Lizenzinformationen angezeigt, wenn Lizenz-Assets

Element	Asset-Komponente	Inventarkomponente
		mit den Anwendungen verknüpft sind.

Nachzuverfolgende Assets festlegen

Eine der ersten Aufgaben beim Einrichten des Asset Managements besteht im Festlegen der nachzuverfolgenden Assets.

Tabellen enthalten häufig Asset-Details wie beispielsweise Einkaufsdaten, Herstellerkontaktdaten, Produktschlüssel. Lizenzdetails und Geräteinformationen. Diese Details eignen sich gut für die Asset-Verfolgung.

Sie können Asset-Informationen in die Komponente Asset Management importieren, um Assets zu erstellen, die mit der Appliance verwaltet und nachverfolgt werden können. Darüber hinaus können Sie Beziehung zwischen den importierten Assets einrichten, um die Informationen nützlicher zu gestalten. Sie können beispielsweise Lizenz- und Hersteller-Assets erstellen, diese Geräten zuordnen und schnell einer Lizenz oder einem Hersteller zugehörige Geräte ermitteln. Informationen zum Importieren von Asset-Informationen finden Sie unter Importieren von Lizenzdaten in CSV-Dateien.

Assets anzeigen und nach Asset-Informationen suchen

Sie können nach Bedarf Assets anzeigen und nach Asset-Informationen suchen.

1. Rufen Sie die Liste *Assets* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Asset Management** und anschließend auf **Assets**.
2. So durchsuchen Sie alle Assettypen mit der erweiterten Suche:
   a. Wählen Sie aus der Dropdown-Liste *Anzeigen nach* die Option **Alle Elemente** aus.
   b. Klicken Sie oberhalb der Liste auf der rechten Seite auf die Registerkarte **Erweiterte Suche**, um den Bereich *Erweiterte Suche* anzuzeigen.
   c. Geben Sie die Suchkriterien ein.

   Wenn Sie beispielsweise nach allen Assets des Herstellers **Smith** suchen möchten, geben Sie die folgenden Kriterien an:

   ```
   Hersteller | hat | Smith
   ```

   d. Klicken Sie auf **Suchen**.

      Assets eines beliebigen Typs (einschließlich Gerät, Lizenz, Software oder Hersteller), die die Kriterien erfüllen, werden angezeigt.
3. So suchen Sie mit der einfachen Suche über alle Assettypen hinweg nach einem Asset, geben Sie im Feld **Suchliste** den vollständigen oder Teile des Inhalts des Felds im Asset an, nach dem gesucht werden soll. Wenn Sie einen Asset suchen, dessen Barcode zz enthält, geben Sie das im Feld ein und drücken Sie Eingabe.

   Assets, die die Kriterien erfüllen, werden angezeigt.
4. So suchen Sie nach einem bestimmten Asset-Typ:
   a. Wählen Sie aus der Dropdown-Liste *Anzeigen nach* die Option **Asset-Typ** > **Asset-Typ** aus.
   b. Klicken Sie oberhalb der Liste auf der rechten Seite auf die Registerkarte **Erweiterte Suche**, um den Bereich *Erweiterte Suche* anzuzeigen.
   c. Geben Sie die Suchkriterien ein.

Wenn Sie beispielsweise nach Lizenz-Assets suchen möchten, die innerhalb der nächsten beiden Monate ablaufen werden, wählen Sie aus der Dropdown-Liste *Anzeigen nach* den Lizenz-Asset-Typ aus und geben dann die folgenden Kriterien an:

```
Ablaufdatum | befindet sich innerhalb der nächsten | 2 Monate
```

d. Klicken Sie auf **Suchen**.

Angezeigt werden Lizenz-Assets, deren Ablaufdatum innerhalb der nächsten beiden Monate liegt.

5. Wenn Sie eine benutzerdefinierte Ansicht erstellen möchten, in der die angegebenen Suchkriterien verwendet werden, klicken Sie über der Liste auf der rechten Seite auf die Registerkarte **Benutzerdefinierte Ansicht** und speichern dann die Ansicht.

   Die benutzerdefinierte Ansicht erscheint in der Dropdown-Liste *Anzeigen nach*. Benutzerdefinierte Ansichten sind benutzerspezifisch. Benutzer können auf ihre eigenen benutzerdefinierten Ansichten zugreifen, aber nicht auf von anderen Benutzern erstellte Ansichten.

Barcodes zu Assets hinzufügen

Sie können nach Bedarf Assets anzeigen und nach Asset-Informationen suchen.

Geben Sie für den Asset-Typ, für den Sie Barcodes angeben möchten, einen oder mehrere Barcode-Tags an. Weitere Informationen hierzu finden Sie unter Asset-Typen hinzufügen oder anpassen.

1. Rufen Sie die Seite *Asset-Detail* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Asset Management** und anschließend auf **Assets**.
   c. Klicken Sie auf den Namen eines Assets.
2. Klicken Sie unter *Barcodes* auf + und geben Sie die folgenden Informationen an:

Option	Beschreibung
Barcodedaten	Die Barcode-Nummer. Barcode-Nummern sind immer eindeutig, sie können nicht von mehreren Assets gemeinsam genutzt werden. Es ist jedoch für ein aktives Asset möglich, einen Barcode mit einem archivierten Asset gemeinsam zu nutzen.
Barcodename	Der mit diesem Asset-Typ verknüpfte Barcode-Tag. Es kann jeweils nur einen Barcode gleichen Typs pro Asset geben.
Barcodeformat	Das Barcodeformat. Beispielsweise UPC-A, Code 11 oder UPC-E.

   Sie können beliebig viele Barcodes nach Bedarf hinzufügen.

3. Optional. Wenn Sie zusätzliche Informationen über jeden Barcode-Tag anzeigen möchten, wie erstes oder letztes Scan-Datum, klicken Sie im Bereich *Barcodes* auf **Alle Spalten anzeigen**. Wenn Sie zur vorigen Ansicht mit weniger Spalten pro Barcode zurückkehren möchten, klicken Sie auf **Weniger Spalten anzeigen**.
4. Klicken Sie auf **Speichern**.

Gerätebesitzer ändern

Sie können Bestand und Gerätebesitzer nach Bedarf ändern.

Dieses Thema beschreibt den Prozess für den Wechsel des Gerätebesitzes mithilfe der Asset-Liste. Sie können auch Gerätebesitzer mithilfe der Seite *Asset Detail* oder *Gerätedetail* ändern.

1. Rufen Sie die Liste *Assets* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Asset Management** und anschließend auf **Assets**.
2. Wählen Sie aus der Dropdown-Liste *Anzeigen nach* die Option **Asset-Typ > Gerät** aus.
3. Wählen Sie In der Liste *Assets* eines oder mehrere Geräte aus, die Sie einem bestimmten Besitzer zuweisen möchten.
4. Wählen Sie **Aktion auswählen** > **Zuweisen zu**.
5. Klicken Sie im angezeigten Dialogfeld *Zuweisen zu* auf *Nicht zugewiesen* und wählen Sie ein Benutzerkonto, das Sie als Besitzer des ausgewählten Bestands zuweisen möchten.

   Die angezeigten Liste zeigt den vollständigen Namen, Kontoname und die E-Mail-Adresse für jeden Benutzer an.
6. Klicken Sie auf **Speichern**.

   Das Dialogfeld *Zuweisen zu* wird geschlossen und die Liste *Assets* wird aktualisiert und zeigt den Name des Bestandsbesitzers in der Spalte *Name des Bevollmächtigten* an.
7. Fügen Sie der Liste *Assets* weitere besitzerbezogene Spalten hinzu.
   a. Klicken Sie in der Liste *Assets* auf ⚙.
   b. Wählen Sie je nach Bedarf eine der folgenden Optionen, um diese Spalten in der Liste *Assets* anzuzeigen: **Bevollmächtigter Anmeldung**, **Bevollmächtigter E-Mail**, **Bevollmächtigter Domäne**, **Bevollmächtigter Budget-Code**, **Bevollmächtigter Standort**, **Bevollmächtigter Rolle** oder **Gebietsschema des Bevollmächtigten**.

      Die gewählten Spalten werden in der Liste *Assets* angezeigt.
8. Wenn Sie geändert den Besitzer eines Geräts geändert haben, können Sie diese Änderung in der Liste *Geräte* beobachten.
   a. Klicken Sie in der linken Navigationsleiste auf **Inventar** und anschließend auf **Geräte**.
   b. Sie sehen in der Liste *Geräte* die Spalte der Zeile *Bevollmächtigter Name*, die das Gerät enthält, dessen Eigentümer Sie geändert haben.

      Die Spalte *Bevollmächtigter Name* zeigt den Namen des Gerätebesitzers an

TIPP: Alternativ können Sie Asset- oder Gerätebesitzer auf der Seite *Asset Detail* oder *Gerätedetail* ändern.

Asset-Lebenszyklus-Einstellungen anzeigen und konfigurieren

Mit Ausnahme der Standorte kann jeder Asset-Typ einen Status haben, der dessen Einsatzbereich oder Verwendungszweck angibt, z. B. aktiv, entsorgt, abgelaufen oder andere.

Zum Konfigurieren von entsprechenden Asset-Lebenszyklus-Einstellungen muss Ihre Benutzerrolle die Schreibberechtigung *Asset-Lebenszyklus* aufweisen. Zum Anzeigen der Asset-Lebenszyklus-Einstellungen ist

eine Leseberechtigung ausreichend. Weitere Informationen zu Benutzerrollen finden Sie unter Verwalten von Organisationsrollen und Benutzerrollen.

Verwenden Sie die Seite *Asset-Lebenszyklus-Einstellungen*, um die Liste der bestehenden Asset-Status-Einträge anzuzeigen und um bei Bedarf neue hinzufügen zu können.

1. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
2. Führen Sie einen der folgenden Schritte aus:
   - **Klicken Sie in der linken Navigationsleiste auf Asset Management und anschließend auf Assets.**
   - **Klicken Sie in der linken Navigationsleiste auf Asset Management und anschließend auf Verträge.**
   - **Klicken Sie in der linken Navigationsleiste auf Asset Management und anschließend auf Lizenzen.**
3. Klicken Sie auf der Listenseite, die angezeigt wird, auf **Aktion wählen** > **Lebenszyklus-Einstellungen konfigurieren**.

   TIPP: Sie können schnell einen Asset-Status ändern, indem Sie das Asset auf der Listenseite auswählen, auf **Aktion wählen** > **Asset-Status ändern** klicken und den entsprechenden Status im Dialogfeld *Asset-Status ändern* wählen. Für die Verwendung dieses Befehls benötigen Sie je nach Bedarf eine Schreibberechtigung für *Assets*, *Verträge* oder *Lizenzen*. Weitere Informationen zu Benutzerrollen finden Sie unter Verwalten von Organisationsrollen und Benutzerrollen.

   Die Seite *Asset-Lebenszyklus-Einstellungen* wird angezeigt.
4. Auf der Seite *Asset-Lebenszyklus-Einstellungen* können Sie unter *Asset-Status* die Liste der Standard-Asset-Statusangaben anzeigen.

   Die folgenden Standard-Asset-Statusangaben sind verfügbar:
   - **Aktiv**: Alle Assets, die bereitgestellt, aktiv oder in Gebrauch sind.
   - **Entsorgt**: Ein Asset, das nicht mehr verfügbar ist.
   - **Abgelaufen** Ein Software-Lizenz oder ein Vertrags-Asset, das abgelaufen ist.
   - **Auf Lager**: Ein vor kurzem empfangenes Asset.
   - **Fehlt** Alle Assets, die nicht gefunden werden können.
   - **Reparieren** Ein Asset, das repariert wird.
   - **Reserviert** Ein Asset, das für eine bestimmte Person oder einen Zweck reserviert ist.
   - **außer Kraft gesetzt**: Alle Assets, die das Ende ihrer Lebensdauer erreicht haben oder nicht mehr in Gebrauch sind.
   - **Gestohlen**: Ein Asset, das als gestohlen gemeldet wurde.
5. Hinzufügen, Löschen oder Bearbeiten eines benutzerdefinierten Asset-Status.

TIPP: Standard-Asset-Statusangaben können nicht geändert oder gelöscht werden.

- Klicken Sie zum Hinzufügen eines neuen Asset-Status auf +, geben Sie den *Namen* und eine *Beschreibung* für den Asset-Status ein und klicken Sie auf **Hinzufügen**.
- Um einen benutzerdefinierten Asset-Status zu löschen, klicken Sie in der Zeile, die die Asset-Status enthält, auf 🗑.
- Um einen benutzerdefinierten Asset-Status zu bearbeiten, klicken Sie in der Zeile, die die Asset-Status enthält, auf ✎ und bearbeiten Sie den *Namen* und/oder die *Beschreibung* des Asset-Status nach Bedarf.

6. Wenn Sie Änderungen an den *Asset-Lebenszyklus-Einstellungen* vorgenommen haben, klicken Sie auf **Speichern**. Andernfalls klicken Sie auf **Abbrechen**, um zur vorherigen Seite zurückzukehren.

Hinzufügen und Anpassen von Asset-Typen und Verwalten von Asset-Informationen

Sie können bei Bedarf Asset-Typen hinzufügen und anpassen. Außerdem können Sie Echtzeitinformationen zu Assets erhalten, indem Sie Ihr Netzwerk in festgelegten regelmäßigen Intervallen scannen.

Darüber hinaus können Sie Untertypen zu Ihren Asset-Typen hinzufügen. Asset-Untertypen ermöglichen es Ihnen, Asset-Eigenschaften, wie z. B. Toner- oder Tintenfüllstände von Druckern, zu verfolgen.

Informationen zu Asset-Typen

Asset-Typen sind Vorlagen für die Erstellung von Assets. Asset-Typen enthalten die Felder und weiteren Informationen, die Assets definieren.

Zu den standardmäßigen Asset-Typen zählen folgende Elemente: Gerät, Kostenstelle, Abteilung, Lizenz, Vertrag, Standort, Kauf, Software und Hersteller und bei Bedarf können Sie benutzerdefinierte Asset-Typen hinzufügen.

Zusätzlich können Sie Asset-Untertypen und benutzerdefinierte Felder für alle Asset-Typen hinzufügen. Dies ist besonders nützlich für die Erfassung zusätzlicher Informationen zu Geräten, bei denen es sich nicht um Computer handelt, z. B. Drucker. Siehe Informationen zu Asset-Untertypen, benutzerdefinierten Feldern und Gerätedetail-Voreinstellungen.

Asset-Typen anpassen

Sie können Felder in Asset-Typen nach Bedarf umbenennen, erstellen und löschen. Anpassungen von Asset-Typen bleiben bei Appliance-Aktualisierungen erhalten.

Informationen zum Umbenennen von Feldern und Ändern von Feldtypen in Asset-Typen

Wenn Sie ein Feld in einem Asset-Typ umbenennen, wird das Feld in allen Assets umbenannt, die auf diesem Asset-Typ basieren. Werte für das umbenannte Feld werden beibehalten.

Wenn Sie jedoch den **Typ** in einen Typ ändern, der die bereits in ein Feld eingegebenen Daten nicht unterstützt, gehen die Daten verloren. Sie haben beispielsweise ein Feld mit dem Namen *Modellnummer* und dem *Typ Text*, das den Wert A123 enthält. Wenn Sie den *Typ* von *Text* in *Nummer* ändern, kann das System A123 nicht in eine gültige Zahl umwandeln. Der Wert für das Feld *Modellnummer* wird auf 0 festgelegt.

Informationen zum Hinzufügen und Löschen von Asset-Feldern

Wenn Sie ein Feld zu einem Asset-Typ hinzufügen, steht das Feld allen Assets dieses Typs zur Verfügung. Löschen Sie ein benutzerdefiniertes Asset-Feld, werden dieses Feld und alle in das Feld eingegebenen Werte aus allen Assets dieses Typs entfernt.

Wenn Sie beispielsweise ein benutzerdefiniertes Feld mit dem Namen *BIOS-Seriennummer* im Asset-Typ "Gerät" erstellt haben, steht dieses Feld für alle Assets des Typs "Gerät" zur Verfügung. Wenn Sie jedoch das benutzerdefinierte Asset *BIOS-Seriennummer* löschen, werden dieses Feld und alle in das Feld eingegebenen Werte aus allen Assets des Typs "Gerät" entfernt.

Wenn Sie ein Asset-Feld löschen, wird die Asset-Zuordnung von allen Assets entfernt, die auf das gelöschte Feld verweisen.

Asset-Typen hinzufügen oder anpassen

Sie können so viele benutzerdefinierte Asset-Typen erstellen, wie Sie benötigen. Außerdem können Sie in jedem Asset-Typ benutzerdefinierte Felder erstellen. Wenn Sie ein benutzerdefiniertes Feld in einem Asset-Typ erstellen, steht dieses Feld allen Assets zur Verfügung, die auf diesem Asset-Typ basieren.

Wenn auf der Appliance die Organisationskomponente aktiviert wurde, können Sie für jede Organisation separat Asset-Typen hinzufügen und anpassen.

1. Rufen Sie die Seite *Details zum Asset-Typ* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Asset Management** und anschließend auf **Asset-Typen**.
   c. Die Seite *Details zum Asset-Typ* zeigen Sie an, wie folgt:
   - Klicken Sie auf den Namen eines Asset-Typs.
   - Wählen Sie **Aktion auswählen** > **Neu**.
2. Fügen Sie im Feld *Name* den Namen hinzu oder ändern Sie ihn bei Bedarf.

   TIPP: Für die Asset-Typen „Gerät“ und „Lizenz“ stehen weitere Optionen zur Verfügung. Siehe Informationen zum Anpassen des Asset-Typs "Gerät" und Anpassen des Lizenz-Asset-Typs.
3. **Alle Asset-Typen, mit Ausnahme von Standorten**. Geben Sie im Feld *Standard-Asset-Status* einen Standard-Asset-Status oder einen benutzerdefinierten ein (falls vorhanden).

Eine Standardinstallation der Appliance umfasst die folgenden Asset-Status:

- **Aktiv**: Alle Assets, die bereitgestellt, aktiv oder in Gebrauch sind.
- **Entsorgt**: Ein Asset, das nicht mehr verfügbar ist.
- **Abgelaufen** Ein Software-Lizenz oder ein Vertrags-Asset, das abgelaufen ist.
- **Auf Lager**: Ein vor kurzem empfangenes Asset.
- **Fehlt** Alle Assets, die nicht gefunden werden können.
- **Reparieren** Ein Asset, das repariert wird.
- **Reserviert** Ein Asset, das für eine bestimmte Person oder einen Zweck reserviert ist.
- **außer Kraft gesetzt**: Alle Assets, die das Ende ihrer Lebensdauer erreicht haben oder nicht mehr in Gebrauch sind.
- **Gestohlen**: Ein Asset, das als gestohlen gemeldet wurde.

4. Wenn Sie Benutzern ohne Administratorrolle erlauben möchten, Assets dieses Typs zu löschen, wählen Sie **Benutzern ohne Administratorberechtigungen das Löschen von Assets erlauben** aus. Diese Option ist standardmäßig deaktiviert. Diese Option kann nur von Administratoren konfiguriert werden. Für andere Benutzertypen wird dieses Feld auf der Seite angezeigt, ist jedoch deaktiviert.

   Weitere Informationen über Benutzerrollen finden Sie unter Benutzerrollen hinzufügen oder bearbeiten.

5. Wenn Assets dieses Typs den Asset-Speicherort in den Asset-Details anzeigen sollen, wählen Sie **Speicherorteinstellungen anzeigen** aus. Diese Option ist standardmäßig deaktiviert.
6. **Nur Gerät-Assets**. Geben Sie im Feld *Standard-Archiv-Asset-Status* den Asset-Status ein, den Sie automatisch einem Gerät zuweisen wollen, wenn es archiviert wird.
7. Wenn Sie möchten, dass die Instanzen dieses Asset-Typs Barcodes verwenden, legen Sie im Bereich *Barcode-Tags* eine oder mehrere Tags fest.

   Assets dieses Typs den Sie erstellen, haben Barcode-Tags für die Konfiguration. Geben Sie beispielsweise einen Unternehmens-Tag und einen Dell Asset-Tag an, sind Barcodes mit diesen beiden Tags zur Auswahl auf der Seite *Asset-Details* verfügbar, wenn Sie einen Asset dieses Asset-Typs erstellen oder bearbeiten.

   Um einen Barcode hinzufügen, klicken Sie auf +, geben Sie den Barcode ein und klicken auf **Speichern**.

8. Im Bereich *Asset-Felder* klicken Sie auf +.

   Eine neue Zeile wird angezeigt.
9. Geben Sie die folgenden Informationen an:

Element	Beschreibung
Name	Der Name des benutzerdefinierten Asset-Felds, z. B. „Asset-Code“, „Kaufdatum“ oder „Adresszeile 1“. Dieser Name wird auf dem Formular angezeigt, mit dem Assets des ausgewählten Asset-Typs erstellt werden.
Verfügbare Werte	Die Werte, die in Feldern mit Wertelisten angezeigt werden. Dieses Feld ist aktiviert, wenn Sie aus der Dropdown-Liste *Typ* die Option **Einfachauswahl** oder **Mehrfachauswahl** auswählen. Wenn Sie **Einfachauswahl** oder **Mehrfachauswahl** auswählen, müssen Sie mindestens einen Wert in dieses Feld eingeben. Wenn Sie mehrere Werte verwenden möchten, trennen Sie die einzelnen Werte mit einem Komma.

Element	Beschreibung
Standardwerte	Der Wert, der standardmäßig im Feld angezeigt wird. Wenn Sie aus der Dropdown-Liste *Typ* die Option **Einfachauswahl** oder **Mehrfachauswahl** auswählen, müssen Sie einen der im Feld *Verfügbare Werte* angegebenen Werte eingeben.
Erforderlich	Gibt an, ob das Feld obligatorisch oder optional ist. Wenn dieses Kontrollkästchen aktiviert ist, müssen Benutzer beim Erstellen von Assets des ausgewählten Typs einen Wert in das Feld eingeben.
Typ	Der Typ des Felds. Es gibt folgende Feldtypen: • **Anhang**: Damit können Benutzer Anhänge zum Asset hinzufügen. • **Währung**: Wird für monetäre Werte verwendet. • **Softwarekatalog**: Damit können Benutzer das Asset mit einer Anwendung im Softwarekatalog verknüpfen. • **Datum**: Wird für Kalenderinformationen verwendet. • **Label**: Damit können Benutzer dem Asset ein Label zuweisen. • **Link**: Wird für Internetlinks verwendet. Links müssen gültige URLs sein, beispielsweise **http://software.quest.com**. • **Mehrfachauswahl**: Zeigt eine Liste an, aus der mehrere Werte ausgewählt werden können. Die maximale Länge für jeden Wert beträgt 255 Zeichen. • **Hinweise**: Wird für zusätzliche Informationen verwendet. • **Nummer**: Wird für numerische Werte verwendet, die als ganze Zahlen ausgedrückt werden. • **Übergeordnet**: Damit können Sie mit dem Asset auf denselben Asset-Typ innerhalb einer Beziehung über-/untergeordneter Elemente verweisen. Sie könnten beispielsweise für Standorttypen eine Verbindung zu einem übergeordneten Element zulassen, sodass New York auf den Standort Nordamerika verweisen kann. Diese Angabe kann im Berichtssystem dazu verwendet werden, alle Assets in Nordamerika anzuzeigen. • **Einfachauswahl**: Zeigt eine Werteliste an, aus der nur ein einzelner Wert ausgewählt

Element	Beschreibung
	werden kann. Die maximale Länge für jeden Wert beträgt 255 Zeichen. • **Text**: Wird für zusätzlichen Text verwendet. Die maximale Länge beträgt 255 Zeichen. • **Zeitstempel**: Damit werden Tag und Uhrzeit zum Datensatz hinzugefügt. • **Benutzer**: Damit werden Benutzerdatensätze mit einem Asset verknüpft. • **Assets Asset-Typ**: Damit werden Beziehungen zwischen Asset-Typen angegeben.
Mehrfachauswahl	Gibt an, ob das Asset-Feld auf andere Assets verweist. Ein Kontrollkästchen ist aktiviert, wenn Sie aus der Dropdown-Liste *Typ* die Option **Assets Asset-Typ** auswählen. Aktivieren Sie dieses Kontrollkästchen, damit dieses benutzerdefinierte Feld auf mehrere Datensätze verweisen kann. Beispiel: Sie möchten, dass ein Feld auf mehrere Geräte verweist, die für eine bestimmte Lizenz genehmigt wurden. In diesem Fall aktivieren Sie das Kontrollkästchen. Für ein Feld mit einer einzelnen Zuordnung, beispielsweise einen Drucker, der nur von einer Abteilung verwendet wird, deaktivieren Sie das Kontrollkästchen. **HINWEIS:** Wenn Sie ein Asset erstellen, werden die verfügbaren Assets des angegebenen Asset-Typs in dieses Feld geladen. Sind keine Assets des angegebenen Typs vorhanden, ist das Feld leer.
Abschnitt	**Nur Lizenz-Assets**. Die Registerkarte, auf der dieses Feld auf der Seite *Lizenzdetails* wird: *Allgemein*, *Kauf*, *Wartung*, *Zugehörig*, *Benutzerdefiniert* oder *Hinweise*. Weitere Informationen zu den Registerkarten auf der Seite *Lizenzdetails* finden Sie unter Lizenzen hinzufügen oder bearbeiten.
Geräteabschnitt	**Nur Gerät-Assets**. Die Stelle auf der Seite *Gerätedetail*, wo das Feld angezeigt wird. Wenn Sie z. B. einen Asset-Untertyp „Drucker“ mit einem Feld *Toner-Füllstand* erstellen, könnten Sie *Hardware* auswählen, weil dieses Feld mit Drucker-Hardware in Beziehung steht. Sie können jedoch in der Dropdown-Liste einen beliebigen Abschnitt für ein beliebiges Feld auswählen.

10. Klicken Sie am Ende der Zeile auf **Speichern** und anschließend unten auf der Seite auf **Speichern**.

Optional: Asset-Untertypen für Asset-Typen hinzufügen. Siehe Asset-Untertypen hinzufügen und Voreinstellungen für die Seite "Gerätedetail" auswählen.

Informationen zum Anpassen des Asset-Typs "Gerät"

Fast alle Geräte-Asset-Daten, ganz gleich ob sie in den Abschnitten *Assets* oder *Inventar* angezeigt werden, stammen aus dem Abschnitt *Assets*.

Die einzigen Geräteinventar- oder Asset-Informationen, die aus dem Bereich *Inventar* stammen, sind die Daten für *Zugeordnetes Inventarfeld* und *Entsprechendes Asset-Feld*. Die Werte für diese Felder werden bei jeder Inventarisierung der Geräte erfasst. Während der Inventarisierung ermittelt die Appliance, ob Geräte bereits über zugeordnete Assets verfügen. Wenn kein Asset gefunden wird, erstellt die Appliance eines.

Der standardmäßige Datentyp für *Zugeordnetes Inventarfeld* ist **Systemname** und für *Entsprechendes Asset-Feld* lautet er **Name**. Wenn Sie jedoch ein erneutes Imaging Ihrer Systeme durchführen, gehen die Informationen unter dem alten Systemnamen in der Komponente Asset Management verloren. Um dies zu vermeiden, ziehen Sie für die Nachverfolgung die Verwendung von BIOS-Seriennummern, IP-Adressen, Mac Adressen oder etwas Ähnlichem in Betracht.

Sie können die Geräte-Asset-Daten jederzeit importieren oder manuell im Abschnitt *Assets* ändern.

> **VORSICHT: Wenn Sie den Standard-Asset-Typ ändern, geht der Verlauf des Assets bis zum Zeitpunkt dieser Änderung verloren, da die Appliance automatisch neue Assets mit der neuen Information erstellt. Daher sollten Sie so früh wie möglich während der Einrichtung entscheiden, ob Sie die Standardwerte ändern möchten.**

Beispiel: Benutzerdefinierte Felder zum Asset-Typ "Gerät" hinzufügen

In diesem Beispiel sehen Sie, wie Sie dem Asset-Typ "Gerät" Felder hinzufügen und sie unter *Zugeordnetes Inventarfeld* und *Entsprechendes Asset-Feld* auswählen.

1. Rufen Sie die Seite *Details zum Asset-Typ* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Asset Management** und anschließend auf **Asset-Typen**.
   c. Klicken Sie auf den Asset-Typ **Gerät**.
2. Klicken Sie rechts auf der Seite auf die Schaltfläche **Hinzufügen**: +.

   Eine neue Zeile wird angezeigt.
3. Geben Sie die folgenden Informationen an:
   a. Geben Sie im Feld *Name* den Wert BIOS-Seriennummer ein.
   b. Wählen Sie aus der Dropdown-Liste *Typ* den Typ **Text** aus.
4. Klicken Sie am Ende der Zeile auf **Speichern**, und fügen Sie eine Zeile hinzu:
   a. Klicken Sie auf die Schaltfläche **Hinzufügen**: +.

      Eine neue Zeile wird angezeigt.
   b. Geben Sie die folgenden Informationen für die neue Zeile an:

   Geben Sie im Feld *Name* den Wert Seriennummer ein.

   Wählen Sie aus der Dropdown-Liste *Typ* den Typ **Text** aus. Verwenden Sie den *Typ* **Nummer** nur für Felder, mit denen Sie Berechnungen durchführen. Bei Verwendung des *Typs* **Nummer** werden möglicherweise die führenden Nullen von Seriennummern entfernt.
5. Klicken Sie am Ende der Zeile auf **Speichern**, und fügen Sie eine Zeile hinzu:
   a. Klicken Sie auf die Schaltfläche **Hinzufügen**: +.

Eine neue Zeile wird angezeigt.

b. Geben Sie die folgenden Informationen für die neue Zeile an:

Geben Sie im Feld *Name* den Wert Kaufdatum ein.

Wählen Sie aus der Dropdown-Liste *Typ* den Typ **Text** aus.

6. Klicken Sie am Ende der Zeile auf **Speichern**, und fügen Sie eine Zeile hinzu:

   a. Klicken Sie auf die Schaltfläche **Hinzufügen**: +.

   Eine neue Zeile wird angezeigt.

   b. Geben Sie die folgenden Informationen für die neue Zeile an:

   Geben Sie im Feld *Name* den Wert Standort ein.

   Wählen Sie aus der Dropdown-Liste *Typ* die Option **Asset-Standort** aus.

7. Klicken Sie am Ende der Zeile auf **Speichern**.
8. Ändern Sie den Wert in der Dropdown-Liste *Zugeordnetes Inventarfeld* in **BIOS-Seriennummer**.
9. Wählen Sie unter *Entsprechendes Asset-Feld* den Eintrag **Seriennummer** aus.
10. Klicken Sie unten auf der Seite auf **Speichern**.

Beziehungen zwischen Asset-Feldern herstellen

Sie können Asset-Typen bearbeiten, um Beziehungen zwischen Assets herzustellen und sie gemeinsam zu verfolgen.

Folgende Beziehungen sind möglich:

- Peer-to-Peer, zum Beispiel Drucker und Geräte
- Hierarchische Struktur, zum Beispiel Kostenstelle und zugehörige Geräte

Beispiel: Felder zum Asset-Typ "Standort" hinzufügen Zeigt, wie Sie eine hierarchische Beziehung zwischen Standorten herstellen, indem Sie dem Standort-Asset-Typ ein Feld hinzufügen.

Beispiel: Felder zum Asset-Typ "Standort" hinzufügen

Sie können nach Bedarf Felder zum Asset-Typ "Standort" hinzufügen.

1. Rufen Sie die Seite *Details zum Asset-Typ* auf:

   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.

   b. Klicken Sie in der linken Navigationsleiste auf **Asset Management** und anschließend auf **Asset-Typen**.

   c. Klicken Sie auf den Asset-Typ **Standort**.

2. Klicken Sie rechts auf der Seite auf die Schaltfläche **Hinzufügen**: +.

   Eine neue Zeile wird angezeigt.

3. Geben Sie im Feld *Name* den Wert Übergeordneter Standort ein.
4. Wählen Sie aus der Dropdown-Liste *Typ* den Typ **Übergeordnet** aus.
5. Klicken Sie am Ende der Zeile auf **Speichern** und anschließend unten auf der Seite auf **Speichern**.

Wenn Sie ein Standort-Asset öffnen, wird das Feld für die *Beziehung mit dem übergeordneten Element* auf der Seite *Asset-Detail* angezeigt.

Beziehungen mit dem übergeordneten Element zu Standort-Assets hinzufügen

Hierarchische Beziehungen können bei der Verwaltung von Assets, z. B. Standort-Assets, nützlich sein.

Fügen Sie wie unter Beispiel: Felder zum Asset-Typ "Standort" hinzufügen beschrieben benutzerdefinierte Felder für *Übergeordneter Standort* hinzu.

Wenn Sie Beziehungen mit einem übergeordneten Element hinzufügen, beginnen Sie mit der höchsten Ebene der Beziehung.

1. Rufen Sie die Liste *Assets* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Asset Management** und anschließend auf **Assets**.
2. **Optional**: Wählen Sie aus der Dropdown-Liste *Anzeigen nach*, die über der Tabelle auf der rechten Seite angezeigt wird, die Option **Asset-Typ** > **Standort** aus.

   Die Anzeige ist auf die Standort-Assets beschränkt.
3. Falls auf der höchsten Ebene (übergeordnete Ebene) kein Standort-Asset vorhanden ist, erstellen Sie es wie folgt:
   a. Wählen Sie **Aktion auswählen** > **Neu** > **Standort**, um die Seite mit den *Standort-Asset-Details* anzuzeigen.
   b. Geben Sie einen Namen für das neue Feld ein. Beispiel: Abteilung West.
   c. Behalten Sie für *Übergeordneter Standort* die Option **Nicht zugewiesen** bei und klicken Sie dann auf **Speichern**, um die Seite *Assets* anzuzeigen.

   HINWEIS: Das Feld *Übergeordneter Standort* ist ein vom Benutzer erstelltes und definiertes Feld.
4. Wenn das Asset auf der zweiten Ebene vorhanden ist, wählen Sie es aus. Falls auf der zweiten Ebene kein Asset vorhanden ist, erstellen Sie es wie folgt:
   a. Wählen Sie **Aktion auswählen** > **Neu** > **Standort**, um die Seite mit den *Standort-Asset-Details* anzuzeigen.
   b. Geben Sie einen Namen für das neue Asset ein. Beispiel: San Jose.
   c. Wählen Sie in diesem Beispiel als *übergeordneten Standort* die **Abteilung West** aus. Falls zahlreiche Standort-Assets vorhanden sind, geben Sie im Feld *Filter* die ersten Zeichen ein, um die verfügbaren Auswahlmöglichkeiten im Feld *Übergeordneter Standort* zu begrenzen.
5. Klicken Sie auf **Speichern**.
6. Erstellen Sie nach Bedarf weitere Standort-Assets.

   Beispielsweise könnten Sie für jedes Gebäude auf einem Gelände oder für jedes Regal in einem Rechenzentrum einen separaten Standort erstellen.

Asset-Typen löschen

Sie können Asset-Typen löschen, wenn diesen Typen keine Assets zugewiesen sind.

Sie haben Asset-Typen, denen keine Assets zugewiesen sind.

1. Rufen Sie die Liste *Asset-Typen* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.

b. Klicken Sie in der linken Navigationsleiste auf **Asset Management** und anschließend auf **Asset-Typen**.

2. Aktivieren Sie das Kontrollkästchen neben einem Asset-Typ.
3. Wählen Sie **Aktion auswählen > Löschen** und klicken Sie dann zum Bestätigen auf **Ja**.

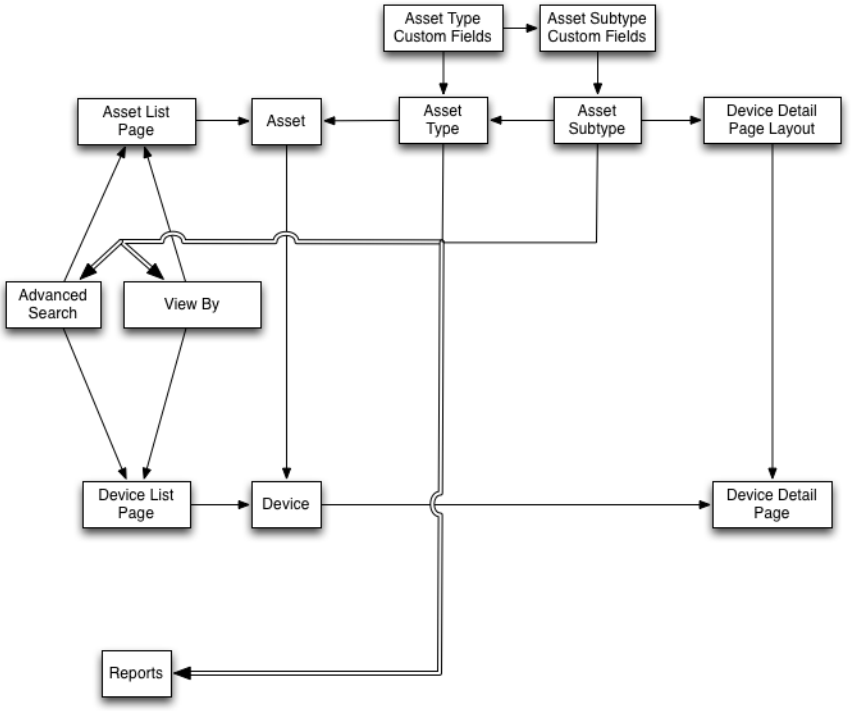
Informationen zu Asset-Untertypen, benutzerdefinierten Feldern und Gerätedetail-Voreinstellungen

Asset-Untertypen sind Unterkategorien von Assets, die Sie zu jedem Asset-Typ hinzufügen können, einschließlich benutzerdefinierter Asset-Typen. So können Sie Untertypen von Assets, z. B. Geräte-Assets wie Computer, Drucker und Router sowie Software-Assets, die auf Windows, Mac oder Linux-Systemen im Appliance-Inventar ausgeführt werden, erkennen und verwalten.

Asset-Untertypen erben die Felder vom Asset-Typ. Sie können benutzerdefinierte Felder hinzufügen, damit die Appliance-Inventarerfassung relevante Informationen zu dem Asset-Untertyp erfassen kann. Sie können beispielsweise den Asset-Untertyp **Drucker** zum Asset-Typ **Gerät** hinzufügen. Daraufhin können Sie ein benutzerdefiniertes Feld für den Untertyp **Drucker** hinzufügen, z. B. *Toner*. Das Feld *Toner* steht daraufhin für Geräte-Assets mit dem Untertyp *Drucker* zur Verfügung.

HINWEIS: Damit die Appliance Felder von Asset-Untertypen von Geräten ohne Agenten-Software ausfüllt, müssen Sie den entsprechenden Asset-Untertyp zuweisen, wenn das Gerät konfiguriert wird, den entsprechenden Objektbezeichner (OID) ermitteln und den Bezeichner auf der Seite *Detail zur SNMP-Inventarkonfiguration* zum Untertypenfeld zuweisen. Sie können SNMP-Geräteuntertypen nach ihrer Konfiguration nicht mehr hinzufügen oder ändern. Siehe Liste der Objektbezeichner (OIDs) mithilfe der Administratorkonsole abrufen.

Darüber hinaus können Sie auswählen, ob die Details ausgeblendet werden sollen, die auf der Seite *Gerätedetail* für jeden Geräte-Asset-Untertyp angezeigt werden. Sie können beispielsweise Informationen, die für Drucker nicht relevant sind – wie *Installierte Programme*, *Erkannte Software* und *Software mit erfasster Nutzung* – auf der Seite *Gerätedetail* für Assets mit dem Untertyp **Drucker** ausblenden.



Workflow für die Verwendung von Asset-Untertypen mit SNMP-Geräten

Um Asset-Untertypen verwenden zu können, müssen Sie sie – neben sämtlichen benutzerdefinierten Feldern, die Sie verwenden möchten – zur Ihren Asset-Typen hinzufügen. Um die Felder mit Daten von SNMP-Geräten (Simple Network Management Protocol) zu bestücken, können Sie auch Objektbezeichner (OIDs) zu den benutzerdefinierten Feldern hinzufügen.

Der Workflow für die Verwendung von Asset-Untertypen mit SNMP-Geräten umfasst die folgenden Aufgaben:

1. Fügen Sie einen Geräte-Asset-Untertyp zum Asset-Typ und anschließend benutzerdefinierte Felder zum Untertyp hinzu. Siehe Asset-Untertypen hinzufügen und Voreinstellungen für die Seite "Gerätedetail" auswählen.
2. Fügen Sie Assets hinzu, die den Asset-Typ und den -Untertyp verwenden. Siehe Asset-Untertypen "Gerät" auf der Seite "Geräte" zuweisen oder ändern.

   WICHTIG: Sie müssen den entsprechenden Asset-Untertyp zuweisen, wenn das Gerät konfiguriert wird. Sie können SNMP-Geräteuntertypen nach ihrer Konfiguration nicht mehr hinzufügen oder ändern.

3. **Optional**: Füllen Sie die Felder aus:
   - Damit das System die Felder mit Daten von den SNMP-Geräten bestücken kann, beziehen Sie die für die benutzerdefinierten Felder zu verwendenden Objektbezeichner (OIDs), fügen Sie das Feld für Geräte ohne Agenten-Software auf der Seite *Detail zur SNMP-Inventarkonfiguration* hinzu, wählen Sie den Asset-Untertyp aus und fügen Sie daraufhin die OID-Information für die Felder hinzu. Siehe Liste der Objektbezeichner (OIDs) mithilfe der Administratorkonsole abrufen.
   - Aktualisieren Sie die Felder bei Bedarf manuell. Siehe Manuelle Aktualisierung von benutzerdefinierten Asset-Feldern.

Asset-Untertypen hinzufügen und Voreinstellungen für die Seite "Gerätedetail" auswählen

Sie können jedem beliebigen Asset-Typ, einschließlich benutzerdefinierter Asset-Typen, Asset-Untertypen hinzufügen und Sie können jedem Asset-Untertyp benutzerdefinierte Felder hinzufügen.

Außerdem können Sie wählen, welche Felder auf der Seite *Gerätedetail* angezeigt werden, und die Abschnitte festlegen, in denen diese Felder angezeigt werden sollen. Dadurch können Sie die Seite *Gerätedetail* anpassen und die wichtigsten Informationen betonen.

HINWEIS: Wenn die Organisationskomponente für die Appliance aktiviert ist, können Sie Asset-Untertypen für jede Organisation separat verwalten.

1. Rufen Sie die Seite *Details zum Asset-Typ* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Asset Management** und anschließend auf **Asset-Typen**.
   c. Die Seite *Details zum Asset-Typ* zeigen Sie an, wie folgt:
   - Klicken Sie auf den Namen eines Asset-Typs.
   - Wählen Sie **Aktion auswählen** > **Neu**.
2. Klicken Sie im Abschnitt *Untertypen* auf **Untertyp hinzufügen**.

HINWEIS: In einer Standardinstallation umfassen die Gerätebestände zwei Asset-Untertypen für Druckergeräte: *Laserdrucker: Farb-* und *Laserdrucker: Monochrom*. Jeder dieser Untertypen bietet eine gemeinsame Gruppe von Feldern, die für die meisten Drucker gelten. Die Appliance verfügt außerdem über eine Reihe von Druckervorlagen für typische SNMP-fähige Druckermodelle, basierend auf diesen Asset-Untertypen. Sie können nach Bedarf diese Vorlagen bearbeiten oder neue hinzufügen. Wenn Sie eine Druckervorlage auf ein Gerät anwenden, werden die in der Vorlage definierten Daten, wie z. B. Tonerfüllstände oder Beschreibungen, für den Drucker im nächsten Bestandzyklus erfasst. Weitere Informationen hierzu finden Sie unter Informationen zu Druckervorlagen.

Die Seite *Detail Asset-Untertyp* wird angezeigt. Im Abschnitt *Geerbte Felder* werden Felder angezeigt, die für den Asset-Untertyp verfügbar sind, da sie zum Asset-Typ hinzugefügt wurden.

3. Geben Sie im oberen Abschnitt die folgenden Informationen an und wählen Sie, ob der Asset-Untertyp als Standard verwendet werden soll:

Option	Beschreibung
Name	Der Name des Asset-Untertyps. Dieser Name wird in der Liste auf der Seite *Detail Asset-Typ* angezeigt.
Standard	Gibt an, ob der Asset-Untertyp als Standard für neue Assets verwendet werden soll. Wenn Sie dieses Kontrollkästchen aktivieren, werden neue Assets des ausgewählten Typs automatisch diesem Asset-Untertyp zugewiesen. Sie können diese Einstellung jederzeit ändern.

4. Klicken Sie im Abschnitt *Untertyp-Felder* in der Überschriftzeile auf der rechten Seite der Tabelle auf die Schaltfläche **Hinzufügen**: +.
5. Geben Sie die folgenden Informationen an:

Element	Beschreibung
Name	Der Name des Asset-Untertyps. Dieser Name bezeichnet den Asset-Untertyp auf der Seite *Asset-Details*.
Verfügbare Werte	Die Werte, die in Feldern mit Wertelisten angezeigt werden. Dieses Feld ist aktiviert, wenn Sie aus der Dropdown-Liste *Typ* die Option **Einfachauswahl** oder **Mehrfachauswahl** auswählen. Wenn Sie **Einfachauswahl** oder **Mehrfachauswahl** auswählen, müssen Sie mindestens einen Wert in dieses Feld eingeben. Wenn Sie mehrere Werte verwenden möchten, trennen Sie die einzelnen Werte mit einem Komma.
Standardwerte	Der Wert, der standardmäßig im Feld angezeigt wird. Wenn Sie aus der Dropdown-Liste *Typ* die Option **Einfachauswahl** oder **Mehrfachauswahl** auswählen, müssen Sie einen der im Feld *Verfügbare Werte* angegebenen Werte eingeben.
Erforderlich	Gibt an, ob das Feld obligatorisch oder optional ist. Wenn dieses Kontrollkästchen aktiviert ist, müssen Benutzer beim Erstellen von Assets

Element	Beschreibung
	des ausgewählten Typs einen Wert in das Feld eingeben.
Typ	Der Typ des Felds. Es gibt folgende Feldtypen: • **Anhang**: Damit können Benutzer Anhänge zum Asset hinzufügen. • **Währung**: Wird für monetäre Werte verwendet. • **Softwarekatalog**: Damit können Benutzer das Asset mit einer Anwendung im Softwarekatalog verknüpfen. • **Datum**: Wird für Kalenderinformationen verwendet. • **Label**: Damit können Benutzer dem Asset ein Label zuweisen. • **Link**: Wird für Internetlinks verwendet. Links müssen gültige URLs sein, beispielsweise **http://software.quest.com**. • **Mehrfachauswahl**: Zeigt eine Liste an, aus der mehrere Werte ausgewählt werden können. Die maximale Länge für jeden Wert beträgt 255 Zeichen. • **Hinweise**: Wird für zusätzliche Informationen verwendet. • **Nummer**: Wird für numerische Werte verwendet, die als ganze Zahlen ausgedrückt werden. • **Übergeordnet**: Damit können Sie mit dem Asset auf denselben Asset-Typ innerhalb einer Beziehung über-/untergeordneter Elemente verweisen. Sie könnten beispielsweise für Standorttypen eine Verbindung zu einem übergeordneten Element zulassen, sodass New York auf den Standort Nordamerika verweisen kann. Diese Angabe kann im Berichtssystem dazu verwendet werden, alle Assets in Nordamerika anzuzeigen. • **Einfachauswahl**: Zeigt eine Werteliste an, aus der nur ein einzelner Wert ausgewählt

Element	Beschreibung
	werden kann. Die maximale Länge für jeden Wert beträgt 255 Zeichen. • **Text**: Wird für zusätzlichen Text verwendet. Die maximale Länge beträgt 255 Zeichen. • **Zeitstempel**: Damit werden Tag und Uhrzeit zum Datensatz hinzugefügt. • **Benutzer**: Damit werden Benutzerdatensätze mit einem Asset verknüpft. • **Assets Asset-Typ**: Damit werden Beziehungen zwischen Asset-Typen angegeben.
Mehrfachauswahl	Gibt an, ob das Asset-Feld auf andere Assets verweist. Ein Kontrollkästchen ist aktiviert, wenn Sie aus der Dropdown-Liste *Typ* die Option **Assets Asset-Typ** auswählen. Aktivieren Sie dieses Kontrollkästchen, damit dieses benutzerdefinierte Feld auf mehrere Datensätze verweisen kann. Beispiel: Sie möchten, dass ein Feld auf mehrere Geräte verweist, die für eine bestimmte Lizenz genehmigt wurden. In diesem Fall aktivieren Sie das Kontrollkästchen. Für ein Feld mit einer einzelnen Zuordnung, beispielsweise einen Drucker, der nur von einer Abteilung verwendet wird, deaktivieren Sie das Kontrollkästchen. **HINWEIS:** Wenn Sie ein Asset erstellen, werden die verfügbaren Assets des angegebenen Asset-Typs in dieses Feld geladen. Sind keine Assets des angegebenen Typs vorhanden, ist das Feld leer.
Geräteabschnitt	Die Stelle auf der Seite *Gerätedetail*, wo das Feld angezeigt wird. Wenn Sie z. B. einen Asset-Untertyp „Drucker“ mit einem Feld *Toner-Füllstand* erstellen, könnten Sie *Hardware* auswählen, weil dieses Feld mit Drucker-Hardware in Beziehung steht. Sie können jedoch in der Dropdown-Liste einen beliebigen Abschnitt für ein beliebiges Feld auswählen.

6. Klicken Sie am Ende der Zeile auf **Speichern**.
7. Wählen Sie für Asset-Untertypen "Gerät" die Informationen, die auf der Seite *Gerätedetail* ein- oder ausgeblendet werden sollen:
   a. Scrollen Sie nach unten zu *Untertyp, Gerätedetails: Abschnitte anzeigen/ausblenden*.
   b. Aktivieren Sie die Kontrollkästchen neben den Elementen, die Sie anzeigen möchten.

   Für einen Untertyp "Drucker" können Sie gegebenenfalls *Inventarinformationen* anzeigen, z. B. *Hardware*, *Drucker*, *Netzwerkschnittstellen* und *SNMP-Daten*.

   c. Deaktivieren Sie die Kontrollkästchen neben den Elementen, die ausgeblendet werden sollen.

Für einen Untertyp "Drucker" können Sie gegebenenfalls die Abschnitte *Software* und *Dell Command | Monitor* ausblenden, da diese für Drucker nicht relevant sind.

8. Klicken Sie unten auf der Seite auf **Speichern**.

Damit das System auf der Seite *Gerätedetail* in die benutzerdefinierten Felder automatisch Daten eintragen kann, müssen Sie die entsprechenden Objektbezeichner abrufen und die Feld-OIDs zuordnen. Siehe:

- Objektbezeichner Feldern in der Inventartabelle zuordnen
- Liste der Objektbezeichner (OIDs) mithilfe der Administratorkonsole abrufen

Die manuelle Aktualisierung benutzerdefinierter Felder ist auf der Seite *Asset-Details* möglich. Siehe Manuelle Aktualisierung von benutzerdefinierten Asset-Feldern.

Asset-Untertypen bearbeiten

Sie können Asset-Untertypen bearbeiten. Wenn für die Appliance die Organisationskomponente aktiviert ist, können Sie die Asset-Untertypen für jede Organisation separat bearbeiten.

1. Rufen Sie die Seite *Details zum Asset-Typ* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Asset Management** und anschließend auf **Asset-Typen**.
   c. Klicken Sie auf den Namen eines Asset-Typs, um die Seite *Details zum Asset-Typ* anzuzeigen.
2. Klicken Sie im Abschnitt *Untertypen* neben jedem zu bearbeitenden Untertyp auf die Schaltfläche **Bearbeiten**: .

   Die Seite *Detail Asset-Untertyp* wird angezeigt. Weitere Informationen über die für Asset-Untertypen verfügbaren Optionen finden Sie unter Asset-Untertypen hinzufügen und Voreinstellungen für die Seite "Gerätedetail" auswählen.
3. Klicken Sie am Ende der Zeile auf **Speichern** und anschließend unten auf der Seite auf **Speichern**.

Asset-Untertyp als Standardeinstellung festlegen

Um ein neues Asset automatisch einem Untertyp zuzuweisen, können Sie ein Asset-Untertyp als Standard markieren.

1. Rufen Sie die Seite *Details zum Asset-Typ* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Asset Management** und anschließend auf **Asset-Typen**.
   c. Die Seite *Details zum Asset-Typ* zeigen Sie an, wie folgt:
   - Klicken Sie auf den Namen eines Asset-Typs.
   - Wählen Sie **Aktion auswählen** > **Neu**.
2. Klicken Sie im Abschnitt *Untertypen* neben jedem zu bearbeitenden Untertyp auf die Schaltfläche **Bearbeiten**: .

Die Seite *Detail Asset-Untertyp* wird angezeigt.

3. Aktivieren Sie im Abschnitt das Kontrollkästchen neben *Standardeinstellung*.
4. Klicken Sie am Ende der Zeile auf **Speichern** und anschließend unten auf der Seite auf **Speichern**.

   Der für den Asset-Untertyp wird als Standard-Untertyp für den Asset-Typ gekennzeichnet. Neue Assets des ausgewählten Typs werden automatisch diesem Asset-Untertyp zugewiesen.

Verfügbare Asset-Untertypen anzeigen

Sie können sich die Asset-Untertypen anzeigen lassen, die für von Ihnen verwaltete Asset-Typen verfügbar sind. Wenn für die Appliance die Organisationskomponente aktiviert ist, können Sie die Asset-Untertypen für jede Organisation separat anzeigen und verwalten.

- Rufen Sie die Seite *Details zum Asset-Typ* auf:

  1. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
  2. Klicken Sie in der linken Navigationsleiste auf **Asset Management** und anschließend auf **Asset-Typen**.
  3. Die Seite *Details zum Asset-Typ* zeigen Sie an, wie folgt:

  - Klicken Sie auf den Namen eines Asset-Typs.
  - Wählen Sie **Aktion auswählen** > **Neu**.

  Die für den Asset-Typ verfügbaren Untertypen stehen in der Tabelle *Untertypen*.

Asset-Untertypen auf der Seite "Assets" anzeigen

Mit dem Menü *Anzeigen nach* können Sie die Seite *Assets* nach Untertypen sortieren.

1. Rufen Sie die Seite *Assets* auf.
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Asset Management** und anschließend auf **Assets**.

   Die Spalte *Untertypen* zeigt die Untertyp-Zuordnungen für Assets. **Kein(e)** bedeutet, dass das Asset keinem Untertyp zugewiesen ist.
2. Zum Anzeigen der Untertypen, die einem bestimmten Asset-Typ zugewiesen sind, wählen Sie oben rechts im Menü *Anzeigen nach* einen Asset-Typ aus.
3. Zum Anzeigen eines einzelnen Untertyps für einen Asset-Typ wählen Sie im Menü *Anzeigen nach* erst einen Asset-Typ und dann einen Untertyp aus.

   Zum Untertyp gehörende Felder wie *Tonerfüllstand* für einen *Drucker*-Untertyp werden als Spalten auf der Seite *Assets* angezeigt.

Asset-Untertypen "Gerät" auf der Seite "Geräte" zuweisen oder ändern

Wenn Sie über vorhandene Geräte-Assets verfügen, die keinen Untertypen zugewiesen sind, können Sie diesen Assets auf der Seite *Geräte* Untertypen zuweisen oder ihre Untertypen-Zuweisungen ändern, wenn es sich bei diesen Geräten nicht um SNMP-Geräte (Simple Network Management Protocol) handelt. Untertypen für SNMP-Geräte müssen bei der Erstkonfiguration der Geräte zugewiesen werden.

Sie verfügen im Appliance-Inventar über vorhandene Geräte-Assets und haben Untertypen für den Geräte-Asset-Typ erstellt. Siehe Asset-Untertypen hinzufügen und Voreinstellungen für die Seite "Gerätedetail" auswählen.

WICHTIG: Bei SNMP-Geräten müssen Sie bei der Gerätekonfiguration den entsprechenden Asset-Untertyp zuweisen. SNMP-Asset-Untertypen können nach der Konfiguration nicht mehr hinzugefügt oder geändert werden.

1. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
2. Wählen Sie **Inventar > Geräte** aus, um die Seite *Geräte* anzuzeigen.
3. So filtern Sie die Liste so, dass nur Geräte angezeigt werden, die einem Untertyp zugewiesen sind:
   a. Klicken Sie oberhalb der Liste auf der rechten Seite auf die Registerkarte **Erweiterte Suche**, um den Bereich *Erweiterte Suche* anzuzeigen.
   b. Geben Sie die Kriterien an, die erforderlich sind, um Geräte zu finden.
   c. Klicken Sie auf **Suchen**.

   TIPP: Sie können auch die Dropdown-Liste *Anzeigen nach* verwenden, um Geräte zu ermitteln, die zu einem bestimmten Asset-Untertyp gehören.
4. Aktivieren Sie die Kontrollkästchen neben den Geräten, die Sie einem Untertyp zuweisen möchten. Um alle Geräte auszuwählen, aktivieren Sie das Kontrollkästchen neben *Name* im oberen Tabellenbereich.
5. Wählen Sie **Aktion auswählen > Status ändern in** aus.

   Der Untertyp wird ausgewählt und die Änderung wird auf der Seite *Gerätedetail* bei der nächsten Inventarmeldung für das Gerät angezeigt.

Assets zu Untertypen zuweisen oder Untertypenzuweisungen auf der Seite "Assets" ändern

Wenn Sie über vorhandene Assets verfügen, die keinen Asset-Untertypen zugewiesen sind, können Sie diesen Assets auf der Seite *Assets* Untertypen zuweisen oder ihre Untertypenzuweisungen ändern, wenn es sich bei diesen Geräten nicht um SNMP-Geräte (Simple Network Management Protocol) handelt. Untertypen für SNMP-Geräte müssen bei der Erstkonfiguration der Geräte zugewiesen werden.

Sie verfügen im Appliance-Inventar über vorhandene Assets und haben Untertypen für Asset-Typen erstellt. Siehe Asset-Untertypen hinzufügen und Voreinstellungen für die Seite "Gerätedetail" auswählen.

WICHTIG: Bei SNMP-Geräten müssen Sie bei der Gerätekonfiguration den entsprechenden Asset-Untertyp zuweisen. SNMP-Asset-Untertypen können nach der Konfiguration nicht mehr hinzugefügt oder geändert werden.

1. Rufen Sie die Liste *Assets* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Asset Management** und anschließend auf **Assets**.
2. So filtern Sie die Liste so, dass nur Assets angezeigt werden, die einem Untertyp zugeordnet sind:
   a. Klicken Sie oberhalb der Liste auf der rechten Seite auf die Registerkarte **Erweiterte Suche**, um den Bereich *Erweiterte Suche* anzuzeigen.
   b. Geben Sie die Kriterien an, die erforderlich sind, um Assets zu finden, deren Untertypen zugewiesen oder geändert werden sollen.
   c. Klicken Sie auf **Suchen**.

TIPP: Sie können auch die Dropdown-Liste *Anzeigen nach* verwenden, um Assets zu ermitteln, die zu einem bestimmten Asset-Untertyp gehören.

3. Aktivieren Sie die Kontrollkästchen neben den Assets, die Sie einem Untertyp zuweisen möchten. Um alle Assets auszuwählen, aktivieren Sie das Kontrollkästchen neben *Name* im oberen Tabellenbereich.
4. Wählen Sie **Nach** > **Asset-Typ** > **Gerät anzeigen** aus und wählen Sie einen der verfügbaren Einträge in der Liste aus. Wenn Sie beispielsweise alle Geräteassets anzeigen möchten, wählen Sie **Alle Geräteuntertypen** aus.
5. Wählen Sie **Aktion auswählen** > **Status ändern in** aus.

   Die ausgewählten Assets werden dem ausgewählten Untertyp zugewiesen.

Manuelle Aktualisierung von benutzerdefinierten Asset-Feldern

Sie können bei Bedarf benutzerdefinierte Asset-Felder manuell aktualisieren. Dies ist nützlich, wenn es Asset-Informationen gibt, die nicht automatisch gesammelt werden können, oder wenn Sie ergänzende Informationen eines Assets nachverfolgen wollen.

Sie haben benutzerdefinierte Asset-Untertypen oder benutzerdefinierte Asset-Felder hinzugefügt.

TIPP: Statt benutzerdefinierte Asset-Felder manuell zu aktualisieren, können Sie die Informationen auch aus einer Tabellenkalkulationsdatei importieren. Siehe Importieren von Lizenzdaten in CSV-Dateien.

1. Rufen Sie die Seite *Asset-Detail* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Asset Management** und anschließend auf **Assets**.
   c. Klicken Sie auf den Namen des zu aktualisierenden Assets.
2. Ändern Sie die Asset-Felder nach Bedarf.
3. Klicken Sie auf **Speichern**.

Asset-Untertypen löschen

Sie können Asset-Untertypen löschen, wenn diesen Untertypen keine Assets zugewiesen sind.

Sie haben Asset-Untertypen, denen keine Assets zugewiesen sind.

1. Rufen Sie die Seite *Details zum Asset-Typ* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Asset Management** und anschließend auf **Asset-Typen**.
   c. Klicken Sie auf den Namen eines Asset-Typs, um die Seite *Details zum Asset-Typ* anzuzeigen:
2. Klicken Sie im Abschnitt *Untertypen* neben jedem zu bearbeitenden Untertyp auf die Schaltfläche **Löschen**: .
3. Klicken Sie im Dialogfenster auf **Ja**.

   Der Asset-Untertyp wird aus dem Asset-Typ gelöscht und damit verbundene Felder werden sofort entfernt.

Verwalten von Software-Assets

Sie können den Software-Asset-Typen anpassen und nach Bedarf Software-Assets für Anwendungen im Inventar der Seite *Software* hinzufügen.

Software-Assetkönnen nur für das Inventar der Seite *Software* hinzugefügt werden. Software-Assets sind für Anwendungen im Inventar des Softwarekatalogs nicht erforderlich.

Software-Asset-Typ anpassen

Sie können die für den Software-Asset-Typ verfügbaren Felder nach Bedarf hinzufügen, ändern und löschen. Der Software-Asset-Typ ist die Vorlage, die beim Hinzufügen von Software-Assets die verfügbaren Felder bestimmt.

Wenn auf der Appliance die Organisationskomponente aktiviert wurde, können Sie den Software-Asset-Typ für jede Organisation separat anpassen.

1. Rufen Sie die Seite *Details zum Asset-Typ* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Asset Management** und anschließend auf **Asset-Typen**.
   c. Klicken Sie in der Spalte **Name** auf **Software**.
2. **Optional**: Ändern Sie Felder oder Werte in der Tabelle *Asset-Felder*.
   a. Klicken Sie auf die Schaltfläche **Bearbeiten** am Ende einer Zeile: .
   b. Ändern Sie die Feldinformationen nach Bedarf und klicken Sie dann am Ende der Zeile auf **Speichern**.
   c. Um ein Feld hinzuzufügen, klicken Sie in der Tabellenüberschrift auf die Schaltfläche **Hinzufügen**: . Fügen Sie Feldinformationen hinzu und klicken Sie dann am Ende der Zeile auf **Speichern**.
   d. Klicken Sie zum Ändern der Feldreihenfolge auf die Schaltfläche **Neu sortieren** am Ende der Zeile: .
   e. Um ein Feld zu entfernen, klicken Sie auf die Schaltfläche **Löschen**: .
3. Klicken Sie unten auf der Seite auf **Speichern**.

Software-Assets hinzufügen

Software-Assets ermöglichen es Ihnen, Informationen zu Anwendungen im Inventar der Seite *Software* zu verfolgen. Sie können beispielsweise nach dem Hinzufügen von Software-Assets für Anwendungen diese Assets Lizenz-Assets zuordnen, um Lizenzinformationen zu verfolgen.

Sie können Software-Assets für Anwendungen erstellen, die automatisch oder manuell zur Appliance hinzugefügt wurden.

HINWEIS: Software-Assets sind nicht erforderlich, um die Lizenz-Compliance für Anwendungen im Inventar des *Softwarekatalogs* einzurichten. Siehe Informationen zur Lizenz-Compliance für Anwendungen im Softwarekatalog.

Wenn auf der Appliance die Organisationskomponente aktiviert wurde, erstellen Sie Software-Assets für jede Organisation separat.

Software-Assets in der Liste "Software" hinzufügen

Sie können Software-Assets für mehrere Anwendungen gleichzeitig hinzufügen, indem Sie die Anwendungen in der Liste *Software* auswählen.

Software-Assets können nur für das Inventar der Seite *Software* hinzugefügt werden. Software-Assets sind für Anwendungen im Inventar des Softwarekatalogs nicht erforderlich.

1. Rufen Sie die Liste *Software* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Inventar** und anschließend auf **Software**.
2. Aktivieren Sie das Kontrollkästchen neben einer oder mehreren Anwendungen.
3. Wählen Sie **Aktion auswählen** > **Asset erstellen**.

Die Assets werden erstellt und in der Liste *Assets* angezeigt.

Software-Assets im Abschnitt "Assets" hinzufügen

Sie können im Abschnitt *Assets* jeweils ein Software-Asset erstellen.

Software-Assets können nur für das Inventar der Seite *Software* hinzugefügt werden. Software-Assets sind für Anwendungen im Inventar des Softwarekatalogs nicht erforderlich.

1. Rufen Sie die Seite *Software-Assets-Details* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Asset Management** und anschließend auf **Assets**.
   c. Wählen Sie **Aktion auswählen** > **Neu** > **Software**.
2. Füllen Sie die Asset-Felder wie folgt aus:

Option	Beschreibung
Untertyp	Der Asset-Subtyp, falls zutreffend.
Asset-Status	Der Asset-Status, falls zutreffend. Sie können einen Standard-Asset-Status oder einen benutzerdefinierten festlegen (falls vorhanden).

Option	Beschreibung
	Eine Standardinstallation des Appliance umfasst die folgenden Asset-Status: • **Aktiv**: Alle Assets, die bereitgestellt, aktiv oder in Gebrauch sind. • **Entsorgt**: Ein Asset, das nicht mehr verfügbar ist. • **Abgelaufen** Ein Software-Lizenz oder ein Vertrags-Asset, das abgelaufen ist. • **Auf Lager**: Ein vor kurzem empfangenes Asset. • **Fehlt** Alle Assets, die nicht gefunden werden können. • **Reparieren** Ein Asset, das repariert wird. • **Reserviert** Ein Asset, das für eine bestimmte Person oder einen Zweck reserviert ist. • **außer Kraft gesetzt**: Alle Assets, die das Ende ihrer Lebensdauer erreicht haben oder nicht mehr in Gebrauch sind. • **Gestohlen**: Ein Asset, das als gestohlen gemeldet wurde. Weitere Informationen hierzu finden Sie unter Asset-Lebenszyklus-Einstellungen anzeigen und konfigurieren.
Standort	Wählen Sie den Standort für den Asset aus der Dropdown-Liste aus. Die Werte in dieser Liste enthalten alle Standorte die auf der Appliance definiert sind. Siehe Standorte verwalten **TIPP:** Standorte können definiert für alle Asset-Standardtypen definiert werden, einschließlich Kostenstellen, Abteilungen, Geräte, Lizenzen, Software und Hersteller.
Name	Der Asset-Name. z. B. Office Pro SW-Asset.
Software	Der Namen der Anwendung, die dem Asset zugeordnt wird. Um nach einem Element zu suchen, tippen Sie dessen Namen in die Liste.
Softwarelabel	Wählen Sie in der Dropdown-Liste ein Label aus. Die Liste ist anfangs noch leer, bis Sie ein Smart Label erstellt haben. Sie können Eingaben im Feld machen, um nach bestimmten Labels zu suchen.
Barcodedaten	Überprüfen oder hinzufügen von Barcodes, die Sie diesem Asset zuordnen möchten. Siehe Barcodes zu Assets hinzufügen.
Barcodename	
Barcodeformat	

a. Geben Sie im Feld *Name* einen Namen für das Asset ein: z. B. Office Pro SW-Asset.
b. **Optional**: Wählen Sie im Feld *Software* den Namen der Anwendung aus, die mit dem Asset verknüpft werden soll. Um nach einem Element zu suchen, tippen Sie dessen Namen in die Liste.
c. **Optional**: Wählen Sie im Feld *Softwarelabel* aus der Dropdown-Liste *Label auswählen* ein Label aus. Die Liste ist anfangs noch leer, bis Sie ein Smart Label erstellt haben. Wenn Sie die Labelliste filtern möchten, geben Sie im Feld *Filter* einige Zeichen des Labelnamens ein.

3. Klicken Sie auf **Speichern**.

Das neue Asset wird auf der Liste *Assets* angezeigt.

Verwalten physischer und logischer Assets

Zu physischen Assets zählen Hardware und Software sowie Büromöbel. Logische Assets beinhalten Standorte, Kostenstellen und Anbieter.

Die Inventarkomponente der Appliance sendet automatisch Informationen zu physischen Assets – wie z. B. Geräte, die das Software- und Hardwareinventar an die Appliance melden – an die Asset Management-Komponente. Bei physischen und logischen Assets, die kein Inventar an die Appliance melden, werden die Informationen jedoch manuell hinzugefügt und aktualisiert. Siehe Manuelle Aktualisierung von benutzerdefinierten Asset-Feldern.

Die Verwaltung logischer Assets ermöglicht Folgendes:

- Kennzeichnen und Schützen logischer Assets
- Erstellen von Beziehungen zwischen logischen Assets und Verwenden dieser Beziehungen in Berichten, beispielsweise geographische Beziehungen oder Beziehungen zwischen Geschäftsentitäten

Des Weiteren können Sie benutzerdefinierte logische Assets (beispielsweise Supportverträge) hinzufügen. Hierüber können Sie zusätzliche Metadaten zu diesen Objekten erfassen.

Physische Asset-Typen hinzufügen

Sie können bei Bedarf physische Asset-Typen hinzufügen.

1. Rufen Sie die Seite *Details zum Asset-Typ* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Asset Management** und anschließend auf **Asset-Typen**.
   c. Wählen Sie **Aktion auswählen** > **Neu**.
2. Geben Sie im Feld *Name* einen aussagekräftigen Namen für das Asset ein, z. B. Laptop.
3. Geben Sie im Feld *Standard-Asset-Status* einen Standard-Asset-Status oder einen benutzerdefinierten ein (falls vorhanden).

Eine Standardinstallation der Appliance umfasst die folgenden Asset-Status:

- **Aktiv**: Alle Assets, die bereitgestellt, aktiv oder in Gebrauch sind.
- **Entsorgt**: Ein Asset, das nicht mehr verfügbar ist.
- **Abgelaufen** Ein Software-Lizenz oder ein Vertrags-Asset, das abgelaufen ist.
- **Auf Lager**: Ein vor kurzem empfangenes Asset.
- **Fehlt** Alle Assets, die nicht gefunden werden können.
- **Reparieren** Ein Asset, das repariert wird.
- **Reserviert** Ein Asset, das für eine bestimmte Person oder einen Zweck reserviert ist.
- **außer Kraft gesetzt**: Alle Assets, die das Ende ihrer Lebensdauer erreicht haben oder nicht mehr in Gebrauch sind.
- **Gestohlen**: Ein Asset, das als gestohlen gemeldet wurde.

4. Wenn Sie Benutzern ohne Administratorrolle erlauben möchten, Assets dieses Typs zu löschen, wählen Sie **Benutzern ohne Administratorberechtigungen das Löschen von Assets erlauben** aus. Diese Option ist standardmäßig deaktiviert. Diese Option kann nur von Administratoren konfiguriert werden. Für andere Benutzertypen wird dieses Feld auf der Seite angezeigt, ist jedoch deaktiviert.

   Weitere Informationen über Benutzerrollen finden Sie unter Benutzerrollen hinzufügen oder bearbeiten.

5. Wenn Assets dieses Typs den Asset-Speicherort in den Asset-Details anzeigen sollen, wählen Sie **Speicherorteinstellungen anzeigen** aus. Diese Option ist standardmäßig deaktiviert.

6. Klicken Sie unter *Barcodes* auf + und geben Sie die folgenden Informationen an:

Option	Beschreibung
Barcodedaten	Die Barcode-Nummer. Barcode-Nummern sind immer eindeutig, sie können nicht von mehreren Assets gemeinsam genutzt werden. Es ist jedoch für ein aktives Asset möglich, einen Barcode mit einem archivierten Asset gemeinsam zu nutzen.
Barcodename	Der mit diesem Asset-Typ verknüpfte Barcode-Tag. Es kann jeweils nur einen Barcode gleichen Typs pro Asset geben.
Barcodeformat	Das Barcodeformat. Beispielsweise UPC-A, Code 11 oder UPC-E.

   Sie können beliebig viele Barcodes nach Bedarf hinzufügen.

7. Klicken Sie rechts auf der Seite auf die Schaltfläche **Hinzufügen**: +.

   Eine neue Zeile wird angezeigt.

8. Geben Sie die folgenden Informationen in die neue Zeile ein. Beispiel:
   a. Geben Sie im Feld *Name* den Wert Marke ein.
   b. Aktivieren Sie in der Spalte *Erforderlich* das Kontrollkästchen, um das Feld als erforderlich festzulegen.
   c. Wählen Sie aus der Dropdown-Liste *Typ* die Option **Einfachauswahl** aus.

      Das Feld *Verfügbare Werte* ist aktiviert.

   d. Kehren Sie zum Feld *Verfügbare Werte* zurück und geben Sie die Marken ein, die Sie verwenden. Diese werden in der Auswahlliste angezeigt. Trennen Sie die Marken mit Kommas.

Beispiel: Apple, Dell, IBM. Damit wird sichergestellt, dass Markennamen wie beispielsweise IBM konsistent und ohne Varianten wie etwa IBM oder International Business Machines verwendet werden.

9. Klicken Sie am Ende der Zeile auf **Speichern**, und fügen Sie eine Zeile hinzu:
   a. Klicken Sie auf die Schaltfläche **Hinzufügen**: +.
   b. Geben Sie zusätzliche Informationen in die neue Zeile ein.

   Beispiel:

   - Geben Sie im Feld *Name* den Wert Seriennummer ein.
   - Wählen Sie aus der Dropdown-Liste *Typ* den Typ **Text** aus.
10. Klicken Sie am Ende der Zeile auf **Speichern**, und fügen Sie eine Zeile hinzu:
    a. Klicken Sie auf die Schaltfläche **Hinzufügen**: +.
    b. Geben Sie zusätzliche Informationen in die neue Zeile ein.

    Beispiel:

    - Geben Sie im Feld *Name* den Wert Standort ein.
    - Wählen Sie aus der Dropdown-Liste *Typ* die Option **Asset-Standort** aus.
11. Klicken Sie am Ende der Zeile auf **Speichern**, und fügen Sie eine Zeile hinzu:
    a. Klicken Sie auf die Schaltfläche **Hinzufügen**: +.
    b. Geben Sie zusätzliche Informationen in die neue Zeile ein.

    Beispiel:

    - Geben Sie im Feld *Name* die Abteilung ein und wählen Sie aus der Dropdown-Liste *Typ* die Option **Asset-Abteilung** aus.
    - Geben Sie im Feld *Name* die Kostenstelle ein und wählen Sie aus der Dropdown-Liste *Typ* die Option **Asset-Kostenstelle** aus.
12. Klicken Sie am Ende der Zeile auf **Speichern**, und fügen Sie eine Zeile hinzu:
    a. Klicken Sie auf die Schaltfläche **Hinzufügen**: +.
    b. Geben Sie zusätzliche Informationen in die neue Zeile ein.

    Beispiel:

    - Geben Sie im Feld *Name* den Wert Ablauf der Garantie ein.
    - Wählen Sie aus der Dropdown-Liste *Typ* den Typ **Datum** aus. Das Format wird in der Form **JJJJ-MM-TT** angegeben. Der unterstützte Wertebereich liegt zwischen 1000-01-01 und 9999-12-31.
13. Klicken Sie am Ende der Zeile auf **Speichern** und anschließend unten auf der Seite auf **Speichern**.

Gerätebestände archivieren

Sie können Gerätebestände nach Bedarf archivieren.

Appliance-Administratoren können Gerätebestände archivieren, die nicht mehr verwendet werden. Wenn Sie einen Gerätebestand archivieren, ist das Gerät nicht mehr in der Anzahl der Knotenlizenzen für die Appliance enthalten. Geräte, die zur Archivierung markiert werden, werden nach einer vordefinierten Anzahl Tage archiviert, gemäß der Angaben in den allgemeinen Einstellungen. Der Standardzeitraum beträgt drei Tage. Dies ermöglicht es Administratoren, die Markierung für das Gerät gegebenenfalls zurückzusetzen.

Weitere Informationen über die Änderung der Zeitspanne, während der Assets zur Archivierung markiert werden, finden Sie unter Allgemeine Einstellungen auf Verwaltungs- oder organisationsspezifischer Ebene konfigurieren

Wurde ein Gerät archiviert, wird sein Datensatz gelöscht und es kann nicht mehr auf den vorherigen aktiven Status zurückgesetzt werden. Sie können die Gerätedetails für einen archivierten Gerätebestand falls erforderlich überprüfen.

1. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
2. Klicken Sie in der linken Navigationsleiste auf **Assets**.
3. Führen Sie einen der folgenden Schritte aus:
   - **Wählen Sie in der Liste** *Assets* **einen Gerätebestand aus. Klicken Sie auf Aktion auswählen > Archiv.**
   - **Wählen Sie in der Liste** *Assets* **den Namen eines Gerätebestands aus. Klicken Sie auf der angezeigten Seite** *Asset Detail* **auf Archivieren.**
4. Geben Sie im angezeigten Dialogfeld *Asset archivieren* im Feld *Archivierungsgrund* den Grund für diese Aktion ein und klicken Sie auf **Speichern**.

   Das Dialogfeld *Asset archivieren* wird geschlossen und die Liste der *Assets* wird aktualisiert und zeigt an, dass die Archivierung des Gerätebestands aussteht ( ). Läuft die Zeitspanne für die ausstehende Archivierung ab, archiviert die Appliance den Bestand und sie erhält den Status „archiviert“ ( ).
5. Wenn Sie einen Gerätebestand aus dem Zustand „Archivierung ausstehend“ löschen möchten:
   a. Klicken Sie in der Liste *Assets* auf den Namen eines Assets, dessen Zustand „Archivierung ausstehend“ ist.
   b. Klicken Sie auf der angezeigten Seite *Asset Detail* auf **Ausstehende Archivierung rückgängig machen**.

   Die Seite *Asset Detail* wird geschlossen und die Liste der *Assets* wird aktualisiert und zeigt an, dass die Archivierung des Gerätebestands nicht länger aussteht.
6. Wenn Sie die Gerätedetails für einen archivierten Gerätebestand überprüfen wollen, klicken Sie in der Liste *Assets* in der Spalte *Name* auf den Gerätenamen in Klammern.

   Die Seite *Gerätedetails* wird angezeigt. Diese Seite enthält eine Teilmenge der Informationen, die normalerweise für nicht archivierten Bestand angezeigt wird. Weitere Informationen zu den Feldern, die auf dieser Seite angezeigt werden, finden Sie unter Elementegruppen und -abschnitte in Gerätedetails.

Verwalten und Verwenden von manuellen Asset-Informationen

Für Assets, die ihr Inventar nicht automatisch an die Appliance melden, können Sie Asset-Informationen manuell hinzufügen. Dies ist nützlich bei logischen Assets, wie z. B. Standorten, Kostenstellen und Anbietern, sowie bei physischen Assets, wie z. B. Büromobiliar und -geräten. Manuell importierte oder hinzugefügte Asset-Informationen müssen bei Änderungen manuell aktualisiert werden.

Es gibt zwei Möglichkeiten, Asset-Informationen auf dem neuesten Stand zu halten:

- Verwalten Sie die Informationen in Excel Tabellen und importieren Sie sie daraufhin regelmäßig in die Appliance.
- Pflegen Sie die Daten manuell in der Komponente "Asset Management".

Wählen Sie in jedem Fall eine Methode aus und verwenden Sie sie konsistent, sodass die Daten stets aktuell sind.

Erstellen einer Administratorrolle für Assets

Sie können eine Administratorrolle für Assets erstellen, um anderen Benutzern das Aktualisieren von Assets in der Appliance zu gestatten.

Informationen zum Erstellen von Rollen finden Sie unter Einrichten von Rollen für Benutzerkonten.

Planen regelmäßiger Importe

Für eine effiziente Pflege der Asset-Informationen sollten Sie die Quellentabellen immer wieder aktualisieren. Bei jedem Importvorgang ermittelt die Komponente Asset Management, ob die Datensätze importiert oder aktualisiert werden müssen. Hierfür wird der zum Zeitpunkt der Asset-Erstellung festgelegte primäre Schlüssel (PS) zugrunde gelegt.

- Wenn der primäre Schlüssel einem vorhandenen Datensatz entspricht, werden die Daten durch die Komponente Asset Management verglichen und der Datensatz wird bei Bedarf aktualisiert.
- Falls die Zeile keinen übereinstimmenden primären Schlüssel enthält, wird ein neuer Datensatz erstellt.

Siehe Importieren von Lizenzdaten in CSV-Dateien.

TIPP: Führen Sie vor dem Importieren neuer Daten ggf. einen Bericht aus, um Ihre aktuellen Daten zu exportieren. Falls die Struktur der neuen Daten einen Fehler enthält, können Sie dadurch die ursprünglichen Daten wiederherstellen.

Verwenden von Asset-Daten in Berichten

Sie können die Daten aus der Komponente Asset Management in Standardberichte exportieren.

Zu den Standardberichten zählen folgende:

- **Nicht genehmigte Softwareinstallation**: Zeigt auf Geräten gefundene Software ohne genehmigte Lizenz an.
- **Software-Compliance, einfach**: Zeigt die Anzahl der verfügbaren Lizenzen an, beispielsweise die Daten aus der Liste *Assets*.
- **Softwarelizenz-Compliance, abgeschlossen**: Listet die Software und die Geräte auf, die von den einzelnen Lizenzen betroffen sind.

Sie haben auch die Möglichkeit, eigene Berichte zu erstellen. Siehe Informationen zu Berichten.

Standorte verwalten

Ein Standort repräsentiert einen physischen Ort, der eine oder mehrere Ihrer Ressourcen enthält.

Sie können nach Bedarf Standorte hinzufügen, ändern, verschieben und löschen.

Standorte verwalten

Standorte stehen für physische Standorte, die ein oder mehrere Assets enthalten. sie basieren auf Standorttypen.

Sie können Standorte hinzufügen, verschieben oder löschen oder Standortdetails nach Bedarf in eine Datei exportieren.

1. Rufen Sie die Liste *Standorte* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.

b. Klicken Sie in der linken Navigationsleiste auf **Asset Management** und anschließend auf **Standorte**.

2. Wählen Sie **Aktion wählen** > **Neu**, um einen Standort hinzuzufügen.

   Weitere Informationen finden Sie unter Standorte hinzufügen oder bearbeiten.

3. So löschen Sie einen Standort:
   a. Wählen Sie die Zeile, die den Standort enthält, den Sie löschen wollen.
   b. Wählen Sie **Aktion auswählen** > **Löschen**.
   c. **Optional**. Im angezeigten Dialogfeld *Standort löschen* geben Sie den neuen Standort, an den Sie alle mit dem Standort, den Sie löschen möchten, verbundenen Assets verschieben wollen.
   d. Klicken Sie auf **Bestätigen**.

   HINWEIS: Löschen eines übergeordneten Standorts löscht seine untergeordneten Standorte nicht vom System.

4. So verändern Sie einen Standort:
   a. Wählen Sie die Zeile mit dem Standort, den Sie verschieben möchten.
   b. Wählen Sie **Aktion auswählen** > **Verschieben**.
   c. Im angezeigten Dialogfeld *Standort verschieben* geben Sie den übergeordneten Standort an, wohin der Standort verschoben werden soll.
   d. Klicken Sie auf **Bestätigen**.

   Die Liste der *Standorte* wird aktualisiert, die verschobenen Standorte werden nicht mehr angezeigt. Klicken Sie in der Zeile die die übergeordneten Standorte enthält auf ▸ rechts neben dem Standortname, um die untergeordneten Standorte der jeweiligen übergeordneten Standorte anzuzeigen.

5. Fügen Sie im Feld *Name* den Namen hinzu oder ändern Sie ihn bei Bedarf.

   TIPP: Für die Asset-Typen „Gerät“ und „Lizenz“ stehen weitere Optionen zur Verfügung. Siehe Informationen zum Anpassen des Asset-Typs "Gerät" und Anpassen des Lizenz-Asset-Typs.

6. So exportieren Sie einen oder mehrere Standorten in eine Datei:
   a. Wählen Sie die Zeilen mit den Standorten, die Sie exportieren möchten.
   b. Wählen Sie **Aktion wählen** > **Exportieren** und dann die jeweilige Option.

   Um beispielsweise alle Standorte in eine CSV-Datei zu exportieren, wählen Sie sie in der Liste aus und wählen dann **Aktion wählenExportAlle in CSV-Format exportieren**.

   Sie können Standortinformationen aus einer Datei unter Verwendung des Assistenten *Importieren von Assets* importieren. Weitere Informationen hierzu finden Sie unter Asset-Daten mithilfe von CSV-Dateien importieren.

Standorte hinzufügen oder bearbeiten

Auf der Seite *Standortdetails* sehen Sie die Details des ausgewählten Standorts.

Standortinformationen sind statisch und ändern sich nur, wenn Sie Daten importieren oder Daten manuell ändern.

1. Rufen Sie die Seite *Standortdetail* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Asset Management** und anschließend auf **Standorte**.

c. Führen Sie eine der folgenden Aktionen aus, um die Seite mit den *Standortdetails* anzuzeigen:

- Klicken Sie auf den Namen eines Standorts.
- Wählen Sie **Aktion auswählen** > **Neu**.

2. Geben Sie die folgenden Informationen über den Standort ein: **Subtyp**, **Name** (erforderlich), **Beschreibung**, **Website**, **Adresse**, **Gebietsschema** und **Telefonnummer**.
3. Wenn Sie einen vorhandenen Standort bearbeiten und einem Gerät zuordnen möchten, klicken Sie im Abschnitt *Zugeordnete Geräte* auf +, wählen Sie ein Gerät aus und klicken Sie auf **Hinzufügen**.

   Das ausgewählte Gerät wird in der Liste unten angezeigt.
4. Wenn Sie einen vorhandenen Standort bearbeiten und mit einem Asset verknüpfen möchten, klicken Sie im Bereich *Zugewiesene Assets* auf +, wählen Sie ein Asset aus und klicken Sie auf **Hinzufügen**.

   Das ausgewählte Asset wird in der Liste unten angezeigt.
5. Klicken Sie auf **Speichern**.

Speicherortfelder anpassen

Sie können Felder auf der Seite *Standortdetail* nach Bedarf umbenennen, erstellen und löschen.

1. Rufen Sie die Seite *Standortdetail* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Asset Management** und anschließend auf **Standorte**.
   c. Führen Sie eine der folgenden Aktionen aus, um die Seite mit den *Standortdetails* anzuzeigen:
   - Klicken Sie auf den Namen eines Standorts.
   - Wählen Sie **Aktion auswählen** > **Neu**.
2. Geben Sie gegebenenfalls Standortuntertypen an.
   a. Klicken Sie im Abschnitt *Untertypen* auf **Untertyp hinzufügen**.

      Die Seite *Asset-Untertypdetails des Speicherorts* wird angezeigt. Im Abschnitt *Geerbte Felder* werden Felder angezeigt, die für den Asset-Untertyp verfügbar sind, da sie zum Asset-Typ hinzugefügt wurden.
   b. Auf der angezeigten Seite *Asset-Untertypdetails des Speicherorts* könne Sie nach Bedarf folgende Optionen überprüfen und bearbeiten:

Optionen	Beschreibung
Name	Name des Standort-Untertyps. Dieser Name wird in der Liste auf der Seite *Standortdetail* angezeigt.
Standard	Gibt an, ob der Standort-Subtyp als Standard für neue Standorte verwendet wird. Wenn Sie dieses Kontrollkästchen aktivieren, werden neue Standorte automatisch diesem Asset-Untertyp zugewiesen. Sie können diese Einstellung jederzeit ändern.
Geerbte Felder	Dieser Abschnitt zeigt die Standardspeicherort Felder an. Sie können an diesem Abschnitt keine Änderungen vornehmen.

Optionen	Beschreibung
Untertyp-Felder	Fügen Sie nach Bedarf Felder hinzu, die spezifisch für diesen Subtyp sind. Klicken Sie auf +, um ein Feld hinzuzufügen und geben Sie die erforderlichen Informationen ein.

c. Klicken Sie auf **Speichern**.

3. Wenn Sie möchten, dass die Standorte Barcodes verwenden, legen Sie im Bereich *Barcode-Tags* ein oder mehrere Tags fest.

   Standorte, die Sie in Zukunft erstellen, verfügen über Barcode-Tags für die Konfiguration. Geben Sie beispielsweise einen Unternehmens-Tag und einen Dell Standort-Tag an, sind Barcodes mit diesen beiden Tags zur Auswahl auf der Seite *Standort-Details* verfügbar, wenn Sie einen Standort erstellen oder bearbeiten.

   Um einen Barcode hinzufügen, klicken Sie auf +, geben Sie den Barcode ein und klicken auf **Speichern**.

4. Geben Sie nach Bedarf zusätzliche Standortfelder an.

   a. Klicken Sie um ein ein Feld im Bereich *Asset Felder* hinzuzufügen auf +.

   b. Geben Sie die folgenden Informationen für jedes neue Feld an:

Option	Beschreibung
Name	Der Feldname.
Verfügbare Werte	Die Werte, die in Feldern mit Wertelisten angezeigt werden. Dieses Feld ist aktiviert, wenn Sie aus der Dropdown-Liste *Typ* die Option **Einfachauswahl** oder **Mehrfachauswahl** auswählen. Wenn Sie **Einfachauswahl** oder **Mehrfachauswahl** auswählen, müssen Sie mindestens einen Wert in dieses Feld eingeben. Wenn Sie mehrere Werte verwenden möchten, trennen Sie die einzelnen Werte mit einem Komma.
Erforderlich	Gibt an, ob das Feld obligatorisch oder optional ist. Wenn dieses Kontrollkästchen aktiviert ist, müssen Benutzer beim Erstellen von Assets des ausgewählten Typs einen Wert in das Feld eingeben.

Option	Beschreibung
Typ	Der Typ des Felds. Es gibt folgende Feldtypen: • **Anhang**: Damit können Benutzer Anhänge zum Asset hinzufügen. • **Währung**: Wird für monetäre Werte verwendet. • **Softwarekatalog**: Damit können Benutzer das Asset mit einer Anwendung im Softwarekatalog verknüpfen. • **Datum**: Wird für Kalenderinformationen verwendet. • **Label**: Damit können Benutzer dem Asset ein Label zuweisen. • **Link**: Wird für Internetlinks verwendet. Links müssen gültige URLs sein, beispielsweise **http://software.quest.com**. • **Mehrfachauswahl**: Zeigt eine Liste an, aus der mehrere Werte ausgewählt werden können. Die maximale Länge für jeden Wert beträgt 255 Zeichen. • **Hinweise**: Wird für zusätzliche Informationen verwendet. • **Nummer**: Wird für numerische Werte verwendet, die als ganze Zahlen ausgedrückt werden. • **Übergeordnet**: Damit können Sie mit dem Asset auf denselben Asset-Typ innerhalb einer Beziehung über-/untergeordneter Elemente verweisen. Sie könnten beispielsweise für Standorttypen eine Verbindung zu einem übergeordneten Element zulassen, sodass New York auf den Standort Nordamerika verweisen kann. Diese Angabe kann im Berichtssystem dazu verwendet werden, alle Assets in Nordamerika anzuzeigen. • **Herausgeber**: Ermöglicht Ihnen die Auswahl aus der aktuellen Liste der Herausgeber im Softwarekatalog. • **Einfachauswahl**: Zeigt eine Werteliste an, aus der nur ein einzelner Wert ausgewählt

Option	Beschreibung
	werden kann. Die maximale Länge für jeden Wert beträgt 255 Zeichen. • **Text**: Wird für zusätzlichen Text verwendet. Die maximale Länge beträgt 255 Zeichen. • **Zeitstempel**: Damit werden Tag und Uhrzeit zum Datensatz hinzugefügt. • **Benutzer**: Damit werden Benutzerdatensätze mit einem Asset verknüpft. • **Assets Asset-Typ**: Damit werden Beziehungen zwischen Asset-Typen angegeben.

   c. Klicken Sie auf **Speichern**.

5. Klicken Sie auf **Speichern**.

Verwalten von Verträgen

Ein Vertrag ist eine Form von Kaufvereinbarung zwischen dem Verkäufer und dem Endbenutzer, der die Nutzungsbedingungen darlegt. Verträge können mit Software und Hardware verbunden sein, die Ihr Unternehmen verwendet, ebenso wie mit materiellen Objekten wie Büromöbeln oder Kaffeemaschinen.

Sie können Verträge nach Bedarf hinzufügen, bearbeiten oder löschen.

Verträge verwalten

Verträge stellen Kauf- oder Dienstvereinbarungen für Hardware- und Softwareelemente dar, die in Ihrem Unternehmen verwendet werden, ebenso wie für materielle Güter oder Dienste, wie Bürostühle oder Kaffeelieferanten.

Sie können Verträge hinzufügen, verschieben oder löschen oder Standortdetails nach Bedarf in eine Datei exportieren.

1. Rufen Sie die Liste *Verträge* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Asset Management** und anschließend auf **Verträge**.
2. Wählen Sie **Aktion wählen** > **Neu**, um einen Vertrag hinzuzufügen.

   Weitere Informationen finden Sie unter Verträge hinzufügen oder bearbeiten.
3. So löschen Sie einen Vertrag:
   a. Wählen Sie die Zeile, die den Vertrag enthält, den Sie löschen wollen.
   b. Wählen Sie **Aktion auswählen** > **Löschen**.
4. So exportieren Sie einen Vertrag oder mehrere Verträge in eine Datei:
   a. Wählen Sie die Zeilen mit den Verträgen, die Sie exportieren möchten.
   b. Wählen Sie **Aktion wählen** > **Exportieren** und dann die jeweilige Option.

   Um beispielsweise alle Verträge in eine CSV-Datei zu exportieren, wählen Sie sie in der Liste aus und wählen dann **Aktion wählen** > **Exportieren** > **Alle in CSV-Format exportieren**.

Sie können Vertragsinformationen aus einer Datei unter Verwendung des Assistenten *Importieren von Assets* importieren. Weitere Informationen hierzu finden Sie unter Asset-Daten mithilfe von CSV-Dateien importieren.

Verträge hinzufügen oder bearbeiten

Auf der Seite *Kontaktdetails* sehen Sie die Details des ausgewählten Kontakts.

Verwenden Sie diese Seite, um Verträge hinzuzufügen oder zu bearbeiten.

1. Rufen Sie die Seite *Vertragsdetail* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Asset Management** und anschließend auf **Verträge**.
   c. Führen Sie eine der folgenden Aktionen aus, um die Seite *Vertragsdetail* anzuzeigen:
   - Klicken Sie auf den Namen eines Vertrags.
   - Wählen Sie **Aktion auswählen** > **Neu** > **Vertrags-Hardware**.
   - Wählen Sie **Aktion auswählen** > **Neu** > **Vertrags-Software**.
   - Wählen Sie **Aktion auswählen** > **Neu** > **Vertrags-Sonstige**.
2. Stellen Sie allgemeine Informationen zum Vertrag bereit.

   Verträge sind eine Form von Asset-Typen, und abgesehen vom Feld *Name*, welches immer erforderlich ist, können die mit jedem Vertragstyp verfügbaren Felder nach Bedarf geändert werden. Weitere Informationen zu Asset-Typen finden Sie unter Informationen zu Asset-Typen

   Die folgenden Felder erscheinen normalerweise auf jedem Vertrags-Datensatz:

Option	Beschreibung
Untertyp	Die Untertyp-Zuweisung dieses Vertrags-Assets, falls zutreffend. *Kein(e)* bedeutet, dass das Asset keinem Untertyp zugewiesen ist. Sie können die Vertrags-Untertypen im verfügbaren Vertrags-Asset-Untertyp (**Vertrags-Software**, **Vertrags-Hardware** oder **Vertrags-Sonstige**) angeben. Weitere Informationen zu Asset-Untertypen finden Sie unter Informationen zu Asset-Untertypen, benutzerdefinierten Feldern und Gerätedetail-Voreinstellungen.
Asset-Status	Der Vertragsstatus, falls zutreffend. Sie können einen Standard-Asset-Status oder einen benutzerdefinierten festlegen (falls vorhanden).

Option	Beschreibung
	Eine Standardinstallation des Appliance umfasst die folgenden Asset-Status: • **Aktiv**: Alle Assets, die bereitgestellt, aktiv oder in Gebrauch sind. • **Entsorgt**: Ein Asset, das nicht mehr verfügbar ist. • **Abgelaufen** Ein Software-Lizenz oder ein Vertrags-Asset, das abgelaufen ist. • **Auf Lager**: Ein vor kurzem empfangenes Asset. • **Fehlt** Alle Assets, die nicht gefunden werden können. • **Reparieren** Ein Asset, das repariert wird. • **Reserviert** Ein Asset, das für eine bestimmte Person oder einen Zweck reserviert ist. • **außer Kraft gesetzt**: Alle Assets, die das Ende ihrer Lebensdauer erreicht haben oder nicht mehr in Gebrauch sind. • **Gestohlen**: Ein Asset, das als gestohlen gemeldet wurde. Weitere Informationen hierzu finden Sie unter Asset-Lebenszyklus-Einstellungen anzeigen und konfigurieren.
Standort	Der Asset-Speicherort.
Name	Der Name des Vertrags.
Vertragsnummer	Die Vertragsnummer.
Vertragsbeschreibung	Weitere Informationen zum Vertrag.
Startdatum des Vertrags	Das Datum, an dem der Vertrag aktiviert wird.
Enddatum des Vertrags	Das Datum, an dem der Vertrag endet.
Jahrestag	**Nur für Software- und Hardware-Verträge**. Eine Anzeige, wann der Vertrag verlängert werden sollte.
Herausgeber	**Nur für Software- und Hardware-Verträge**. Der Herausgeber des Vertrags.
Herausgeber-Programm	**Nur für Software-Verträge**. Die zur Auswahl verfügbaren Einträge werden aus dem Softwarekatalog ausgefüllt, je nachdem, was Sie im Feld *Herausgeber* angegeben haben. Wenn Sie einen Herausgeber auswählen, werden die zur Auswahl in diesem Feld verfügbaren Einträge mit den mit dem ausgewählten Herausgeber

Option	Beschreibung
	verbundenen Programmeinträgen verknüpft, die in Ihrem Softwarekatalog vorliegen.
Hersteller	Der Name der Anwendung, die dem Vertrag zugeordnet ist. Sie können eine Auswahl aus den verfügbaren Herstellereinträgen vornehmen.
Hersteller-Vereinbarungsnummer	Die Nummer der Herstellervereinbarung, die dem Vertrag zugeordnet ist.
Hersteller	**Nur für Hardware-Verträge**. Der Hersteller des Geräts, das dem Vertrag zugeordnet ist.
Hardwaretyp	**Nur für Hardware-Verträge**. Der Typ des Hardwaregeräts, das dem Vertrag zugeordnet ist, wie etwa ein Laptop oder Server.
Hardware-Serie	**Nur für Hardware-Verträge**. Die Serie des Hardwaregeräts, das dem Vertrag zugeordnet ist.
Hardwaremodell	**Nur für Hardware-Verträge**. Die Modellnummer des Hardwaregeräts, das dem Vertrag zugeordnet ist.
Bestellnummer	Die Bestellnummer, die dem Vertrag zugeordnet ist.
Bestelldatum	Das Bestelldatum, das dem Vertrag zugeordnet ist.
Verknüpfter Vertrag	Ein weiterer Vertrag, der mit diesem Vertragseintrag verknüpft ist.
Name der Kontaktperson	Der Name der mit dem Vertrag verbundenen Kontaktperson.
Kontakt-E-Mail	Die E-Mail-Adresse der mit dem Vertrag verbundenen Kontaktperson.
Kontakt-Telefonnummer	Die Telefonnummer der mit dem Vertrag verbundenen Kontaktperson.
Anmerkungen	Weitere Informationen zu diesem Vertrag.
Anhang 1, **Anhang 2**	Jegliche zum Vertrag gehörige Dateianhänge.

3. **Optional**. Fügen Sie nach Bedarf einen oder mehrere Barcodes zum Vertrag hinzu.
   a. Klicken Sie unter *Barcodes* auf + und geben Sie die folgenden Informationen an:

Option	Beschreibung
Barcodedaten	Die Barcode-Nummer. Barcode-Nummern sind immer eindeutig, sie können nicht von mehreren Assets gemeinsam genutzt werden. Es ist jedoch für

Option	Beschreibung
	ein aktives Asset möglich, einen Barcode mit einem archivierten Asset gemeinsam zu nutzen.
Barcodename	Der mit diesem Asset-Typ verknüpfte Barcode-Tag. Es kann jeweils nur einen Barcode gleichen Typs pro Asset geben.
Barcodeformat	Das Barcodeformat. Beispielsweise UPC-A, Code 11 oder UPC-E.

4. Prüfen Sie die Informationen im Abschnitt *Service Desk*. Wenn Sie einen bestehenden Vertrag bearbeiten, der mit einem oder mehreren Service Desk-Tickets verknüpft ist, werden diese in diesem Abschnitt aufgelistet.
5. Prüfen Sie die Informationen im Abschnitt *Zugehörige Assets*. Wenn Sie einen bestehenden Vertrag bearbeiten, der mit einer oder mehreren Lizenzen verknüpft ist, werden diese in diesem Abschnitt aufgelistet.
6. Klicken Sie auf **Speichern**.

Verwalten von Lizenzen

Eine Lizenzvereinbarung ermöglicht Ihnen, logische oder physische Assets wie etwa eine Software oder Hardware zu verwenden.

Sie können Lizenzen hinzufügen, bearbeiten oder löschen und sie mit logischen oder physischen Assets verknüpfen.

Lizenzen verwalten

Lizenzen gestatten Ihnen die Verwendung Ihrer logischen oder physischen Assets, wie die in Ihrem Unternehmen verwendete Software oder Hardware.

Sie können Lizenzen hinzufügen, verschieben oder löschen oder Lizenzdetails nach Bedarf in eine Datei exportieren.

1. Rufen Sie die Liste *Lizenzen* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Asset Management** und anschließend auf **Lizenzen**.
2. Wählen Sie **Aktion wählen** > **Neu**, um einen Lizenz hinzuzufügen.

   Weitere Informationen finden Sie unter Lizenzen hinzufügen oder bearbeiten.
3. So löschen Sie eine Lizenz:
   a. Wählen Sie die Zeile, die die Lizenz enthält, die Sie löschen wollen.
   b. Wählen Sie **Aktion auswählen** > **Löschen**.
4. So exportieren Sie einen Lizenzeintrag oder mehrere Lizenzeinträge in eine Datei:
   a. Wählen Sie die Zeilen mit den Lizenzen, die Sie verschieben möchten.
   b. Wählen Sie **Aktion wählen** > **Exportieren** und dann die jeweilige Option.

Um beispielsweise alle Lizenzen in eine CSV-Datei zu exportieren, wählen Sie sie in der Liste aus und wählen dann **Aktion wählen** > **Exportieren** > **Alle in CSV-Format exportieren**.

Sie können Lizenzinformationen aus einer Datei unter Verwendung des Assistenten *Importieren von Assets* importieren. Weitere Informationen hierzu finden Sie unter Asset-Daten mithilfe von CSV-Dateien importieren.

Lizenzen hinzufügen oder bearbeiten

Auf der Seite *Lizenzdetails* sehen Sie die Details der ausgewählten Lizenz.

Verwenden Sie diese Seite, um Lizenzen hinzuzufügen oder zu bearbeiten. Lizenzen sind eine Form von Asset-Typen, und abgesehen vom Lizenznamen, der immer erforderlich ist, können die mit jedem Lizenz-Datensatz verfügbaren Felder nach Bedarf geändert werden. Weitere Informationen zu Asset-Typen finden Sie unterInformationen zu Asset-Typen.

1. Rufen Sie die Seite *Lizenzdetails* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Asset Management** und anschließend auf **Lizenzen**.
   c. Führen Sie eine der folgenden Aktionen aus, um die Seite *Lizenzdetails* anzuzeigen:
   - Klicken Sie auf den Namen einer Lizenz.
   - Wählen Sie **Aktion auswählen** > **Neu**.
2. Geben Sie auf der Seite *Lizenz-Asset-Details* auf der Registerkarte *Allgemein* die folgenden Informationen an:

Option	Beschreibung
Untertyp	Der mit der Lizenz zu verknüpfende Asset-Untertyp. Siehe Informationen zu Asset-Untertypen, benutzerdefinierten Feldern und Gerätedetail-Voreinstellungen.
Asset-Status	Der Lizenzstatus, falls zutreffend. Sie können einen Standard-Asset-Status oder einen benutzerdefinierten festlegen (falls vorhanden).

Option	Beschreibung
	Eine Standardinstallation des Appliance umfasst die folgenden Asset-Status: • **Aktiv**: Alle Assets, die bereitgestellt, aktiv oder in Gebrauch sind. • **Entsorgt**: Ein Asset, das nicht mehr verfügbar ist. • **Abgelaufen** Ein Software-Lizenz oder ein Vertrags-Asset, das abgelaufen ist. • **Auf Lager**: Ein vor kurzem empfangenes Asset. • **Fehlt** Alle Assets, die nicht gefunden werden können. • **Reparieren** Ein Asset, das repariert wird. • **Reserviert** Ein Asset, das für eine bestimmte Person oder einen Zweck reserviert ist. • **außer Kraft gesetzt**: Alle Assets, die das Ende ihrer Lebensdauer erreicht haben oder nicht mehr in Gebrauch sind. • **Gestohlen**: Ein Asset, das als gestohlen gemeldet wurde. Weitere Informationen hierzu finden Sie unter Asset-Lebenszyklus-Einstellungen anzeigen und konfigurieren.
Standort	Der Name des Standorts, in dem sich die Organisation befindet. Siehe Standorte verwalten.
Name	Name der Lizenz, beispielsweise **Office Professional Bestellnr. 1234**. Dies ist der Name, über den Sie nach dem Asset suchen. Wenn Sie mehrere Lizenzen mit einer Anwendung verknüpfen möchten, geben Sie die Bestellnummer oder das Kaufdatum in die nachstehenden Felder ein, um die Lizenzen voneinander zu unterscheiden.
Lizenzanzahl	Die Anzahl der Installationen oder Arbeitsplätze, die gemäß der Lizenz zulässig sind. Beispiel: 50.
Gültig für katalogisierte Software	Anwendungen im Softwarekataloginventar, für das die Lizenz gilt. Gegebenenfalls können Sie Lizenz-Assets mehreren Anwendungen im Softwarekatalog zuordnen. Es ist jedoch nicht erforderlich, Lizenz-Assets mit mehreren Versionen der gleichen Anwendung zu verknüpfen, da die Appliance dies automatisch durchführt, um Upgrades und Downgrades zu unterstützen. Sie können einfach beim Hinzufügen der Lizenzinformationen die aktuelle Version dem Lizenz-Asset zuordnen. Wenn Sie Anwendungen von anderen Herausgebern, z. B. von Microsoft Office oder Adobe Acrobat, dem gleichen Lizenz-Asset

Option	Beschreibung
	zuweisen, wird jeder Anwendung die im Lizenz-Asset angegebene Gesamtzahl der Lizenzplätze zugewiesen. Wenn das Lizenz-Asset z. B. über 100 Lizenzplätze verfügt, werden sowohl Microsoft Office als auch Adobe Acrobat 100 Lizenzplätze zugewiesen.
Gültig für Software	Lassen Sie dieses Feld leer. Eine Lizenz kann jedoch nicht gleichzeitig mit im Inventar der Seite *Softwarekatalog* und der Seite *Software* enthaltenen Anwendungen verknüpft werden. Weitere Informationen zum Erstellen von Lizenz-Assets finden Sie unter Hinzufügen von Lizenz-Assets für das Inventar der Seite "Software".
Lizenzmodus	Der Modus des Lizenz-Assets. Für Anwendungen, die Lizenzen erfordern, und zum Anzeigen von Lizenznutzungsinformationen auf der Seite *Lizenz-Compliance* wählen Sie entweder *Unternehmen* oder *Lizenz für Einheit* aus. **HINWEIS:** Die meisten Modi, einschließlich *Nicht angegeben*, *Client-Lizenz*, *Abonnement*, *Shareware*, *Freeware*, *OpenSource*, *Keine Lizenzierung* und *Standortlizenz*, werden nicht für die Lizenz-Compliance verwendet. Der Lizenzmodus wird in den folgenden Abschnitten der **Administratorkonsole** verwendet: • Liste *Lizenz-Compliance*. Siehe Anzeigen von Informationen zur Lizenz-Compliance für Anwendungen im Softwarekatalog. • In der auf dem *Dashboard* angezeigten Lizenz-Compliance-Tabelle. Werte, die auf der Seite *Asset-Details* ignoriert wurden, werden mit einer Nutzung von 100 Prozent angezeigt. Siehe Informationen zu Dashboard-Widgets.

3. Klicken Sie auf **Weiter**.
4. Geben Sie auf der Seite *Lizenz-Asset-Details* auf der Registerkarte *Einkauf* die folgenden Informationen an:

Option	Beschreibung
Vertrag	Das mit der Lizenz verbundene Vertrags-Asset.
Gültig für katalogisierte Software	Anwendungen im Softwarekataloginventar, für das die Lizenz gilt. Gegebenenfalls können Sie Lizenz-Assets mehreren Anwendungen im Softwarekatalog zuordnen. Es ist jedoch nicht erforderlich, Lizenz-Assets mit mehreren Versionen der gleichen Anwendung zu verknüpfen, da die Appliance dies automatisch durchführt, um Upgrades und Downgrades zu unterstützen. Sie können einfach

Option	Beschreibung
	beim Hinzufügen der Lizenzinformationen die aktuelle Version dem Lizenz-Asset zuordnen. Wenn Sie Anwendungen von anderen Herausgebern, z. B. von Microsoft Office oder Adobe Acrobat, dem gleichen Lizenz-Asset zuweisen, wird jeder Anwendung die im Lizenz-Asset angegebene Gesamtzahl der Lizenzplätze zugewiesen. Wenn das Lizenz-Asset z. B. über 100 Lizenzplätze verfügt, werden sowohl Microsoft Office als auch Adobe Acrobat 100 Lizenzplätze zugewiesen.
Produktschlüssel	Den mit der Lizenz verbundenen Produktschlüssel. Sie können die Standardinformationen ändern und bearbeiten, die für jeden Lizenz-Asset-Typ erfasst werden können.
Kosten pro Einheit	Die mit der Lizenz verbundenen Einheitskosten. Sie können die Standardinformationen ändern und bearbeiten, die für jeden Lizenz-Asset-Typ erfasst werden können.
Hersteller	Der Name des Hersteller-Assets, das Sie mit der Anwendung verknüpfen möchten. Die Dropdown-Liste *Hersteller* ist leer, wenn Sie kein Hersteller-Asset hinzugefügt haben. Um nach einem Hersteller zu suchen, tippen Sie seinen Namen in die Liste. **HINWEIS:** Die Zuweisung mehrerer Hersteller zu einem einzigen Softwarelizenz-Asset wird nicht empfohlen, da dies zu fehlerhaften Lizenz-Compliance-Informationen führen kann.
Bestellnummer	Die mit der Lizenz verknüpfte Bestellnummer.
Kaufdatum	Das Datum des Kaufs. Klicken Sie in das Feld und wählen Sie dann im Kalender ein Datum aus.
Kauf	Wählen Sie einen oder mehrere mit dieser Lizenz verknüpfte Einkaufsdatensätze aus. Siehe Kaufdatensätze verwalten.

5. Klicken Sie auf **Weiter**.
6. Geben Sie auf der Seite *Lizenz-Asset-Details* auf der Registerkarte *Wartung* die folgenden Informationen an:

Option	Beschreibung
Schließt Upgrade-Rechte ein	Gibt an, ob die Lizenz Upgrade-Rechte einschließt. Upgrade-Rechte beziehen sich auf die Möglichkeit, auf eine neuere Version der lizenzierten Software aufzurüsten, wenn eine solche Version verfügbar wird. Weitere Informationen hierzu finden Sie unter

Option	Beschreibung
	Informationen zu Lizenz-Upgrades. Wählen Sie eine der folgenden Optionen aus: • **Ja**: Upgrade-Rechte werden durch Vergleich der bestehenden Lizenzen für die ausgewählte Software und die Anzahl verfügbarer Lizenzen für neuere Versionen der gleichen Software berechnet. • **Ja - aus Liste auswählen**: Wählen Sie eine oder mehrere Softwareversionen, für die Sie Upgrade-Rechte gewähren möchten. Klicken Sie unter *Software-Liste aktualisieren* auf **Katalogisierte Software zum Hinzufügen auswählen**. Die daraufhin angezeigte Liste wird mit höheren Versionen der ausgewählten Software ausgefüllt, auf die die Lizenz aktualisiert werden kann. Wenn Sie auf einen Eintrag in der Liste klicken, erscheint Ihre Auswahl im Feld *Liste der Upgrade-Software*. Sie können nach Bedarf eine oder mehrere Versionen hinzufügen. Um ein Element aus der Liste zu löschen, wählen Sie es im Feld *Liste der Upgrade-Software* aus und klicken Sie auf **Entfernen**. • **Nein**: Wenn Sie keine Upgrade-Rechte für die ausgewählte Software gewähren möchten, aktivieren Sie diese Option.
Service inklusive	Gibt an, ob die Lizenz die Benutzer zum Upgrade der installierten Version der Anwendung berechtigt. Siehe Informationen zur Lizenz-Compliance für Anwendungen im Softwarekatalog.
Ablaufdatum	Das Ablaufdatum des Wartungszeitraums, wenn die Lizenz Wartung beinhaltet. Die Lizenz-Compliance-Funktion der Appliance nutzt Softwarekataloginformationen, z. B. das Herausgabedatum von Anwendungen. Wenn während des Wartungszeitraums neue Anwendungsversionen herausgegeben werden, sind diese automatisch durch dieses Lizenz-Asset abgedeckt.
Schließt Downgrade-Rechte ein	Gibt an, ob die Lizenz Downgrade-Rechte einschließt. Downgrade-Rechte beziehen sich auf die Möglichkeit, Lizenzen für neuere Softwareversionen auf ältere Versionen der gleichen Software anzuwenden. Weitere Informationen hierzu finden Sie unter Informationen zu Lizenz-Downgrades. Wählen Sie eine der folgenden Optionen aus: • **Ja**: Downgrade-Rechte werden durch Vergleich der bestehenden Lizenzen für die ausgewählte Software und die Anzahl

Option	Beschreibung
	verfügbarer Lizenzen für ältere Versionen der gleichen Software berechnet. • **Ja - aus Liste auswählen**: Wählen Sie eine oder mehrere Softwareversionen, für die Sie Downgrade-Rechte gewähren möchten. Klicken Sie unter *Software-Liste zurückstufen* auf **Katalogisierte Software zum Hinzufügen auswählen**. Die daraufhin angezeigte Liste wird mit niedrigeren Versionen der ausgewählten Software ausgefüllt, auf die die Lizenz herabgestuft werden kann. Wenn Sie auf einen Eintrag in der Liste klicken, erscheint Ihre Auswahl im Feld *Liste der Downgrade-Software*. Sie können nach Bedarf eine oder mehrere Versionen hinzufügen. Um ein Element aus der Liste zu löschen, wählen Sie es im Feld *Liste der Downgrade-Software* aus und klicken Sie auf **Entfernen**. • **Nein**: Wenn Sie keine Downgrade-Rechte für die ausgewählte Software gewähren möchten, aktivieren Sie diese Option.

7. Klicken Sie auf **Weiter**.
8. Geben Sie auf der Seite *Lizenz-Asset-Details* auf der Registerkarte *Zugehörig* die folgenden Informationen an:

Option	Beschreibung
Abteilung	Die Unternehmensgruppe oder Abteilung, der diese Anwendung gehört.
Kostenstelle	Die mit der Abteilung, der diese Anwendung gehört, verknüpfte Kostenstelle.
Genehmigt für Gerät	Die Geräte, die die Lizenz verwenden dürfen. Diese Information wird für Lizenz-Compliance-Berichte verwendet. Wenn die Anwendung zum Beispiel auf Geräten installiert ist, die nicht in der Liste genehmigter Geräte enthalten sind, werden diese Geräte im Bericht *Nicht genehmigte Softwareinstallation* aufgeführt. Die Lizenz-Compliance wird von der Appliance jedoch nicht erzwungen. Sie verhindert beispielsweise nicht, dass Anwendungen auf verwalteten Geräten installiert werden, wenn eine Lizenz abgelaufen ist oder anderweitig gegen die Compliance-Vorgaben verstoßen wird.
Barcodes	Fügen Sie bei Bedarf Barcodes hinzu, die mit dieser Lizenz verknüpft sind, bzw. bearbeiten Sie diese.

Option	Beschreibung
	Weitere Informationen hierzu finden Sie unter Barcodes zu Assets hinzufügen.

9. Klicken Sie auf **Weiter**.
10. Geben Sie auf der Seite *Lizenz-Asset-Details* auf der Registerkarte *Benutzerdefiniert* zusätzliche benutzerdefinierte Daten an. Sie können den Lizenz-Asset-Typ ändern und so viele weitere Felder aufnehmen, wie für Ihre geschäftlichen Ziele notwendig sind. Weitere Informationen hierzu finden Sie unter Asset-Typen hinzufügen oder anpassen.
11. Klicken Sie auf **Weiter**.
12. Geben Sie auf der Seite *Lizenz-Asset-Details* auf der Registerkarte *Hinweise* die folgenden Informationen an:

Option	Beschreibung
Anmerkungen	Geben Sie nach Bedarf beliebige weitere Informationen ein.
Lizenztext	Ergänzende Informationen zur Lizenz, z. B. eine Lizenznummer.

13. Klicken Sie auf **Speichern**.

Kaufdatensätze verwalten

Kaufdatensätze dokumentieren den Erwerb von physischen und Softwareprodukten für Ihre Organisation. Ihre Administratoren können einzelne Kaufdatensätze nachverfolgen und diese mit zugehörigen Lizenzvereinbarungen verknüpfen. Eine Lizenzvereinbarung für ein bestimmtes Asset kann mit einem oder mehreren Kaufdatensätzen verknüpft werden. Beispielsweise kann Ihr Unternehmen über eine Lizenzvereinbarung für Adobe Acrobat verfügen und mehrere Kaufdatensätze für diese Softwarelizenz (einen für jede Gruppe in der Organisation) haben.

Sie können Kaufdatensätze nach Bedarf hinzufügen, bearbeiten oder löschen und sie mit entsprechenden Lizenzvereinbarungen verknüpfen.

Kaufdatensätze verwalten

Ihre Administratoren können einzelne Kaufdatensätze nachverfolgen, die für den Einkauf von physischen und Softwareprodukten für Ihr Unternehmen eingesetzt werden.

Sie können nach Bedarf Kaufdatensätze hinzufügen, verschieben oder löschen oder Kaufdatensatzdetails in eine Datei exportieren.

1. Rufen Sie die Liste *Käufe* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Asset Management** und anschließend auf **Assets**.
2. Wählen Sie **Aktion wählen > Neu**, um einen Kaufdatensatz hinzuzufügen.

   Weitere Informationen finden Sie unter Kaufdatensätze hinzufügen oder bearbeiten.
3. So löschen Sie einen Kaufdatensatz:
   a. Wählen Sie die Zeile mit dem Kaufdatensatz aus, den Sie löschen wollen.

b. Wählen Sie **Aktion auswählen** > **Löschen**.

4. So exportieren Sie einen Kaufdatensatz oder mehrere Kaufdatensätze in eine Datei:
   a. Wählen Sie die die Zeilen mit den Kaufdatensätzen aus, die Sie exportieren möchten.
   b. Wählen Sie **Aktion wählen** > **Exportieren** und dann die jeweilige Option.

   Um beispielsweise alle Kaufdatensätze in eine CSV-Datei zu exportieren, wählen Sie sie in der Liste aus und wählen dann **Aktion wählen** > **Exportieren** > **Alle in CSV-Format exportieren**.

Kaufdatensätze hinzufügen oder bearbeiten

Auf der Seite *Kaufdetails* sehen Sie die Details des ausgewählten Kaufdatensatzes.

Verwenden Sie diese Seite, um Kaufdatensätze hinzuzufügen oder zu bearbeiten. Lizenzen sind eine Form von Asset-Typen, und abgesehen vom Kaufdatensatzname und von der Einheitsmenge, die immer erforderlich sind, können die mit jedem Lizenz-Datensatz verfügbaren Felder nach Bedarf geändert werden. Weitere Informationen zu Asset-Typen finden Sie unterInformationen zu Asset-Typen.

1. Rufen Sie die Seite *Lizenzdetails* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Asset Management** und anschließend auf **Assets**.
   c. Führen Sie eine der folgenden Aktionen aus, um die *Kaufdetailseite* anzuzeigen:

   - Klicken Sie auf den Namen einer verknüpften Appliance.
   - Wählen Sie **Aktion auswählen** > **Neu**.

2. Geben Sie auf der Seite *Kaufdetail* die folgenden Informationen an:

Option	Beschreibung
Untertyp	Der mit der Kaufdatensatz zu verknüpfende Asset-Untertyp. Sie können Kaufdatensätze für *Hardware*- oder *Software*elemente erstellen. Siehe Informationen zu Asset-Untertypen, benutzerdefinierten Feldern und Gerätedetail-Voreinstellungen.
Asset-Status	Der Status des Kaufdatensatzes, falls zutreffend. Sie können einen Standard-Asset-Status oder einen benutzerdefinierten festlegen (falls vorhanden).

Option	Beschreibung
	Eine Standardinstallation des Appliance umfasst die folgenden Asset-Status: • **Aktiv**: Alle Assets, die bereitgestellt, aktiv oder in Gebrauch sind. • **Entsorgt**: Ein Asset, das nicht mehr verfügbar ist. • **Abgelaufen** Ein Software-Lizenz oder ein Vertrags-Asset, das abgelaufen ist. • **Auf Lager**: Ein vor kurzem empfangenes Asset. • **Fehlt** Alle Assets, die nicht gefunden werden können. • **Reparieren** Ein Asset, das repariert wird. • **Reserviert** Ein Asset, das für eine bestimmte Person oder einen Zweck reserviert ist. • **außer Kraft gesetzt**: Alle Assets, die das Ende ihrer Lebensdauer erreicht haben oder nicht mehr in Gebrauch sind. • **Gestohlen**: Ein Asset, das als gestohlen gemeldet wurde. Weitere Informationen hierzu finden Sie unter Asset-Lebenszyklus-Einstellungen anzeigen und konfigurieren.
Standort	Der Name des Standorts, an dem sich die mit diesem Kauf erhaltene Ressource befindet. Siehe Standorte verwalten.
Name	Der Name des Kaufdatensatzes, beispielsweise **Office Professional Bestellnr. 1234**. Dies ist der Name, mit dem Sie diese Bestellung gegebenenfalls mit einer Lizenzvereinbarung verknüpfen.
Beschreibung	Die Beschreibung des Kaufdatensatzes.
Bestellnummer	Die Nummer der in Ihrem Unternehmen ausgestellten Bestellung.
Bestelldatum	Das Datum, an dem Ihr Unternehmen die Bestellung ausgestellt hat.
Anzahl	Die Anzahl der gekauften Einheiten.
Kosten pro Einheit	Die Kosten einer einzelnen gekauften Einheit.
Hersteller	Der Name des Herstellers, von dem das Gerät erworben wurde.

Option	Beschreibung
Hersteller-Bestellnummer	Die Bestellnummer, die vom Hersteller ausgestellt wurde.
Hersteller-Bestelldatum	Das Datum, an dem der Hersteller die Bestellung ausgestellt hat.
Kaufbeleg	Ein Bild, das ein Foto des Kaufdatensatzes zeigt.
Anmerkungen	Geben Sie nach Bedarf beliebige weitere Informationen ein.
Softwaretitel	**Nur Software**. Der Name der gekaufte Software.
Herausgeber	**Nur Software**. Der Herausgeber der gekaufte Software.
Vertrag	**Nur Software**. Der mit dem Softwarekauf verbundene Vertrag.
Produktschlüssel	**Nur Software**. Der Produktschlüssel der erworbenen Software.
Wartungsablaufdatum	**Nur Software**. Das Datum, an dem die Unterstützung der erworbenen Software endet.
Wartungsnachweis	**Nur Software**. Ein Bild mit dem Foto des Wartungsvertrags.
Hersteller	**Nur Hardware**. Der Hersteller des gekauften Hardwareelements.
Modell	**Nur Hardware**. Der Modellname des erworbenen Hardwareelements.
Spezifikationen	**Nur Hardware**. Alle Spezifikationen für das erworbene Hardwareelement, sofern zutreffend.
Seriennummer	**Nur Hardware**. Die Seriennummer des gekauften Hardwareelements.
Vertrag	**Nur Hardware**. Der mit dem gekauften Hardwareelement verbundene Vertrag.
Startdatum der Garantie	**Nur Hardware**. Das Datum, an dem die Herstellergarantie für das gekaufte Hardwareelement beginnt.
Enddatum der Garantie	**Nur Hardware**. Das Datum, an dem die Herstellergarantie für das erworbene Hardwareelement endet.

Option	Beschreibung
Enddatum des Supports	**Nur Hardware**. Das Datum, an dem der Support für das erworbene Hardwareelement endet.
Barcodes	Fügen Sie Barcode für mit dieser Bestellung verbundene Elemente hinzu oder bearbeiten Sie sie nach Bedarf. Weitere Informationen hierzu finden Sie unter Barcodes zu Assets hinzufügen.

Einrichten der Lizenz-Compliance

Um die Informationen zur Lizenz-Compliance für Anwendungen zu verfolgen, müssen Sie Lizenz-Assets erstellen. Lizenz-Assets können entweder Anwendungen im Inventar des Softwarekatalogs oder Anwendungen im Inventar der Seite *Software* zugeordnet werden. Es ist nicht möglich, Lizenz-Assets beiden Inventartypen gleichzeitig zuzuordnen.

Die Optionen für die Verfolgung von Lizenzen und die Anforderungen für die Einrichtung der Lizenz-Compliance für das Inventar des Softwarekatalogs unterscheiden sich von den Optionen und Anforderungen des Inventars der Seite *Software*.

Informationen zur Lizenz-Compliance für Anwendungen im Softwarekatalog

Die Appliance ermöglicht Ihnen die Anzeige von Informationen zur Lizenz-Compliance für Anwendungen im Inventar des Softwarekatalogs. Diese Informationen werden auf der Seite *Lizenz-Compliance* sowie im Dashboard-Widget zur Lizenz-Compliance angezeigt.

Nachdem Sie Lizenz-Assets für Anwendungen im Softwarekataloginventar konfiguriert haben, können Sie die Anzahl der auf agentenverwalteten Geräten installierten Arbeitsplätze, die Anzahl verfügbarer Arbeitsplätze, den Typ der Lizenzen und – sofern die Nutzungserfassung für die Anwendung aktiviert ist – Informationen zur Nutzung anzeigen. Darüber hinaus nutzt die Appliance Informationen im Softwarekatalog, um automatisch die richtigen Lizenzen auf Anwendungsversionen anzuwenden, die als Upgrade oder Downgrade eingeordnet wurden.

So richten Sie die Lizenz-Compliance für Anwendungen im Softwarekataloginventar ein:

- (Optional) Passen Sie den Lizenz-Asset-Typ gemäß Ihren Anforderungen an die Informationsverwaltung an. Siehe Anpassen des Lizenz-Asset-Typs.
- (Optional) Aktivieren Sie die Nutzungserfassung für Anwendungen im Softwarekatalog. Wenn die Nutzungserfassung aktiviert ist, wird auf der Seite "Lizenz-Compliance" angezeigt, ob Anwendungen in den letzten 30, 60 und 90 Tagen verwendet wurden. Siehe Informationen zur Erfassung der Softwarenutzung.
- Erstellen Sie Lizenz-Assets und ordnen Sie sie Anwendungen im Softwarekataloginventar zu. Siehe Hinzufügen von Lizenz-Assets für das Softwarekataloginventar.
- (Optional) Legen Sie Schwellenwerte für die Lizenz-Compliance fest, die im Dashboard-Widget verwendet werden. Standardmäßig beträgt der *Warnungsschwellenwert* 90. Der *Kritische Schwellenwert* 100. Siehe Konfigurieren von Warnungsschwellenwerten für die Lizenznutzung.

Informationen zu Lizenz-Upgrades

Pläne zur Anwendungswartung ermöglichen es Benutzern oft, Upgrades auf neuere Versionen der Anwendungen durchzuführen, wenn entsprechende Versionen verfügbar werden. Auf der Seite *Lizenz-Compliance* wird die Anzahl von Installationen angezeigt, bei denen es sich um Upgrades handelt.

Um Upgrades zu verfolgen, verwendet die Appliance Informationen im Softwarekatalog und die Lizenzdetails zur Bestimmung, ob neue Anwendungsversionen vorhandenen Lizenzen zugeordnet werden können. Wenn ein Lizenz-Asset beispielsweise für Version 1.0 einer Anwendung erstellt wurde und der Wartungsplan dem Benutzer ein Upgrade anbietet, wird Version 2.0 der Anwendung automatisch vom Lizenz-Asset abgedeckt, sobald sie veröffentlicht wird. In diesem Beispiel muss das Lizenz-Asset wie folgt konfiguriert werden:

- Das Feld *Service inklusive* muss auf *Ja* festgelegt werden.
- Das *Wartungsablaufdatum* muss nach dem Datum der allgemeinen Verfügbarkeit der Version 2.0 im Softwarekatalog liegen.
- Der *Lizenzmodus* muss *Unternehmen* oder *Lizenz für Einheit* lauten.
- *Upgrade-Rechte einschließen* muss auf *Ja* oder *Ja - Auswahl aus Liste* eingestellt werden.

Weitere Informationen zu diesen Einstellungen finden Sie unter Hinzufügen von Lizenz-Assets für das Softwarekataloginventar.

Informationen zu Lizenz-Downgrades

Anbieter ermöglichen es Benutzern oft, Lizenzen für neuere Anwendungsversionen auf ältere Versionen anzuwenden. Eine solche Installation wird als "Downgrade" bezeichnet. Auf der Seite *Lizenz-Compliance* wird die Anzahl von Installationen angezeigt, bei denen es sich um Downgrades handelt.

Lizenzplätze werden zunächst Installationen der neuesten Anwendungsversion zugewiesen. Falls daraufhin zusätzliche Arbeitsplätze verfügbar sind und der Anbieter Downgrades ermöglicht, werden diese Plätze automatisch Installationen zugewiesen, bei denen es sich um Downgrades handelt.

Lizenzen für Upgrades werden immer vor Lizenzen für Downgrades zugewiesen.

Anpassen des Lizenz-Asset-Typs

Sie können die für den Lizenz-Asset-Typ verfügbaren Felder nach Bedarf hinzufügen, ändern und löschen. Der Lizenz-Asset-Typ ist die Vorlage, die beim Hinzufügen von Lizenz-Assets die verfügbaren Felder bestimmt.

Wenn auf der Appliance die Organisationskomponente aktiviert wurde, können Sie den Lizenz-Asset-Typ für jede Organisation separat anpassen.

1. Rufen Sie die Liste *Asset-Typen* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Asset Management** und anschließend auf **Asset-Typen**.
2. Klicken Sie in der Spalte *Name* auf **Lizenz**, um die Seite *Details zum Asset-Typ* anzuzeigen.
3. Geben Sie im Feld *Standard-Asset-Status* einen Standard-Asset-Status oder einen benutzerdefinierten ein (falls vorhanden).

Eine Standardinstallation der Appliance umfasst die folgenden Asset-Status:

- **Aktiv**: Alle Assets, die bereitgestellt, aktiv oder in Gebrauch sind.
- **Entsorgt**: Ein Asset, das nicht mehr verfügbar ist.
- **Abgelaufen** Ein Software-Lizenz oder ein Vertrags-Asset, das abgelaufen ist.
- **Auf Lager**: Ein vor kurzem empfangenes Asset.
- **Fehlt** Alle Assets, die nicht gefunden werden können.
- **Reparieren** Ein Asset, das repariert wird.
- **Reserviert** Ein Asset, das für eine bestimmte Person oder einen Zweck reserviert ist.
- **außer Kraft gesetzt**: Alle Assets, die das Ende ihrer Lebensdauer erreicht haben oder nicht mehr in Gebrauch sind.
- **Gestohlen**: Ein Asset, das als gestohlen gemeldet wurde.

4. Geben Sie im Feld *Name* den Namen des Asset-Typs ein.

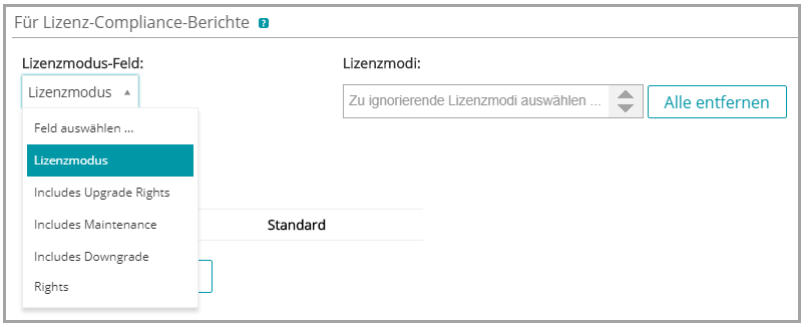
   Der Standardname für diesen Asset-Typ ist *Lizenz*.

5. **Optional**: Wählen Sie im Abschnitt *Für Lizenz-Compliance-Berichte* die Felder aus, die für die Lizenz-Compliance verwendet werden sollen.

   Informationen aus dem ausgewählten Feld *Lizenzmodus* werden im Dashboard-Widget *Lizenz-Compliance* angezeigt.

6. Führen Sie einen der folgenden Schritte aus:

   - **In der Dropdown-Liste *Lizenzmodus-Feld* muss die Standardoption Feld auswählen ausgewählt sein. Dadurch werden alle Werte im *Lizenzmodus-Feld* für die Lizenz-Compliance verfügbar. Wenn die Liste *Asset-Felder* mehrere Einfach- oder Mehrfachauswahlfelder enthält, wird das erste in der Liste angezeigte Feld mit all seinen Werten im Lizenz-Compliance-Widget verwendet.**
   - **Wählen Sie aus der Dropdown-Liste *Lizenzmodus-Feld* ein Feld für die Lizenz-Compliance aus, z. B. Lizenzmodus. Diese Dropdown-Liste enthält standardmäßig nur ein Feld, Sie können bei Bedarf aber weitere Felder hinzufügen. Wenn Sie ein Feld auswählen, beispielsweise Lizenzmodus (wie in der folgenden Abbildung dargestellt), wird nur das ausgewählte Feld für die Lizenz-Compliance verwendet.**



   Bei der Auswahl eines Felds können Sie außerdem gegebenfalls die Werte auswählen, die Sie in der Lizenz-Compliance-Tabelle ignorieren möchten. Ignorierte Werte werden mit einer Nutzung von 100 Prozent aufgeführt und in Grau angezeigt.
   Standardmäßig ist *Lizenzmodus* das einzige verfügbare Einfach- oder Mehrfachauswahlfeld und damit das einzige aufgeführte Feld. Wenn Sie in der Tabelle *Asset-Felder* Einfach- oder Mehrfachauswahlfelder hinzufügen, werden sie ebenfalls in dieser Liste angezeigt. Sie werden außerdem auf der Seite *Asset-Details* angezeigt, wenn Sie ein Lizenz-Asset hinzufügen. Allerdings wird nur das ausgewählte Feld beziehungsweise das erste Feld in der Liste *Asset-Felder* im Widget *Lizenz-Compliance* verwendet.

7. **Optional**: Ändern Sie das Feld *Lizenzmodus* oder Werte in der Tabelle *Asset-Felder*.

a. Klicken Sie auf die Schaltfläche **Bearbeiten** am Ende einer Zeile: .
b. Ändern Sie die Feldinformationen nach Bedarf und klicken Sie dann am Ende der Zeile auf **Speichern**.
c. Um ein Feld hinzuzufügen, klicken Sie in der Tabellenüberschrift auf die Schaltfläche **Hinzufügen**: . Fügen Sie Feldinformationen hinzu und klicken Sie dann am Ende der Zeile auf **Speichern**.
d. Um die Reihenfolge der Felder zu ändern, verwenden Sie die Schaltfläche **Neu sortieren**: .
e. Um ein Feld zu entfernen, klicken Sie auf die Schaltfläche **Löschen**: .

8. Klicken Sie unten auf der Seite auf **Speichern**.

Verwandte Themen

Anzeigen von Informationen zur Lizenz-Compliance und -Konfiguration.

Hinzufügen von Lizenz-Assets für das Softwarekataloginventar

Sie können Lizenz-Assets für Anwendungen im Softwarekataloginventar hinzufügen. Durch das Hinzufügen von Lizenz-Assets können Sie Lizenz-Compliance-Informationen in der Liste *Lizenz-Compliance* und im Dashboard-Widget *Lizenz-Compliance* anzeigen.

Anwendungen im Softwarekatalog müssen als *Erkannt*, *Nicht erkannt* oder *Lokal katalogisiert* klassifiziert werden. Lizenz-Assets für als *Nicht katalogisiert* klassifizierte Anwendungen können nicht hinzugefügt werden.

Wenn Sie Lizenz-Assets mit Anwendungen verknüpfen, können Sie auch auf der Seite *Softwarekatalogdetails* Lizenzinformationen anzeigen. Wenn auf der Appliance die Organisationskomponente aktiviert ist, können Sie die Lizenzinformationen für jede Organisation separat verwalten.

TIPP: Um Lizenz-Assets für mehrere Anwendungen auf einmal hinzuzufügen, können Sie die Informationen aus Tabellen oder CSV-Dateien importieren. Siehe Beispiel: Lizenzdaten aus vorbereiteten Tabellen importieren.

1. Rufen Sie die Liste *Softwarekatalog* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Inventar** und anschließend auf **Softwarekatalog**.
2. Klicken Sie auf den Namen einer Anwendung, um die *Softwarekatalog-Detailseite* anzuzeigen.
3. Klicken Sie am unteren Seitenrand auf **Neue Lizenz hinzufügen**, um die *Lizenz-Asset-Detailseite* anzuzeigen.
4. Geben Sie auf der Seite *Lizenz-Asset-Details* auf der Registerkarte *Allgemein* die folgenden Informationen an:

Option	Beschreibung
Untertyp	Der mit der Lizenz zu verknüpfende Asset-Untertyp. Siehe Informationen zu Asset-Untertypen, benutzerdefinierten Feldern und Gerätedetail-Voreinstellungen.
Asset-Status	Der Lizenzstatus, falls zutreffend. Sie können einen Standard-Asset-Status oder einen

Option	Beschreibung
	benutzerdefinierten festlegen (falls vorhanden). Eine Standardinstallation des Appliance umfasst die folgenden Asset-Status: • **Aktiv**: Alle Assets, die bereitgestellt, aktiv oder in Gebrauch sind. • **Entsorgt**: Ein Asset, das nicht mehr verfügbar ist. • **Abgelaufen** Ein Software-Lizenz oder ein Vertrags-Asset, das abgelaufen ist. • **Auf Lager**: Ein vor kurzem empfangenes Asset. • **Fehlt** Alle Assets, die nicht gefunden werden können. • **Reparieren** Ein Asset, das repariert wird. • **Reserviert** Ein Asset, das für eine bestimmte Person oder einen Zweck reserviert ist. • **außer Kraft gesetzt**: Alle Assets, die das Ende ihrer Lebensdauer erreicht haben oder nicht mehr in Gebrauch sind. • **Gestohlen**: Ein Asset, das als gestohlen gemeldet wurde. Weitere Informationen hierzu finden Sie unter Asset-Lebenszyklus-Einstellungen anzeigen und konfigurieren.
Standort	Der Name des Standorts, in dem sich die Organisation befindet. Siehe Standorte verwalten.
Name	Name der Lizenz, beispielsweise **Office Professional Bestellnr. 1234**. Dies ist der Name, über den Sie nach dem Asset suchen. Wenn Sie mehrere Lizenzen mit einer Anwendung verknüpfen möchten, geben Sie die Bestellnummer oder das Kaufdatum in die nachstehenden Felder ein, um die Lizenzen voneinander zu unterscheiden.
Lizenzanzahl	Die Anzahl der Installationen oder Arbeitsplätze, die gemäß der Lizenz zulässig sind. Beispiel: 50.
Gültig für katalogisierte Software	Anwendungen im Softwarekataloginventar, für das die Lizenz gilt. Gegebenenfalls können Sie Lizenz-Assets mehreren Anwendungen im Softwarekatalog zuordnen. Es ist jedoch nicht erforderlich, Lizenz-Assets mit mehreren Versionen der gleichen Anwendung zu verknüpfen, da die Appliance dies automatisch durchführt, um Upgrades und Downgrades zu unterstützen. Sie können einfach beim Hinzufügen der Lizenzinformationen die aktuelle Version dem Lizenz-Asset zuordnen. Wenn Sie Anwendungen von anderen Herausgebern, z. B. von Microsoft Office oder

Option	Beschreibung
	Adobe Acrobat, dem gleichen Lizenz-Asset zuweisen, wird jeder Anwendung die im Lizenz-Asset angegebene Gesamtzahl der Lizenzplätze zugewiesen. Wenn das Lizenz-Asset z. B. über 100 Lizenzplätze verfügt, werden sowohl Microsoft Office als auch Adobe Acrobat 100 Lizenzplätze zugewiesen.
Gültig für Software	Lassen Sie dieses Feld leer. Eine Lizenz kann jedoch nicht gleichzeitig mit im Inventar der Seite *Softwarekatalog* und der Seite *Software* enthaltenen Anwendungen verknüpft werden. Weitere Informationen zum Erstellen von Lizenz-Assets finden Sie unter Hinzufügen von Lizenz-Assets für das Inventar der Seite "Software".
Lizenzmodus	Der Modus des Lizenz-Assets. Für Anwendungen, die Lizenzen erfordern, und zum Anzeigen von Lizenznutzungsinformationen auf der Seite *Lizenz-Compliance* wählen Sie entweder *Unternehmen* oder *Lizenz für Einheit* aus. **HINWEIS:** Die meisten Modi, einschließlich *Nicht angegeben*, *Client-Lizenz*, *Abonnement*, *Shareware*, *Freeware*, *OpenSource*, *Keine Lizenzierung* und *Standortlizenz*, werden nicht für die Lizenz-Compliance verwendet. Der Lizenzmodus wird in den folgenden Abschnitten der **Administratorkonsole** verwendet: • Liste *Lizenz-Compliance*. Siehe Anzeigen von Informationen zur Lizenz-Compliance für Anwendungen im Softwarekatalog. • In der auf dem *Dashboard* angezeigten Lizenz-Compliance-Tabelle. Werte, die auf der Seite *Asset-Details* ignoriert wurden, werden mit einer Nutzung von 100 Prozent angezeigt. Siehe Informationen zu Dashboard-Widgets.

5. Klicken Sie auf **Weiter**.
6. Geben Sie auf der Seite *Lizenz-Asset-Details* auf der Registerkarte *Einkauf* die folgenden Informationen an:

Option	Beschreibung
Vertrag	Das mit der Lizenz verbundene Vertrags-Asset.
Gültig für katalogisierte Software	Anwendungen im Softwarekataloginventar, für das die Lizenz gilt. Gegebenenfalls können Sie Lizenz-Assets mehreren Anwendungen im Softwarekatalog zuordnen. Es ist jedoch nicht erforderlich, Lizenz-Assets mit mehreren Versionen der gleichen Anwendung zu verknüpfen, da die Appliance dies automatisch durchführt, um Upgrades und Downgrades zu unterstützen. Sie können einfach

Option	Beschreibung
	beim Hinzufügen der Lizenzinformationen die aktuelle Version dem Lizenz-Asset zuordnen. Wenn Sie Anwendungen von anderen Herausgebern, z. B. von Microsoft Office oder Adobe Acrobat, dem gleichen Lizenz-Asset zuweisen, wird jeder Anwendung die im Lizenz-Asset angegebene Gesamtzahl der Lizenzplätze zugewiesen. Wenn das Lizenz-Asset z. B. über 100 Lizenzplätze verfügt, werden sowohl Microsoft Office als auch Adobe Acrobat 100 Lizenzplätze zugewiesen.
Produktschlüssel	Den mit der Lizenz verbundenen Produktschlüssel. Sie können die Standardinformationen ändern und bearbeiten, die für jeden Lizenz-Asset-Typ erfasst werden können.
Kosten pro Einheit	Die mit der Lizenz verbundenen Einheitskosten. Sie können die Standardinformationen ändern und bearbeiten, die für jeden Lizenz-Asset-Typ erfasst werden können.
Hersteller	Der Name des Hersteller-Assets, das Sie mit der Anwendung verknüpfen möchten. Die Dropdown-Liste *Hersteller* ist leer, wenn Sie kein Hersteller-Asset hinzugefügt haben. Um nach einem Hersteller zu suchen, tippen Sie seinen Namen in die Liste. **HINWEIS:** Die Zuweisung mehrerer Hersteller zu einem einzigen Softwarelizenz-Asset wird nicht empfohlen, da dies zu fehlerhaften Lizenz-Compliance-Informationen führen kann.
Bestellnummer	Die mit der Lizenz verknüpfte Bestellnummer.
Kaufdatum	Das Datum des Kaufs. Klicken Sie in das Feld und wählen Sie dann im Kalender ein Datum aus.
Kauf	Wählen Sie einen oder mehrere mit dieser Lizenz verknüpfte Einkaufsdatensätze aus. Siehe Kaufdatensätze verwalten.

7. Klicken Sie auf **Weiter**.
8. Geben Sie auf der Seite *Lizenz-Asset-Details* auf der Registerkarte *Wartung* die folgenden Informationen an:

Option	Beschreibung
Schließt Upgrade-Rechte ein	Gibt an, ob die Lizenz Upgrade-Rechte einschließt. Upgrade-Rechte beziehen sich auf die Möglichkeit, auf eine neuere Version der lizenzierten Software aufzurüsten, wenn eine solche Version verfügbar wird. Weitere Informationen hierzu finden Sie unter

Option	Beschreibung
	Informationen zu Lizenz-Upgrades. Wählen Sie eine der folgenden Optionen aus: • **Ja**: Upgrade-Rechte werden durch Vergleich der bestehenden Lizenzen für die ausgewählte Software und die Anzahl verfügbarer Lizenzen für neuere Versionen der gleichen Software berechnet. • **Ja - aus Liste auswählen**: Wählen Sie eine oder mehrere Softwareversionen, für die Sie Upgrade-Rechte gewähren möchten. Klicken Sie unter *Software-Liste aktualisieren* auf **Katalogisierte Software zum Hinzufügen auswählen**. Die daraufhin angezeigte Liste wird mit höheren Versionen der ausgewählten Software ausgefüllt, auf die die Lizenz aktualisiert werden kann. Wenn Sie auf einen Eintrag in der Liste klicken, erscheint Ihre Auswahl im Feld *Liste der Upgrade-Software*. Sie können nach Bedarf eine oder mehrere Versionen hinzufügen. Um ein Element aus der Liste zu löschen, wählen Sie es im Feld *Liste der Upgrade-Software* aus und klicken Sie auf **Entfernen**. • **Nein**: Wenn Sie keine Upgrade-Rechte für die ausgewählte Software gewähren möchten, aktivieren Sie diese Option.
Service inklusive	Gibt an, ob die Lizenz die Benutzer zum Upgrade der installierten Version der Anwendung berechtigt. Siehe Informationen zur Lizenz-Compliance für Anwendungen im Softwarekatalog.
Ablaufdatum	Das Ablaufdatum des Wartungszeitraums, wenn die Lizenz Wartung beinhaltet. Die Lizenz-Compliance-Funktion der Appliance nutzt Softwarekataloginformationen, z. B. das Herausgabedatum von Anwendungen. Wenn während des Wartungszeitraums neue Anwendungsversionen herausgegeben werden, sind diese automatisch durch dieses Lizenz-Asset abgedeckt.
Schließt Downgrade-Rechte ein	Gibt an, ob die Lizenz Downgrade-Rechte einschließt. Downgrade-Rechte beziehen sich auf die Möglichkeit, Lizenzen für neuere Softwareversionen auf ältere Versionen der gleichen Software anzuwenden. Weitere Informationen hierzu finden Sie unter Informationen zu Lizenz-Downgrades. Wählen Sie eine der folgenden Optionen aus: • **Ja**: Downgrade-Rechte werden durch Vergleich der bestehenden Lizenzen für die ausgewählte Software und die Anzahl

Option	Beschreibung
	verfügbarer Lizenzen für ältere Versionen der gleichen Software berechnet. • **Ja - aus Liste auswählen**: Wählen Sie eine oder mehrere Softwareversionen, für die Sie Downgrade-Rechte gewähren möchten. Klicken Sie unter *Software-Liste zurückstufen* auf **Katalogisierte Software zum Hinzufügen auswählen**. Die daraufhin angezeigte Liste wird mit niedrigeren Versionen der ausgewählten Software ausgefüllt, auf die die Lizenz herabgestuft werden kann. Wenn Sie auf einen Eintrag in der Liste klicken, erscheint Ihre Auswahl im Feld *Liste der Downgrade-Software*. Sie können nach Bedarf eine oder mehrere Versionen hinzufügen. Um ein Element aus der Liste zu löschen, wählen Sie es im Feld *Liste der Downgrade-Software* aus und klicken Sie auf **Entfernen**. • **Nein**: Wenn Sie keine Downgrade-Rechte für die ausgewählte Software gewähren möchten, aktivieren Sie diese Option.

9. Klicken Sie auf **Weiter**.
10. Geben Sie auf der Seite *Lizenz-Asset-Details* auf der Registerkarte *Zugehörig* die folgenden Informationen an:

Option	Beschreibung
Abteilung	Die Unternehmensgruppe oder Abteilung, der diese Anwendung gehört.
Kostenstelle	Die mit der Abteilung, der diese Anwendung gehört, verknüpfte Kostenstelle.
Genehmigt für Gerät	Die Geräte, die die Lizenz verwenden dürfen. Diese Information wird für Lizenz-Compliance-Berichte verwendet. Wenn die Anwendung zum Beispiel auf Geräten installiert ist, die nicht in der Liste genehmigter Geräte enthalten sind, werden diese Geräte im Bericht *Nicht genehmigte Softwareinstallation* aufgeführt. Die Lizenz-Compliance wird von der Appliance jedoch nicht erzwungen. Sie verhindert beispielsweise nicht, dass Anwendungen auf verwalteten Geräten installiert werden, wenn eine Lizenz abgelaufen ist oder anderweitig gegen die Compliance-Vorgaben verstoßen wird.
Barcodes	Fügen Sie bei Bedarf Barcodes hinzu, die mit dieser Lizenz verknüpft sind, bzw. bearbeiten Sie diese.

Option	Beschreibung
	Weitere Informationen hierzu finden Sie unter Barcodes zu Assets hinzufügen.

11. Klicken Sie auf **Weiter**.
12. Geben Sie auf der Seite *Lizenz-Asset-Details* auf der Registerkarte *Benutzerdefiniert* zusätzliche benutzerdefinierte Daten an. Sie können den Lizenz-Asset-Typ ändern und so viele weitere Felder aufnehmen, wie für Ihre geschäftlichen Ziele notwendig sind. Weitere Informationen hierzu finden Sie unter Asset-Typen hinzufügen oder anpassen.
13. Klicken Sie auf **Weiter**.
14. Geben Sie auf der Seite *Lizenz-Asset-Details* auf der Registerkarte *Hinweise* die folgenden Informationen an:

Option	Beschreibung
Anmerkungen	Geben Sie nach Bedarf beliebige weitere Informationen ein.
Lizenztext	Ergänzende Informationen zur Lizenz, z. B. eine Lizenznummer.

15. Klicken Sie auf **Speichern**.

    Das neue Lizenz-Asset wird auf der Seite *Lizenzen* angezeigt. Der Wert von *Lizenzanzahl* ändert sich erst, wenn Sie das Asset aktualisieren. Dagegen ändert sich der Wert in der Spalte *Installiert*, sobald sich verwaltete Geräte, auf denen die Software installiert ist, bei der Appliance anmelden. Auf diese Weise können Sie die Anzahl der erworbenen und installierten Lizenzen verfolgen.

Führen Sie die folgenden optionalen Aufgaben aus:

- Aktivieren Sie die Nutzungserfassung für das Softwarekataloginventar. Wenn die Nutzungserfassung aktiviert ist, wird auf der Seite *Lizenz-Compliance* angezeigt, ob in den vergangenen 90 Tagen Anwendungen verwendet bzw. nicht verwendet worden sind. Siehe Informationen zur Erfassung der Softwarenutzung.
- Stellen Sie die Warnungsschwellenwerte für die Lizenznutzung ein. Diese Schwellenwerte werden vom Dashboard-Widget "Lizenz-Compliance" zur Erkennung von Lizenz-Compliance-Problemen genutzt.

Hinzufügen von Lizenz-Assets für das Inventar der Seite "Software"

Sie können Lizenz-Assets erstellen, um Informationen für Anwendungen zu verfolgen, die Lizenzen erfordern.

Bevor Sie Lizenz-Assets erstellen, sollten Ihnen Informationen wie die Anzahl der von der Lizenz abgedeckten Installationen (bzw. Lizenzplätze), der Produktschlüssel, die Bestellnummer und alle weiteren Informationen vorliegen, die Sie im Lizenz-Asset verwalten möchten.

HINWEIS: Um Lizenz-Assets für im Inventar der Seite *Software* enthaltene Anwendungen erstellen zu können, müssen Sie zunächst Software-Assets für diese Anwendungen erstellen. Für im Inventar der Seite *Softwarekatalog* enthaltene Anwendungen brauchen Sie keine Software-Assets zu erstellen.

Wenn auf der Appliance die Organisationskomponente aktiviert wurde, können Sie für jede Organisation Lizenz-Assets separat erstellen.

TIPP: Sie können Lizenz-Asset-Typen an Ihre Anforderungen anpassen. Siehe Anpassen des Lizenz-Asset-Typs.

1. Rufen Sie die Seite *Lizenz-Asset-Details* auf:

a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.

b. Führen Sie einen der folgenden Schritte aus:

- Klicken Sie in der linken Navigationsleiste auf **Lizenzen**. Wählen Sie **Aktion auswählen** > **Neu**.
- Klicken Sie in der linken Navigationsleiste auf **Inventar** und anschließend auf **Softwarekatalog**. Klicken Sie auf den Namen einer Anwendung. Klicken Sie auf der Seite *Softwarekatalogdetails* auf **Neue Lizenz hinzufügen**.

2. Geben Sie auf der Seite *Lizenz-Asset-Details* auf der Registerkarte *Allgemein* die folgenden Informationen an:

Option	Beschreibung
Untertyp	Der mit der Lizenz zu verknüpfende Asset-Untertyp. Siehe Informationen zu Asset-Untertypen, benutzerdefinierten Feldern und Gerätedetail-Voreinstellungen.
Asset-Status	Der Lizenzstatus, falls zutreffend. Sie können einen Standard-Asset-Status oder einen benutzerdefinierten festlegen (falls vorhanden). Eine Standardinstallation des Appliance umfasst die folgenden Asset-Status: • **Aktiv**: Alle Assets, die bereitgestellt, aktiv oder in Gebrauch sind. • **Entsorgt**: Ein Asset, das nicht mehr verfügbar ist. • **Abgelaufen** Ein Software-Lizenz oder ein Vertrags-Asset, das abgelaufen ist. • **Auf Lager**: Ein vor kurzem empfangenes Asset. • **Fehlt** Alle Assets, die nicht gefunden werden können. • **Reparieren** Ein Asset, das repariert wird. • **Reserviert** Ein Asset, das für eine bestimmte Person oder einen Zweck reserviert ist. • **außer Kraft gesetzt**: Alle Assets, die das Ende ihrer Lebensdauer erreicht haben oder nicht mehr in Gebrauch sind. • **Gestohlen**: Ein Asset, das als gestohlen gemeldet wurde. Weitere Informationen hierzu finden Sie unter Asset-Lebenszyklus-Einstellungen anzeigen und konfigurieren.
Standort	Der Name des Standorts, in dem sich die Organisation befindet. Siehe Standorte verwalten.

Option	Beschreibung
Name	Name der Lizenz, beispielsweise **Office Professional Bestellnr. 1234**. Dies ist der Name, über den Sie nach dem Asset suchen. Wenn Sie mehrere Lizenzen mit einer Anwendung verknüpfen möchten, geben Sie die Bestellnummer oder das Kaufdatum in die nachstehenden Felder ein, um die Lizenzen voneinander zu unterscheiden.
Lizenzanzahl	Die Anzahl der Installationen oder Arbeitsplätze, die gemäß der Lizenz zulässig sind. Beispiel: 50.
Gültig für katalogisierte Software	Anwendungen im Softwarekataloginventar, für das die Lizenz gilt. Gegebenenfalls können Sie Lizenz-Assets mehreren Anwendungen im Softwarekatalog zuordnen. Es ist jedoch nicht erforderlich, Lizenz-Assets mit mehreren Versionen der gleichen Anwendung zu verknüpfen, da die Appliance dies automatisch durchführt, um Upgrades und Downgrades zu unterstützen. Sie können einfach beim Hinzufügen der Lizenzinformationen die aktuelle Version dem Lizenz-Asset zuordnen. Wenn Sie Anwendungen von anderen Herausgebern, z. B. von Microsoft Office oder Adobe Acrobat, dem gleichen Lizenz-Asset zuweisen, wird jeder Anwendung die im Lizenz-Asset angegebene Gesamtzahl der Lizenzplätze zugewiesen. Wenn das Lizenz-Asset z. B. über 100 Lizenzplätze verfügt, werden sowohl Microsoft Office als auch Adobe Acrobat 100 Lizenzplätze zugewiesen.
Gültig für Software	Lassen Sie dieses Feld leer. Eine Lizenz kann jedoch nicht gleichzeitig mit im Inventar der Seite *Softwarekatalog* und der Seite *Software* enthaltenen Anwendungen verknüpft werden. Weitere Informationen zum Erstellen von Lizenz-Assets finden Sie unter Hinzufügen von Lizenz-Assets für das Inventar der Seite "Software".
Lizenzmodus	Der Modus des Lizenz-Assets. Für Anwendungen, die Lizenzen erfordern, und zum Anzeigen von Lizenznutzungsinformationen auf der Seite *Lizenz-Compliance* wählen Sie entweder *Unternehmen* oder *Lizenz für Einheit* aus. **HINWEIS:** Die meisten Modi, einschließlich *Nicht angegeben*, *Client-Lizenz*, *Abonnement*, *Shareware*, *Freeware*, *OpenSource*, *Keine Lizenzierung* und *Standortlizenz*, werden nicht für die Lizenz-Compliance verwendet.

Option	Beschreibung
	Der Lizenzmodus wird in den folgenden Abschnitten der **Administratorkonsole** verwendet: • Liste *Lizenz-Compliance*. Siehe Anzeigen von Informationen zur Lizenz-Compliance für Anwendungen im Softwarekatalog. • In der auf dem *Dashboard* angezeigten Lizenz-Compliance-Tabelle. Werte, die auf der Seite *Asset-Details* ignoriert wurden, werden mit einer Nutzung von 100 Prozent angezeigt. Siehe Informationen zu Dashboard-Widgets.

3. Klicken Sie auf **Weiter**.
4. Geben Sie auf der Seite *Lizenz-Asset-Details* auf der Registerkarte *Einkauf* die folgenden Informationen an:

Option	Beschreibung
Vertrag	Das mit der Lizenz verbundene Vertrags-Asset.
Gültig für katalogisierte Software	Anwendungen im Softwarekataloginventar, für das die Lizenz gilt. Gegebenenfalls können Sie Lizenz-Assets mehreren Anwendungen im Softwarekatalog zuordnen. Es ist jedoch nicht erforderlich, Lizenz-Assets mit mehreren Versionen der gleichen Anwendung zu verknüpfen, da die Appliance dies automatisch durchführt, um Upgrades und Downgrades zu unterstützen. Sie können einfach beim Hinzufügen der Lizenzinformationen die aktuelle Version dem Lizenz-Asset zuordnen. Wenn Sie Anwendungen von anderen Herausgebern, z. B. von Microsoft Office oder Adobe Acrobat, dem gleichen Lizenz-Asset zuweisen, wird jeder Anwendung die im Lizenz-Asset angegebene Gesamtzahl der Lizenzplätze zugewiesen. Wenn das Lizenz-Asset z. B. über 100 Lizenzplätze verfügt, werden sowohl Microsoft Office als auch Adobe Acrobat 100 Lizenzplätze zugewiesen.
Produktschlüssel	Den mit der Lizenz verbundenen Produktschlüssel. Sie können die Standardinformationen ändern und bearbeiten, die für jeden Lizenz-Asset-Typ erfasst werden können.
Kosten pro Einheit	Die mit der Lizenz verbundenen Einheitskosten. Sie können die Standardinformationen ändern und bearbeiten, die für jeden Lizenz-Asset-Typ erfasst werden können.
Hersteller	Der Name des Hersteller-Assets, das Sie mit der Anwendung verknüpfen möchten. Die Dropdown-Liste *Hersteller* ist leer, wenn Sie kein Hersteller-

Option	Beschreibung
	Asset hinzugefügt haben. Um nach einem Hersteller zu suchen, tippen Sie seinen Namen in die Liste. **HINWEIS:** Die Zuweisung mehrerer Hersteller zu einem einzigen Softwarelizenz-Asset wird nicht empfohlen, da dies zu fehlerhaften Lizenz-Compliance-Informationen führen kann.
Bestellnummer	Die mit der Lizenz verknüpfte Bestellnummer.
Kaufdatum	Das Datum des Kaufs. Klicken Sie in das Feld und wählen Sie dann im Kalender ein Datum aus.
Kauf	Wählen Sie einen oder mehrere mit dieser Lizenz verknüpfte Einkaufsdatensätze aus. Siehe Kaufdatensätze verwalten.

5. Klicken Sie auf **Weiter**.
6. Geben Sie auf der Seite *Lizenz-Asset-Details* auf der Registerkarte *Wartung* die folgenden Informationen an:

Option	Beschreibung
Schließt Upgrade-Rechte ein	Gibt an, ob die Lizenz Upgrade-Rechte einschließt. Upgrade-Rechte beziehen sich auf die Möglichkeit, auf eine neuere Version der lizenzierten Software aufzurüsten, wenn eine solche Version verfügbar wird. Weitere Informationen hierzu finden Sie unter Informationen zu Lizenz-Upgrades. Wählen Sie eine der folgenden Optionen aus: • **Ja**: Upgrade-Rechte werden durch Vergleich der bestehenden Lizenzen für die ausgewählte Software und die Anzahl verfügbarer Lizenzen für neuere Versionen der gleichen Software berechnet. • **Ja - aus Liste auswählen**: Wählen Sie eine oder mehrere Softwareversionen, für die Sie Upgrade-Rechte gewähren möchten. Klicken Sie unter *Software-Liste aktualisieren* auf **Katalogisierte Software zum Hinzufügen auswählen**. Die daraufhin angezeigte Liste wird mit höheren Versionen der ausgewählten Software ausgefüllt, auf die die Lizenz aktualisiert werden kann. Wenn Sie auf einen Eintrag in der Liste klicken, erscheint Ihre Auswahl im Feld *Liste der Upgrade-Software*. Sie können nach Bedarf eine oder mehrere Versionen hinzufügen. Um ein Element aus der Liste zu löschen, wählen Sie es im Feld *Liste der Upgrade-Software* aus und klicken Sie auf **Entfernen**. • **Nein**: Wenn Sie keine Upgrade-Rechte für die ausgewählte Software gewähren möchten, aktivieren Sie diese Option.

Option	Beschreibung
Service inklusive	Gibt an, ob die Lizenz die Benutzer zum Upgrade der installierten Version der Anwendung berechtigt. Siehe Informationen zur Lizenz-Compliance für Anwendungen im Softwarekatalog.
Ablaufdatum	Das Ablaufdatum des Wartungszeitraums, wenn die Lizenz Wartung beinhaltet. Die Lizenz-Compliance-Funktion der Appliance nutzt Softwarekataloginformationen, z. B. das Herausgabedatum von Anwendungen. Wenn während des Wartungszeitraums neue Anwendungsversionen herausgegeben werden, sind diese automatisch durch dieses Lizenz-Asset abgedeckt.
Schließt Downgrade-Rechte ein	Gibt an, ob die Lizenz Downgrade-Rechte einschließt. Downgrade-Rechte beziehen sich auf die Möglichkeit, Lizenzen für neuere Softwareversionen auf ältere Versionen der gleichen Software anzuwenden. Weitere Informationen hierzu finden Sie unter Informationen zu Lizenz-Downgrades. Wählen Sie eine der folgenden Optionen aus: • **Ja**: Downgrade-Rechte werden durch Vergleich der bestehenden Lizenzen für die ausgewählte Software und die Anzahl verfügbarer Lizenzen für ältere Versionen der gleichen Software berechnet. • **Ja - aus Liste auswählen**: Wählen Sie eine oder mehrere Softwareversionen, für die Sie Downgrade-Rechte gewähren möchten. Klicken Sie unter *Software-Liste zurückstufen* auf **Katalogisierte Software zum Hinzufügen auswählen**. Die daraufhin angezeigte Liste wird mit niedrigeren Versionen der ausgewählten Software ausgefüllt, auf die die Lizenz herabgestuft werden kann. Wenn Sie auf einen Eintrag in der Liste klicken, erscheint Ihre Auswahl im Feld *Liste der Downgrade-Software*. Sie können nach Bedarf eine oder mehrere Versionen hinzufügen. Um ein Element aus der Liste zu löschen, wählen Sie es im Feld *Liste der Downgrade-Software* aus und klicken Sie auf **Entfernen**. • **Nein**: Wenn Sie keine Downgrade-Rechte für die ausgewählte Software gewähren möchten, aktivieren Sie diese Option.

7. Klicken Sie auf **Weiter**.
8. Geben Sie auf der Seite *Lizenz-Asset-Details* auf der Registerkarte *Zugehörig* die folgenden Informationen an:

Option	Beschreibung
Abteilung	Die Unternehmensgruppe oder Abteilung, der diese Anwendung gehört.
Kostenstelle	Die mit der Abteilung, der diese Anwendung gehört, verknüpfte Kostenstelle.
Genehmigt für Gerät	Die Geräte, die die Lizenz verwenden dürfen. Diese Information wird für Lizenz-Compliance-Berichte verwendet. Wenn die Anwendung zum Beispiel auf Geräten installiert ist, die nicht in der Liste genehmigter Geräte enthalten sind, werden diese Geräte im Bericht *Nicht genehmigte Softwareinstallation* aufgeführt. Die Lizenz-Compliance wird von der Appliance jedoch nicht erzwungen. Sie verhindert beispielsweise nicht, dass Anwendungen auf verwalteten Geräten installiert werden, wenn eine Lizenz abgelaufen ist oder anderweitig gegen die Compliance-Vorgaben verstoßen wird.
Barcodes	Fügen Sie bei Bedarf Barcodes hinzu, die mit dieser Lizenz verknüpft sind, bzw. bearbeiten Sie diese. Weitere Informationen hierzu finden Sie unter Barcodes zu Assets hinzufügen.

9. Klicken Sie auf **Weiter**.
10. Geben Sie auf der Seite *Lizenz-Asset-Details* auf der Registerkarte *Benutzerdefiniert* zusätzliche benutzerdefinierte Daten an. Sie können den Lizenz-Asset-Typ ändern und so viele weitere Felder aufnehmen, wie für Ihre geschäftlichen Ziele notwendig sind. Weitere Informationen hierzu finden Sie unter Asset-Typen hinzufügen oder anpassen.
11. Klicken Sie auf **Weiter**.
12. Geben Sie auf der Seite *Lizenz-Asset-Details* auf der Registerkarte *Hinweise* die folgenden Informationen an:

Option	Beschreibung
Anmerkungen	Geben Sie nach Bedarf beliebige weitere Informationen ein.
Lizenztext	Ergänzende Informationen zur Lizenz, z. B. eine Lizenznummer.

13. Klicken Sie auf **Speichern**.

Das neue Lizenz-Asset wird auf der Seite *Lizenzen* angezeigt. Der Wert von *Lizenzanzahl* ändert sich erst, wenn Sie das Asset aktualisieren. Dagegen ändert sich der Wert in der Spalte *Installiert*, sobald sich verwaltete Geräte, auf denen die Software installiert ist, bei der Appliance anmelden. Auf diese Weise können Sie die Anzahl der erworbenen und installierten Lizenzen verfolgen.

Verwandte Themen

Anpassen des Lizenz-Asset-Typs

Anzeigen von Informationen zur Lizenz-Compliance und -Konfiguration

Informationen zu Berichten

Importieren von Lizenzdaten in CSV-Dateien

Wenn Ihre Lizenzdaten in einer Tabelle erfasst sind, können Sie sie in das CSV-Format (durch Komma getrennte Werte) exportieren und anschließend in die Appliance importieren. Alternativ können Sie mit einem Text-Editor eine CSV-Datei erstellen, die die Daten enthält, und anschließend diese Datei importieren.

Falls die CSV-Datei neue Assets für von Ihnen definierte Asset-Typen enthält, werden die neuen Assets hinzugefügt.

Behandlung von Asset-Informationen während des Imports

Beim Importieren von Asset-Informationen vergleicht die Appliance die neuen Informationen mit vorhandenen Informationen, um zu ermitteln, wie die neuen Informationen behandelt werden soll.

Abhängig davon, ob die Informationen neu, vorhanden oder doppelt sind, führt die Appliance die folgenden Schritte aus:

- **Erstellung des Assets**: Wenn der Wert des primären Schlüssels keinem vorhandenen Wert entspricht, wird das Asset erstellt.
- **Aktualisierung des Assets**: Wenn der Wert des primären Schlüssels einem vorhandenen Wert entspricht, werden die Asset-Informationen aktualisiert.
- **Kennzeichnung des Assets als Duplikat**: Wenn mehrere Datensätze für den Asset-Typ dem Wert des als primärer Schlüssel gewählten CSV-Felds entsprechen ODER wenn mehrere Datensätze dem zugehörigen Asset entsprechen, wird das Asset als Duplikat gekennzeichnet. Doppelte Datensätze werden nicht importiert.

Asset-Daten mithilfe von CSV-Dateien importieren

Sie können Asset-Daten wie Software-Lizenzdaten mithilfe von CSV-Dateien (Comma Separated Value, durch Trennzeichen getrennte Werte) importieren.

Asset-Daten vor dem Import vorbereiten

Stellen Sie sicher, dass Asset-Daten vor dem Import ordnungsgemäß vorbereitet und formatiert wurden.

1. Legen Sie die grundlegenden Felder für Ihre Assets fest. Wenn Sie Produktnamen verwenden, wählen Sie diese so, dass das Asset einfach identifiziert werden kann. Siehe Software-Assets hinzufügen.
2. Fügen Sie Überschriftenzeilen zu Ihren Daten hinzu. In der Komponente "Asset Management" wird für Verweise auf Spalten ohne Überschriften deren Spaltennummer verwendet. Bei einer Spaltenüberschriftenzeile lassen sich Daten daher leichter identifizieren.
3. Überprüfen Sie, ob alle Spalten die *Asset-Felder* im Asset-Typ widerspiegeln.

   Asset-Typen sind z. B. Standardfelder wie *Asset-Name*, *Bestellnummer* oder *Anbieter*. Sie können Asset-Felder aber auch bei Bedarf anpassen. Siehe Informationen zum Hinzufügen und Löschen von Asset-Feldern.

   TIPP: Rufen Sie die Seite *Asset-Details* auf, um die Standardfelder anzuzeigen. Siehe Asset-Typen anpassen.

4. Entscheiden Sie, welche Felder Sie als primärer Schlüssel (PS) für die importierten Assets verwenden möchten.

   Bei primären Schlüsseln handelt es sich um Felder oder eine Kombination von Feldern, die als zuverlässige eindeutige Bezeichner für importierte Assets dienen. Beim Importieren von Assets kann die Appliance kann anhand von primären Schlüsseln ermitteln, ob ein vorhandener Datensatz aktualisiert

oder ein neuer Datensatz erstellt werden soll. Sie können ein Feld oder eine Kombination von Feldern als primären Schlüssel auswählen.

5. Speichern Sie die Tabellenkalkulation als CSV-Datei an einem Speicherort, auf den Sie mit der Administratorkonsole zugreifen können.

Beispiel: Lizenzdaten aus vorbereiteten Tabellen importieren

Sie können Lizenzdaten aus vorbereiteten CSV-Dateien importieren.

In diesem Beispiel wird beschrieben, wie Sie Lizenzbestände für die Softwarekatalog-Bestandsaufnahme importieren, entweder als einmaligen Import oder als geplanten Import, der eine Datei aus einer Netzwerkfreigabe verwendet. Das Beispiel zeigt nur die Felder, die zum Importieren des Lizenz-Assets erforderlich sind. Sie können passend zu Ihren Verwaltungsanforderungen weitere Dateien mit Informationen wie Stückpreise, Publisher, Produktschlüssel usw. hinzufügen.

Wenn Sie die importierten Assets einem Asset-Untertyp zuweisen wollen, fügen Sie den Untertyp vor dem Importieren der Assets hinzu. Siehe Asset-Untertypen hinzufügen und Voreinstellungen für die Seite "Gerätedetail" auswählen.

1. Erstellen Sie eine Datei in einem Tabellenkalkulationsprogramm wie Excel.
2. Fügen Sie die folgenden Zeilen und Spalten hinzu. Die erste Zeile enthält die Überschriften:

Asset-Name	Lizenzanzahl	Lizenzmodus	Service inklusive	Anwenden auf den Softwarekatalog
Softwaretitel 1	100	Unternehmen	Ja	Softwaretitel 1
Softwaretitel 2	150	Unternehmen	Ja	Softwaretitel 2
Softwaretitel 3	200	Unternehmen	Ja	Softwaretitel 3
Softwaretitel 4	500	Unternehmen	Ja	Softwaretitel 4

3. Speichern Sie die Datei im CSV-Format.

   Die Werte in jeder Spalte werden durch Kommas getrennt. Beispiel: `Software Title 1,100,Unternehmen,Ja,Softwaretitel 1`
4. Rufen Sie die Seite *Datei hochladen* im Abschnitt *Assets importieren* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Asset Management** und anschließend auf **Assets importieren**.

   - Wenn ein oder mehrere Asset-Importvorgänge geplant sind, wird die Seite „Asset-Liste importieren“ mit einer Liste der Importvorgänge angezeigt. Um Assets aus einer CSV-Datei zu importieren, klicken Sie auf **Aktion auswählen** > **Neu**, um den Assistenten *Assets importieren* zu starten.
   - Wenn keine geplanten Asset-Importe auf der Appliance vorhanden sind, wird der Assistent *Assets importieren* angezeigt.
5. Wählen Sie im Assistenten *Assets importieren* eine der folgenden Optionen aus:

Option	Beschreibung
Eine Asset-Import-Datei im CSV-Format hochladen	Wählen Sie diese Option aus, um einen einmaligen Asset-Import aus einer CSV-Datei durchzuführen.

Option	Beschreibung
	Klicken Sie dann auf **Durchsuchen** oder **Datei auswählen** und wählen Sie die CSV-Datei aus.
Asset-Import planen	Wählen Sie diese Option aus, um in ausgewählten Zeitintervallen mehrere Assets aus einer CSV-Datei auf einem Netzlaufwerk zu importieren. Geben Sie dann die folgenden Informationen an: • **Dateiübertragungsprotokoll für Asset-Import auswählen**: ◦ **Samba**: Wählen Sie diese Option aus, um über das Samba-Protokoll auf die Datei zuzugreifen, und geben Sie die folgenden Informationen an: ▪ **Geben Sie den UNC-Pfad zur Samba-Freigabe ein**: Geben Sie den Verzeichnispfad zur CSV-Datei ein. ◦ **FTP**: Wählen Sie diese Option aus, um auf die Datei auf einem FTP-Server zuzugreifen, und geben Sie die folgenden Informationen an: ▪ **Geben Sie den Hostnamen oder die IP-Adresse des FTP-Servers ein**: Geben Sie den Hostnamen oder die IP-Adresse des FTP-Servers ein. ▪ **Geben Sie das FTP-Unterverzeichnis ein, falls vorhanden**: Geben Sie den Verzeichnispfad zur CSV-Datei auf dem FTP-Server ein. ◦ **Sicherer FTP**: Wählen Sie diese Option aus, um auf die Datei auf einem sicheren FTP-Server zuzugreifen, und geben Sie die folgenden Informationen an: ▪ **Geben Sie den Hostnamen oder die IP-Adresse des sicheren FTP-Servers ein**: Geben Sie den Hostnamen oder die IP-Adresse des sicheren FTP-Servers ein. ▪ **Geben Sie den vollständigen SFTP-Pfad ein**: Geben Sie den Verzeichnispfad zur CSV-Datei auf dem sicheren FTP-Server ein. • **CSV-Dateiname für Asset-Import**: Geben Sie den Namen der CSV-Datei ein, die Sie importieren möchten. • **Anmeldeinformationen**: Wählen Sie die Zugangsdaten aus, die Sie für den Zugriff auf die angegebene Netzwerkressource verwenden möchten. Alle in der Appliance

Option	Beschreibung
	definierten Anmeldedaten werden in der Liste angezeigt. Weitere Informationen hierzu finden Sie unter Verwalten von Anmeldeinformationen.

6. Falls die CSV-Datei wie in diesem Beispiel eine Überschriftenzeile enthält, aktivieren Sie das Kontrollkästchen *Kopfzeile der Datei* und klicken Sie auf **Weiter**.
7. **Nur geplante Asset-Importe**. Erstellen Sie auf der angezeigten Seite *Zeitplan für Asset-Importauswahl* einen Zeitplan für den Import der CSV-Datei.
   a. Geben Sie im Feld *Name des Asset-Importplans* den Namen ein, den Sie diesem Zeitplan zuweisen möchten.
   b. Wählen Sie **Asset-Zeitplan aktivieren** aus.
   c. Geben Sie im Abschnitt *Zeitplan* den gewünschten Importzeitplan an.

Option	Beschreibung
Kein(e)	Die Ausführung erfolgt im Zusammenhang mit einem Ereignis anstatt zu einem bestimmten Datum oder zu einem bestimmten Zeitpunkt.
jede Stunde	Der Vorgang wird im angegebenen Intervall durchgeführt.
Täglich/an einem bestimmten Tag um HH:MM	Die Erfassung wird täglich zu einem bestimmten Zeitpunkt oder an einem bestimmten Wochentag um eine bestimmte Uhrzeit ausgeführt.
Ausführen am n-ten jedes Monats/eines bestimmten Monats um HH:MM	Die Erfassung wird jeden Monat oder in einem bestimmten Monat an einem festgelegten Datum zu einer festgelegten Uhrzeit ausgeführt.
Ausführen am n-ten Wochentag **jedes Monats/ eines bestimmten Monats um HH:MM**	Die Erfassung wird jeden Monat oder in einem bestimmten Monat an einem festgelegten Wochentag zu einer festgelegten Uhrzeit ausgeführt.

Benutzerdefiniert	Führen Sie die Erfassung nach einem benutzerdefinierten Zeitplan aus.
	Verwenden Sie das Standard-5-Feld-Cron-Format (das erweiterte Cron-Format wird nicht unterstützt):
	`* * * * *`
	`| | | | +————Wochentag (0-6) (Sonntag=0)`
	`| | | +————Monat (1-12)`
	`| | +————Monatstag (1-31)`
	`| +————Stunde (0-23)`
	`+————Minute (0-59)`
	Verwenden Sie bei der Angabe von Werten die folgenden Zeichen:
	• **Leerzeichen( )**: Die einzelnen Felder mit einem Leerzeichen trennen.
	• **Sternchen (*)**: Ein Sternchen repräsentiert den gesamten Wertebereich in einem Feld.

Option	Beschreibung
	Zum Beispiel repräsentiert ein Sternchen im Stundenfeld eine beliebige Stunde. • **Kommas (,)**: Mehrere Werte in einem Feld werden mit einem Komma getrennt. Zum Beispiel werden mit `0,6` im Feld „Wochentag“ Sonntag und Samstag angegeben. • **Bindestriche (-)**: Mit einem Bindestrich wird ein Wertebereich in einem Feld angegeben. Zum Beispiel entspricht `1-5` im Feld „Wochentag“ `1,2,3,4,5`, d. h. Montag bis Freitag. • **Schrägstriche (/)**: Die Angabe der Zeitabstände, mit denen eine Aktion wiederholt werden soll, erfolgt mit einem Schrägstrich. Zum Beispiel entspricht `*/3` im Feld Stunde `0,3,6,9,12,15,18,21`. Das Sternchen (`*`) gibt jede Stunde an, mit `/3` erfolgt aber eine Einschränkung auf durch drei teilbare Stunden. Beispiele: • `15 * * * * Jeden Tag 15 Minuten nach jeder vollen Stunde ausführen` • `0 22 * * * Jeden Tag um 22:00 Uhr ausführen` • `0 0 1 1,6 * Am 1. Januar und 1. Juni um 00:00 Uhr ausführen` • `30 8,12 * * 1-5 An Wochentagen um 08:30 Uhr und 12:30 Uhr ausführen` • `0 2 */2 * * Jeden zweiten Tag um 02:00 Uhr ausführen`

8. Führen Sie auf der angezeigten Seite *Asset-Typauswahl* die folgenden Schritte aus:
   a. Wählen Sie aus der Dropdown-Liste *Asset-Typ* die Option **Lizenz** aus.
   b. Wählen Sie in der Dropdown-Liste *Asset-Untertyp* die Option **Produktivität** aus.

   HINWEIS: In diesem Beispiel wurde der Asset-Untertyp *Produktivität* zum Lizenz-Asset-Typ hinzugefügt. Die Dropdown-Liste *Untertyp* ist leer, wenn Sie keine Untertypen für den Lizenz-Asset-Typ hinzugefügt haben. Beim Importieren werden die ausgewählten Assets dem ausgewählten Untertyp zugewiesen.

   c. Klicken Sie auf **Weiter**.

   Die Seite *Zuordnung* wird angezeigt.
9. In der Dropdown-Liste *CSV-Felder* wählen Sie die Felder aus, die den Appliance-Feldern *Erforderliche Standardfelder* und *Erforderliche Asset-Felder* entsprechen. Die Zuweisung der Felder hängt vom Inhalt der CSV-Datei und vom Asset-Typ ab. Für das Beispiel in diesem Abschnitt verwenden Sie folgende Werte:
   - *Asset-Name*=**Name**
   - *Standort*=**Standort**
   - *Asset-Status*=**Asset-Status**

HINWEIS: Wenn Sie diese Zuordnung nicht angeben, wird jedem importierten Asset-Eintrag der Standardstatus zugewiesen, der mit dem ausgewählten Asset-Typ verknüpft ist.

- *Lizenzanzahl*=**Lizenzanzahl**
- *Gültig für katalogisierte Software*=**Softwarekatalog**
- *Lizenzmodus*=**Modus**

HINWEIS: Sie können nur dann Werte für den Asset-Bevollmächtigten importieren, wenn es sich bei dem importierten Asset um ein Gerät handelt.

10. Aktivieren Sie das Kontrollkästchen **PK** neben dem Feld *Asset-Name*.

HINWEIS: Bei primären Schlüsseln handelt es sich um Felder oder eine Kombination von Feldern, die als zuverlässige eindeutige Bezeichner für importierte Assets dienen. Beim Importieren von Assets kann die Appliance kann anhand von primären Schlüsseln ermitteln, ob ein vorhandener Datensatz aktualisiert oder ein neuer Datensatz erstellt werden soll. Sie können ein Feld oder eine Kombination von Feldern als primären Schlüssel auswählen.

11. Wenn die Assets, die Sie importieren Barcodes verwenden geben Sie im Bereich *Barcodefelder* an, wie Sie die Barcodes importieren möchten.

Option	Beschreibung
Asset-Barcodes mit ausgewählten aktualisieren	Überprüfen Sie, ob die Barcodes in diesem Bereich bereits vorhanden sind, wenn ja, aktualisieren Sie diese. Wenn sie nicht vorhanden sind, werden sie für die angegebenen Assets erstellt.
Alle Asset-Barcodes durch ausgewählte ersetzen	Ersetzen Sie die vorhandenen Barcodes mit den angegebenen Barcodes.
Barcodedaten	Das Feld in der CSV-Datei, das den Barcode enthält. Es kann jeweils nur einen Barcode gleichen Typs pro Asset geben.
Barcodename	Das Feld in der CSV-Datei, das den Barcode-Tag enthält. Barcode-Nummern sind immer eindeutig, sie können nicht von mehreren Assets gemeinsam genutzt werden. Es ist jedoch für ein aktives Asset möglich, einen Barcode mit einem archivierten Asset gemeinsam zu nutzen.
Barcodeformat	Das Feld in der CSV-Datei, das das Barcode-Format enthält. Beispielsweise UPC-A, Code 11 oder UPC-E.

12. Klicken Sie auf **Vorschau**, um die Daten auf der Seite *Bestätigung* zu überprüfen.
13. **Nur einmalige Importe**. Führen Sie folgende Schritte durch.
    a. Klicken Sie auf **Importieren**, um den Importvorgang abzuschließen.

       Die Seite *Ergebnis für Asset-Import* wird angezeigt.

    b. Klicken Sie auf **Fertig**, um zur Seite *Assets*zurückzukehren.
14. **Nur geplante Importe**. Führen Sie einen der folgenden Schritte aus:
    - Klicken Sie auf **Speichern**, um den neu erstellten geplanten Import zu speichern. Die Listenseite *Assets importieren* wird geöffnet und zeigt den geplanten Importeintrag in der Liste an.
    - Klicken Sie auf **Jetzt ausführen**, um Assets aus der CSV-Datei zu importieren und die geplanten Importeinstellungen zu speichern.

Die Listenseite *Assets importieren* wird angezeigt.

Wenn der Importvorgang abgeschlossen ist, werden die Assets in der Liste *Assets* angezeigt. Stimmten die Titel der Software mit Titeln im Softwarekatalog-Inventar überein, werden die Assets den Inventarelementen zugeordnet. Sie können diese auf der Seite *Softwarekatalogdetails* anzeigen.

Verwalten der Lizenz-Compliance

Sie können die Anzahl der erworbenen Software-Lizenzen, die Anzahl der auf verwalteten Geräten verwendeten Lizenzen und die Anzahl der verfügbaren Lizenzen nachverfolgen. Diese Art der Verfolgung hilft Ihnen dabei, sicherzustellen, dass Ihr Unternehmen die Softwarelizenz-Anforderungen erfüllt.

Wenn Sie beispielsweise 100 Lizenzen für Adobe® Creative Suite besitzen, möchten Sie möglicherweise wissen, wie viele dieser Lizenzen wirklich auf verwalteten Geräten genutzt werden. Außerdem möchten Sie vielleicht wissen, wann 80 oder 90 Prozent dieser Lizenzen genutzt werden, damit Sie nötigenfalls die Lizenzkapazität erhöhen können. Sie können die Warnungsschwellenwerte für die Lizenznutzung anpassen, um die Lizenz-Compliance zu verfolgen.

Anzeigen von Informationen zur Lizenz-Compliance für Anwendungen im Softwarekatalog

Um sicherzustellen, dass Ihre Organisation die richtigen Lizenzen für installierte Software besitzt, können Sie die Lizenz-Compliance-Informationen in der Liste *Lizenz-Compliance* und im Dashboard-Widget zur Lizenz-Compliance anzeigen. Die Liste *Lizenz-Compliance* enthält alle Software-Lizenzinformationen, die Sie mit Lizenz-Assets hinzugefügt haben, sowie Informationen aus dem Softwarekatalog über Anwendungen, die Lizenzen erfordern.

- Auf den agentenverwalteten Geräten im Inventar Ihrer Appliance laufen Softwareanwendungen, die im Softwarekatalog verfügbar sind.
- Sie haben die Anzahl der verfügbaren Arbeitsplätze für installierte Softwarekatalog-Anwendungen als Lizenz-Assets und den Lizenzmodus angegeben. Siehe Hinzufügen von Lizenz-Assets für das Inventar der Seite "Software".
- Sie haben Warnungsschwellwerte für die Lizenznutzung in den allgemeinen Einstellungen der Appliance oder Organisation eingerichtet. Siehe Allgemeine Einstellungen auf Verwaltungs- oder organisationsspezifischer Ebene konfigurieren.

1. Die vollständigen Lizenz-Compliance-Informationen finden Sie auf der Seite *Lizenz-Compliance*:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Asset Management** und anschließend auf **Lizenz-Compliance**.

HINWEIS: Die Informationen auf der Liste *Lizenz-Compliance* werden jeden Tag nach dem täglichen Sicherungsvorgang der Appliance aktualisiert. Wenn die Liste leer ist, sind entweder keine erkannten Anwendungen im Inventar des Softwarekatalogs vorhanden oder die Informationen auf der Seite wurden nicht aktualisiert. Sind zudem alle Differenzen negative Zahlen, bedeutet das, dass es mehr Installationen als Lizenzplätze gibt. Überprüfen Sie dann, ob Sie Lizenz-Assets für die Anwendungen hinzugefügt haben. Siehe Hinzufügen von Lizenz-Assets für das Softwarekataloginventar.

2. Um die Appliance zum Aktualisieren der Lizenz-Compliance-Informationen zu zwingen, klicken Sie links über der Liste auf *Jetzt aktualisieren*. Je nach Anzahl der Anwendungen im Inventar kann dieser Prozess einige Minuten dauern.

   TIPP: Wenn Sie auf **Jetzt aktualisieren** klicken, aktualisiert die Appliance die Daten jedes Elements in der Liste. Wenn Sie jedoch rechts über der Liste auf **Aktualisieren** klicken, werden von der Appliance nur die bereits erfassten Informationen angezeigt. Neue Informationen zur Lizenznutzung werden dabei nicht berücksichtigt.

   Auf der Seite *Lizenz-Compliance* finden Sie Informationen wie:

Spaltenname	Beschreibung
Name	Der Name der Anwendung
Herausgeber	Der Name des Herausgebers der Anwendung
Installiert	Die Anzahl der Anwendungsinstallationen auf agentenverwalteten Geräten
Lizenziert	Die Anzahl der Lizenzplätze, die für die Lizenz verbleiben
Differenz	Die Differenz zwischen der Anzahl der verfügbaren Lizenzplätze und der Anzahl der Anwendungsinstallationen (falls vorhanden). Eine negative Zahl bedeutet, dass die Anwendung auf mehr Geräten als nach der Lizenz zulässig installiert wurde, was gegen die Compliance-Vorgaben verstößt.
In den letzten 90 Tagen verwendet **In den letzten 60 Tagen verwendet** **In den letzten 30 Tagen verwendet**	Die Anzahl der Anwendungsinstallationen, die in den letzten 90, 60 oder 30 Tagen gestartet wurden. Ein Strich in dieser Spalte bedeutet, dass die Erfassung nicht für die Anwendung aktiviert ist. **HINWEIS:** Um korrekte Erfassungsinformationen zu erhalten, müssen Sie zunächst die Erfassung für die Anwendung und für die Geräte aktivieren, auf denen die Anwendung installiert ist. Siehe Erfassung von Geräten und Anwendungen aktivieren und konfigurieren.
Nicht in den letzten 90 Tagen verwendet **Nicht in den letzten 60 Tagen verwendet** **Nicht in den letzten 30 Tagen verwendet**	Die Anzahl der Anwendungsinstallationen, die in den letzten 90, 60 oder 30 Tagen nicht gestartet wurden. Ein Strich in dieser Spalte bedeutet, dass die Erfassung nicht für die Anwendung aktiviert ist.

Spaltenname	Beschreibung
	HINWEIS: Um korrekte Erfassungsinformationen zu erhalten, müssen Sie zunächst die Erfassung für die Anwendung und für die Geräte aktivieren, auf denen die Anwendung installiert ist. Siehe Erfassung von Geräten und Anwendungen aktivieren und konfigurieren.
Deckung	Der Lizenztyp. Es gibt folgende Lizenztypen: • **Upgrade**: Die installierte Anwendung ist ein Upgrade einer früheren Version (erfordert einen Servicevertrag). • **Downgrade**: Die installierte Anwendung verwendet eine Lizenz für eine spätere Version (erfordert Downgrade-Berechtigungen). • **Original**: Die installierte Anwendung verwendet eine Lizenz, die mit ihrer Versionsnummer übereinstimmt. • **Keine**: Die Anwendung wurde ohne Lizenz installiert.
Plattform	Das Betriebssystem, auf dem die Anwendung ausgeführt wird.
Edition	Der Name der Edition im Zusammenhang mit der Anwendung, z. B. "Professional Edition" oder "Standard Edition".

3. Zum Sortieren der Liste klicken Sie auf **Anzeigen nach** und wählen dann eine Ansicht aus.

   Sie können Anwendungen nach Produkt wie "Microsoft Office" oder nach Produkt und Edition wie "Microsoft Office Professional" und "Office Standard" anzeigen. Wenn Sie z. B. alle Editionen von Microsoft Office-Anwendungen unter einer Überschrift anzeigen wollten, könnten Sie in der Dropdown-Liste *Anzeigen nach* die Option **Produkt** auswählen. Die Spalte *Lizenziert* zeigt die Anzahl der Lizenzplätze, die für alle Anwendungen in der Microsoft Office-Gruppe verfügbar sind. Zum Anzeigen von Microsoft Office-Anwendung nach Edition wählen Sie in der Dropdown-Liste Ansicht *Anzeigen nach* die Option **Produkt und Edition** aus. Die Spalte *Lizenziert* zeigt die Anzahl der Lizenzplätze, die für jede Edition von Microsoft Office verfügbar sind.

   TIPP: Wenn eine Gruppe wie "Office" reduziert ist und nur das übergeordnete Element angezeigt wird, sehen Sie links neben der Spalte *Name* dann ein Warnsymbol, wenn ein Element in der Gruppe eine negative Differenz aufweist oder mehr Plätze verwendet als nach der Lizenz zulässig. ⚠.

4. Zum Anzeigen des Widgets "Lizenz-Compliance" klicken Sie auf der **Startseite** in der linken Navigationsleiste auf die Seite *Dashboard* für Administratoren.

   TIPP: Wird das Widget "Lizenz-Compliance" nicht angezeigt, klicken Sie oben rechts auf **Anpassen**, um es zu installieren. Siehe Dashboard-Seiten anpassen.

5. Zum Anzeigen oder Ändern von Informationen zur Anzahl der unter einer Lizenz verfügbaren Lizenzplätze rufen Sie die Detailseite für das *Lizenz*-Asset auf. Siehe Assets anzeigen und nach Asset-Informationen suchen.

Rückgewinnen ungenutzter Softwarelizenzen

Appliance-Administratoren können eine Richtlinie festlegen, anhand derer katalogisierte Software auf Grundlage dessen, wie häufig bestimmte Softwareanwendungen auf Benutzergeräten verwendet werden, deinstalliert werden können, um nicht ausgelastete Software zu erfassen und sie ggf. neu zu verwenden.

Sie haben eine Möglichkeit, Lizenzen für eine bestimmte Softwareanwendung zurückzufordern, die in den letzten 30, 60 oder 90 Tagen oder mit allen zugehörigen Lizenzen nicht verwendet wurde.

1. Rufen Sie die Seite *Lizenz-Compliance* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Asset Management** und anschließend auf **Lizenz-Compliance**.
2. Erweitern Sie in der Spalte **Name** den Namen der Anwendung und wählen Sie eine Version der Softwarelizenz aus, die Sie freigeben möchten.

   HINWEIS: Sie können nur Lizenzen für jeweils eine Softwareversion gleichzeitig zurückgewinnen. Die Auswahl mehrerer Versionen führt zu einem Fehler.
3. Wenn Sie Lizenzen für die Softwareversion zurückgewinnen möchten, wählen Sie **Aktion wählen > Software zurückgewinnen** aus und wählen Sie nach Bedarf eine der folgenden Optionen:
   - **Nicht in den letzten 30 Tagen verwendet**
   - **Nicht in den letzten 60 Tagen verwendet**
   - **Nicht in den letzten 90 Tagen verwendet**
   - **Alle**

   Die Seite *Verwaltete Installationsdetails* wird angezeigt, auf der Sie einen Prozess erstellen können, der die Installation des ausgewählten Softwareelements von den zugehörigen Endbenutzergeräten entfernt.
4. Erstellen Sie ggf. eine neue verwaltete Installation. Weitere Informationen finden Sie nach Bedarf in den folgenden Abschnitten:
   - Verwaltete Installationen für Windows Geräte erstellen
   - Verwaltete Installationen für Mac OS X Geräte erstellen
   - Verwaltete Installationen für RPM-Dateien erstellen

Manuelle Aktualisierung der Softwarelizenz-Compliance-Informationen

Sie können die Softwarelizenz-Compliance-Informationen jederzeit manuell aktualisieren. Bei einer großen Anzahl von Appliances kann die Aktualisierung der Informationen jedoch einige Minuten dauern.

Auf den agentenverwalteten Geräten im Inventar Ihrer Appliance laufen Softwareanwendungen, die im Softwarekatalog verfügbar sind.

Die Softwarelizenz-Compliance-Informationen werden automatisch jeden Tag nach dem täglichen Sicherungsvorgang der Appliance aktualisiert. Durch manuelles Aktualisieren der Lizenz-Compliance-Informationen erhalten Sie Informationen auf dem neuesten Stand.

HINWEIS: Haben Sie keine Lizenz-Assets für Anwendungen im Inventar hinzugefügt, zeigt die Seite *Lizenz-Compliance* bei der Anzahl der für Anwendungen verfügbaren Arbeitsplätze "0" an. Die Differenz entspricht der Anzahl der Software-Installationen.

1. Rufen Sie die Seite *Lizenz-Compliance* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Asset Management** und anschließend auf **Lizenz-Compliance**.
2. Klicken Sie über der Liste auf **Jetzt aktualisieren**.

   Die Appliance überprüft, ob die neuesten Lizenznutzungsinformationen vorliegen, und aktualisiert die Liste.

   TIPP: Wenn Sie rechts über der Liste auf **Aktualisieren** klicken, werden die bereits erfassten Informationen angezeigt. Neue Informationen zur Lizenznutzung werden dabei nicht berücksichtigt.

Konfigurieren von Warnungsschwellenwerten für die Lizenznutzung

Sie können Warnungsschwellenwerte für die Lizenznutzung anpassen und damit den Prozentsatz der Lizenznutzung angeben, der als Wert für eine Warnung oder als kritischer Wert eingestuft wird.

Lizenz-Compliance-Informationen werden auf dem Appliance-Dashboard angezeigt. Wenn auf der Appliance die Organisationskomponente aktiviert wurde, können Sie für jede Organisation separat Warnungsschwellenwerte für die Lizenznutzung erstellen.

1. Rufen Sie die Seite *Allgemeine Einstellungen* auf der Verwaltungsebene auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Einstellungen** und anschließend auf **Systemsteuerung**.
   c. Klicken Sie in der *Systemsteuerung* auf **Allgemeine Einstellungen**.
2. Scrollen Sie nach unten zum Bereich *Warnkonfigurationen zur Lizenznutzung*.
3. Geben Sie in den Feldern *Warnungsschwellenwert* und *Kritischer Schwellenwert* neue Werte ein.

   Standardmäßig beträgt der *Warnungsschwellenwert* 90. Der *Kritische Schwellenwert* 100.
4. Klicken Sie zum Speichern auf **Dienste speichern und neu starten**.

   Die Schwellenwerte werden festgelegt. Wenn Sie Lizenz-Assets erstellt haben, werden Lizenz-Compliance-Informationen auf der Seite *Dashboard* der **Administratorkonsole** angezeigt.

Verwandte Themen

Hinzufügen von Lizenz-Assets für das Inventar der Seite "Software"

Anzeigen von Informationen zur Lizenz-Compliance und -Konfiguration

Anzeigen von Informationen zur Lizenz-Compliance und -Konfiguration

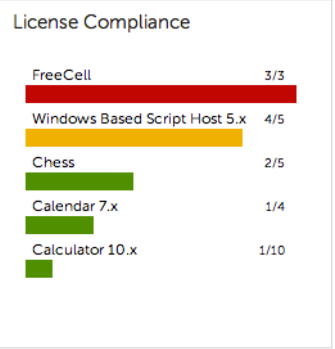
Wenn Sie Lizenz-Assets für Anwendungen eingerichtet haben, können Sie Lizenz-Compliance- und Konfigurationsinformationen für diese Anwendungen anzeigen.

Informationen stehen für Lizenz-Assets zur Verfügung, die mit Anwendungen auf den Registerkarten *Software* und *Softwarekatalog* verknüpft sind. Siehe Einrichten der Lizenz-Compliance.

Wenn Sie mehrere Organisationen haben, können Sie die Lizenzinformationen für jede Organisation getrennt anzeigen.

1. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
2. Klicken Sie auf **Startseite**.

   Software-Compliance-Informationen werden im Widget *Lizenz-Compliance* angezeigt.

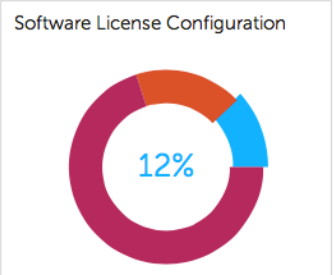


> **HINWEIS:** Die Appliance aktualisiert die Daten im Widget *Lizenz-Compliance* alle acht Stunden. Wenn Sie auf die Schaltfläche **Aktualisieren** klicken, werden die Daten nicht aktualisiert, sondern nur die bereits erfassten Daten angezeigt.

Die folgenden Farben geben die Nutzung an:

Farbe	Beschreibung
Rot	Die Nutzung hat den kritischen Schwellenwert erreicht oder überschritten.
Orange	Die Nutzung hat den Warnungsschwellenwert erreicht oder überschritten, liegt aber unter dem kritischen Schwellenwert.
Grün	Die Nutzung liegt unter dem Warnungsschwellenwert.

Im Widget *Softwarelizenz-Konfiguration* werden die Prozentsätze für die Softwarelizenzen angezeigt, die als Einheiten- und Standortlizenzen und weitere Lizenzmodi kategorisiert sind.



Optional: Weitere Informationen hierzu finden Sie auf der Seite *Lizenz-Compliance*. Siehe Anzeigen von Informationen zur Lizenz-Compliance für Anwendungen im Softwarekatalog.

Einrichten des Service Desks

Einrichten des Service Desks umfasst das Einrichten von Rollen für Service Desk-Mitarbeiter sowie das Konfigurieren von Ticket- und E-Mail-Einstellungen.

Einrichten von Rollen für Benutzerkonten

Der Service Desk verwendet berechtigungsbasierte Rollen, um den Zugriff auf Service Desk-Funktionen und -Informationen zu steuern. Diese Rollen können Benutzern bei der Anmeldung automatisch zugewiesen werden. Hierfür können Standardrollen oder benutzerdefinierte Rollen verwendet werden.

Informationen zu Standardrollen

Standardrollen sind für standardmäßige Benutzerkontotypen wie Administrator, Endbenutzer und Benutzer mit begrenztem Zugriff verfügbar.

Folgende Optionen sind standardmäßig verfügbar: Weitere Informationen zur Verwaltung von Organisationsrollen finden Sie unter Verwalten von Organisationsrollen und Benutzerrollen.

Rolle	Beschreibung
Organisationsrollen	Organisationsrollen sind Berechtigungsgruppen, die Organisationen zugewiesen werden, und anhand derer die Berechtigungen festgelegt werden, die für die Benutzer in den jeweiligen Organisationen verfügbar sind. Wird einer Organisation beispielsweise eine Organisationsrolle zugewiesen, bei der die Registerkarte *Verteilung* ausgeblendet ist, können die Benutzer in dieser Organisation, einschließlich des Admin-Benutzers, nicht auf die Registerkarte *Verteilung* zugreifen. **HINWEIS:** Organisationsrollen sind nur in Appliances mit aktivierter Organisationskomponente verfügbar.
Standardrolle	Die Standardrolle im Abschnitt über Organisationsrollen verfügt über Schreib- und Leseberechtigungen für alle Registerkarten. Sie können die Standardrolle zwar nicht bearbeiten

Rolle	Beschreibung
	oder löschen, aber stattdessen zusätzliche Organisationsrollen erstellen.
Benutzerrollen	Benutzern zugewiesene Rollen, um deren Zugang zur **Administratorkonsole** und **Benutzerkonsole** zu steuern. Wenn die Organisationskomponente in Ihrer Appliance aktiviert ist, sind die zu diesen Rollen verfügbaren Berechtigungen von der Organisationsrolle abhängig, die einer Organisation zugewiesen ist.
Administrator	Dies ist die Benutzerrolle mit den umfassendsten Berechtigungen in der Appliance. Benutzer mit der **Administrator**rolle können standardmäßig Informationen und Einstellungen anzeigen und ändern. Hierzu zählt auch das Hoch- oder Herabstufen anderer Benutzer durch Ändern ihrer Rollen. Die **Administrator**rolle kann weder geändert noch gelöscht werden. Weisen Sie diese Rolle nur vertrauenswürdigen Administratoren zu. Mitarbeiter, denen die **Administratorrolle** zugewiesen wurde, sind berechtigt, Service-Desk-Tickets auf der Registerkarte *Tickets* in der **Administratorkonsole** zu verwalten und zu ändern, obwohl sie selbst möglicherweise keine Tickets besitzen dürfen. Benutzer mit der **Administrator**rolle können außerdem die Sicherheits-, Skripterstellungs- und Verteilungsfunktionen zur Auflösung von Service-Desk-Tickets verwenden und die Probleme anschließend in der Knowledge Base dokumentieren. Die Rolle des **Administrators** interagiert vor allem über die **Administratorkonsole** mit der Appliance.
Kein Zugriff	Benutzer mit dieser Rolle können sich nicht bei der **Administratorkonsole** oder **Benutzerkonsole** anmelden.
Administrator mit Leseberechtigung	Diese Rolle berechtigt Inhaber dazu, Informationen oder Einstellungen in der Appliance anzuzeigen, jedoch nicht dazu, sie zu ändern. Sie eignet sich für Mitarbeiter mit Überwachungsfunktion, wie beispielsweise Vorgesetzte. Diese Rolle interagiert vor allem über die **Administratorkonsole** mit der Appliance.
Nur Benutzerkonsole	Diese Rolle ist für Appliance-Benutzer gedacht. Sie enthält standardmäßig die Berechtigung, Service-Desk-Tickets zu erstellen, anzuzeigen oder zu ändern. Diese Rolle interagiert ausschließlich über die **Benutzerkonsole** mit der Appliance.

Rolle für Service Desk-Mitarbeiter erstellen

Sie können eine Rolle für Service Desk-Mitarbeiter erstellen, um Berechtigungen für Benutzer festzulegen, die an Service Desk-Einstellungen und -Komponenten arbeiten.

Benutzer mit der **Administrator**rolle können alle Service Deck-Komponenten ändern sowie Benutzer erstellen und entfernen. Außerdem können Sie eine eingeschränktere Service Desk-Rolle für Ihre Organisation erstellen. Benutzer mit dieser Rolle haben die Berechtigung, Tickets zu bearbeiten, Elemente hinzuzufügen, die von der **Benutzerkonsole** heruntergeladen werden können, Artikel zur Knowledge Base hinzuzufügen und auf der Startseite der **Benutzerkonsole** angezeigte Ankündigungen zu verwalten. Sie haben jedoch nicht die Berechtigung, Benutzer zu verwalten, Berichte auszuführen oder die Appliance-Einstellungen zu ändern. In diesem Handbuch wird diese Gruppe als **Service Desk-Administrator** bezeichnet.

Wenn die Organisationskomponente in Ihrer Appliance aktiviert ist, können Sie separate Rollen für Service Desk-Administrator für jede Organisation erstellen.

1. Rufen Sie die Seite *Rollendetail* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie auf der linken Navigationsleiste auf **Einstellungen** und anschließend auf **Rollen**.
   c. Wählen Sie **Aktion auswählen** > **Neu**.
2. Geben Sie im Feld *Name* den Namen ein, beispielsweise Service Desk-Administrator.
3. Geben Sie im Feld *Beschreibung* eine Kurzbeschreibung der Rolle ein, beispielsweise Wird verwendet für Service Desk-Administratoren.

   Diese wird in der Liste *Rollen* angezeigt.
4. Klicken Sie auf den Link **[Alle erweitern]** neben Administratorkonsole *Berechtigungen*, um die Berechtigungseinstellungen für alle Kategorien anzuzeigen.
5. Wählen Sie diese benutzerdefinierten Berechtigungen für die neue Rolle aus:

Kategorie	Element	Berechtigungsstufe
Startseite	**Alle**	Alle lesen
Inventar	**Geräte**	SCHREIBEN
	Software	SCHREIBEN
	Softwarekatalog	SCHREIBEN
	Lizenz-Compliance	AUSBLENDEN
	Prozesse	AUSBLENDEN
	Startprogramme	AUSBLENDEN
	Dienste	AUSBLENDEN
	Erkennungszeitpläne	AUSBLENDEN
	Erkennungsergebnisse	AUSBLENDEN

Kategorie	Element	Berechtigungsstufe
	SNMP-Inventarkonfigurationen	AUSBLENDEN
Überwachung	**Geräte**	LESEN
	Warnungen	SCHREIBEN
	Profile	AUSBLENDEN
	Wartungsfenster	AUSBLENDEN
	Log Enablement Packages	AUSBLENDEN
Assets	**Alle**	AUSBLENDEN
Verteilung	**Alle**	AUSBLENDEN
Skripterstellung	**Alle**	AUSBLENDEN
Sicherheit	**Alle**	AUSBLENDEN
Service Desk	**Tickets**	SCHREIBEN
	Benutzerdownloads	SCHREIBEN
	Knowledge Base	SCHREIBEN
	Ankündigungen	SCHREIBEN
	Archiv	LESEN
	Konfiguration	LESEN
Berichterstellung	**Alle**	Alle ausblenden
Einstellungen	**Alle**	Alle ausblenden
Benutzerkonsole	**Alle**	Alle lesen

6. Klicken Sie auf **Speichern**.

Die Seite *Rollen* wird mit der neuen Rolle angezeigt. Wenn sich ein Benutzer anmeldet, der dieser Rolle zugeordnet ist, werden in der Leiste für Appliance-Komponenten die verfügbaren Funktionen angezeigt.

Benutzerrollen zuweisen

Nach dem Importieren oder Erstellen von Benutzerkonten können Sie diesen Konten Benutzerrollen zuweisen.

HINWEIS: Benutzerkonten können von einem LDAP-Server importiert werden. Siehe Importieren von Benutzern aus einem LDAP-Server.

1. Rufen Sie die Liste *Benutzer* auf:

a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.

b. Klicken Sie auf der linken Navigationsleiste auf **Einstellungen** und anschließend auf **Benutzer**.

2. Weisen Sie Ihren Service Desk-Administratoren die Rolle **Administrator** zu:

   a. Aktivieren Sie das Kontrollkästchen neben mindestens einem Benutzer.

   b. Wählen Sie **Aktion auswählen** > **Rolle übernehmen** > **Administrator**.

   Administratorbenutzer haben standardmäßig Besitzer-/Absender-Berechtigungen.

3. Weisen Sie Ihren Teambenutzern die Rolle **Service Desk-Mitarbeiter** zu:

   a. Aktivieren Sie das Kontrollkästchen neben mindestens einem Benutzer.

   b. Wählen Sie **Aktion auswählen** > **Rolle übernehmen** > **Service Desk-Mitarbeiter**.

4. Weisen Sie den Mitgliedern des Service Desk-Teams das Label **Alle Ticketbesitzer** zu.

   a. Aktivieren Sie das Kontrollkästchen neben mindestens einem Benutzer.

   b. Wählen Sie **Aktion auswählen** > **Label zuweisen** > **Alle Ticketbesitzer**.

   Das Label wird angewendet und neben jedem Benutzernamen angezeigt.

5. Erstellen Sie ein Label namens **Benutzer** und weisen Sie dann das Label **Benutzer** und die Rolle Ihren Benutzern zu.

Verwandte Themen

Benutzerdefinierte Ticketfelder definieren

Rolle für Service Desk-Mitarbeiter erstellen

Label "Alle Ticketbesitzer" hinzufügen

Labels und Rollen auf Service Desk-Mitarbeiter anwenden

Sie können Labels und Rollen auf Service Desk-Mitarbeiter anwenden, um deren Berechtigungen zu verwalten.

Weitere Informationen zum Erstellen von Labels und Rollen finden Sie unter Einrichten von Rollen für Benutzerkonten und Labels für Benutzerkonten festlegen.

1. Fügen Sie dem Alias **DefaultTicketOwners@meinedomain.com** einen Benutzer hinzu.
2. Rufen Sie die Seite *Benutzerdetails* auf.

   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.

   b. Klicken Sie auf der linken Navigationsleiste auf **Einstellungen** und anschließend auf **Benutzer**.

   c. Führen Sie eine der folgenden Aktionen aus, um die Seite *Benutzerdetails* anzuzeigen:

   - Klicken Sie auf den Namen eines Benutzers.
   - Wählen Sie **Aktion auswählen** > **Neu**.

3. Klicken Sie im Feld *Zuweisen zu Label* auf **Bearbeiten**.
4. Ziehen Sie im Fenster "Label" das Label **Alle Ticketbesitzer** mit der Maus in das Feld *Zuweisen zu* und klicken Sie dann auf **Speichern**.

HINWEIS: Wenn das Label noch nicht vorhanden ist, müssen Sie es erstellen.

5. Wählen Sie im Feld *Rolle* die Rolle **Service Desk-Mitarbeiter** aus.
6. Klicken Sie auf **Speichern**.

Der Benutzer ist nun berechtigt, Tickets zu besitzen, zu bearbeiten, zu lösen und abzuschließen. Außerdem erhält er automatisch eine E-Mail, wenn ein Ticket erstellt wurde.

Verwandte Themen

Label "Alle Ticketbesitzer" hinzufügen

Rolle für Service Desk-Mitarbeiter erstellen

Konto "DefaultTicketOwners" erstellen

Wenn Ihre Service Desk-Mitarbeiter E-Mail-Benachrichtigungen erhalten sollen, wenn neuen Tickets erstellt wurden, können Sie ein Benutzerkonto DefaultTicketOwners erstellen.

Sie können dann die Seite *Details zum Ticket* konfigurieren, damit Sie das Konto wie in Konfigurieren der Ticketeinstellungen beschrieben verwenden können.

Weitere Informationen zu E-Mail-Benachrichtigungen finden Sie unter Informationen zu E-Mail-Benachrichtigungen.

1. Rufen Sie die Seite *Benutzerdetails* auf.
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie auf der linken Navigationsleiste auf **Einstellungen** und anschließend auf **Benutzer**.
   c. Wählen Sie **Aktion auswählen** > **Neu**.
2. Geben Sie mindestens die folgenden Details an:

Feld	Beschreibung
Anmeldung	DefaultTicketOwners
Name	DefaultTicketOwners
E-Mail	DefaultTicketOwners@**meinedomain.com**
Kennwort	Geben Sie ein Kennwort ein.
Kennwort bestätigen	Geben Sie das Kennwort erneut ein.
Rolle	Kein Zugriff
Zuweisen zu Label	Alle Ticketbesitzer

3. Klicken Sie auf **Speichern**.
4. Wenn Sie diesen neuen Benutzer als Standardbesitzer von Tickets zuweisen möchten, wählen Sie wie in Konfigurieren der Ticketeinstellungen beschrieben die Option **DefaultTicketOwners**.

HINWEIS: Der erste Standardbesitzer bleibt immer der Standardbesitzer eines Tickets. Der Standardbesitzer eines Tickets ändert sich beispielsweise nicht, wenn Sie ein vorhandenes Ticket in eine andere Kategorie mit einem anderen Besitzer verschieben.

Konfigurieren der E-Mail-Einstellungen

Sie können eine E-Mail-Benachrichtigungsstrategie für eine Warteschlange einrichten. Wenn Sie mehrere Warteschlangen haben, können Sie die E-Mail-Einstellungen für jede Warteschlange individuell anpassen.

In den Systemanforderungen wird eine E-Mail-Benachrichtigungsstrategie beschrieben.

Standardmäßig sendet der Service Desk automatisch eine E-Mail, um Ihre Mitarbeiter zu benachrichtigen, wenn ein Ticket zu lange in einem bestimmten Status verbleibt. Außerdem wird ein Ticket mit der Priorität **Hoch** eskaliert, wenn es nicht innerhalb von 30 Minuten geändert oder abgeschlossen wird. Informationen zum Ändern der Eskalationszeiten und der Liste der Tickets, für die sie gelten, finden Sie unter Seite Details zum Ticket anpassen.

Grundsätzlich sollte die Appliance nie konfiguriert werden, an sich selbst E-Mails zu schicken. Wenn die E-Mail-Adresse einer Warteschlange beispielsweise `helpdesk@example.com` lautet, dann sollte die E-Mail-Adresse `helpdesk@example.com` nicht für die Liste *Kategorie-CC* oder andere Einstellungen gültig sein, für die E-Mail-Adressen eingegeben werden können.

Folgende E-Mail-Benachrichtigungsstrategie wird von den meisten Quest KACE Kunden verwendet, um zu verhindern, dass ihre Mitarbeiter mit unnötigen Benachrichtigungen überflutet werden:

- Wenn ein Ticket erstellt wurde, erhalten alle Service Desk-Mitarbeiter eine E-Mail-Benachrichtigung. Weitere Hinweise zu E-Mail-Benachrichtigungen finden Sie unter Informationen zu E-Mail-Benachrichtigungen.
- Nachdem ein Service Desk-Mitarbeiter Besitzer des Tickets geworden ist, erhalten die anderen Mitarbeiter keine E-Mails mehr zum Ticket, es sei denn, der Fall wird eskaliert (sie können jedoch nach dem Ticket suchen).
- Die Ticketabsender und -besitzer werden jedes Mal per E-Mail benachrichtigt, wenn sich der *Zustand* oder *Status* des Tickets ändert.
- Der Ticketbesitzer wird über jede Änderung am Ticket benachrichtigt.
- Wenn ein Ticket eskaliert wird, werden sowohl der Ticketbesitzer als auch jede in der Liste *Kategorie CC* enthaltene Person benachrichtigt.

Informationen zu E-Mail-Benachrichtigungen

Wenn Service-Desk-Tickets erstellt oder geändert werden, sendet die Appliance E-Mail-Benachrichtigungen basierend auf der Methode für die Ticketübermittlung, den Einstellungen für E-Mail bei Ereignissen und ausgeführten Aktionen.

Folgende Regeln werden auf E-Mail-Benachrichtigungen angewendet:

- Wenn Tickets über die **Administratorkonsole** oder **Benutzerkonsole** übermittelt oder geändert werden, erhält der Ticketabsender keine E-Mail-Bestätigung, es sei denn *Neues Ticket über Portal* wurde für den *Absender* im Abschnitt *E-Mail zu Ereignissen* auf der Seite *Service Desk Warteschlange-E-Mail-Einstellungen* aktiviert (weitere Informationen zu E-Mail-Einstellungen speziell für Warteschlangen finden Sie unter E-Mail-Auslöser konfigurieren). Andere mit diesem Ticket verknüpfte Benutzer, beispielsweise **Besitzer**, **Genehmiger**, **CC-Liste** und **Kategorie-CC**, erhalten E-Mail-Benachrichtigungen, wie im Abschnitt *E-Mail bei Ereignissen* auf der Seite *Warteschlangen-Detail* festgelegt. Vollständige Angaben finden Sie unter E-Mail-Auslöser und E-Mail-Vorlagen konfigurieren.
- Wenn Tickets per E-Mail erstellt werden, erhält der Ticketabsender eine E-Mail-Bestätigung. Wenn ein Ticket jedoch per E-Mail geändert wird, wird keine Benachrichtigung an den Ticketabsender geschickt.
- E-Mail-Nachrichten mit Benachrichtigungen über Änderungen werden beim Ändern von Tickets absichtlich verzögert. Mit dieser Verzögerung soll die Anzahl der bei Änderungen gesendeten E-Mail-Benachrichtigungen verringert werden. Wenn beispielsweise ein Ticketbesitzer einen Kommentar hinzufügt

und das Ticket speichert und dann sofort eine zweite Änderung am Ticket vornimmt, wird nur eine Änderungsbenachrichtigung gesendet.

> **HINWEIS:** E-Mail-Nachrichten ist folgender Text vorangestellt: +++++ Fügen Sie oberhalb dieser Zeile einen Kommentar hinzu +++++.

- Wenn verwaltete Geräte oder Benutzerkonten aus dem Inventar gelöscht werden, werden E-Mail-Benachrichtigungen für Service-Desk-Tickets zu diesen Geräten unterdrückt, um unnötige Benachrichtigungen zu vermeiden.

Informationen zu Ticketregeln

Wenn die Standard-E-Mail-Einstellung Ihren Anforderungen nicht genügt, können Sie diese mithilfe von Ticketregeln ändern.

Weitere Informationen zu Ticketregeln finden Sie unter Verwenden von Ticketregeln.

Zahlreiche komplexe Ticketregeln, z. B. zur Änderung des Verhaltens von E-Mail-Benachrichtigungen, finden Sie auf der Website von **Quest Support** unter https://support.quest.com/contact-support.

Informationen zu POP3-E-Mail-Konten

Sie können die Appliance für den Empfang von E-Mails von POP3-Servern konfigurieren.

Führen Sie hierzu folgende Schritte durch:

- Aktivieren und konfigurieren Sie einen externen SMTP-Server in den Netzwerkeinstellungen der Appliance. Siehe Externen SMTP-Server oder sicheren SMTP-Server verwenden.
- **Optional**. Konfigurieren Sie die E-Mail-Voreinstellungen des Service Desk. Siehe E-Mail-Voreinstellungen konfigurieren.
- Konfigurieren Sie die SMTP-Server- und POP3-Einstellungen in den Service Desk-Ticketwarteschlangen. Siehe Warteschlangen-spezifische E-Mail-Einstellungen konfigurieren.

Wenn Sie keinen POP3-E-Mail-Server nutzen, können Sie den in die KACE SMA integrierten SMTP-Server verwenden, um eingehende E-Mail-Nachrichten von Ihrem internen E-Mail-Server zu empfangen.

> **WICHTIG: Der POP3-E-Mail-Server der Appliance muss die Authentifizierungsdaten und den E-Mail-Text selbst als unverschlüsselten Text übermitteln.**

POP3-E-Mail-Konten erstellen und konfigurieren

Sie können POP3-E-Mail-Konten zur Verwendung durch die Service Desk-Mitarbeiter und Benutzer erstellen und konfigurieren:

Es gibt zwei Konten:

- **Support@meinedomain.com**. Diese E-Mail-Adresse wird für Folgendes verwendet:
  - Um alle neuen Tickets nach ihrer Erstellung zu empfangen
  - Um Benutzern und Service Desk-Mitarbeitern zu ermöglichen, Tickets automatisch zu erstellen und zu ändern
  - Als E-Mail-Adresse, an die Benutzer eine Antwort schicken können

An diese Adresse zugestellte E-Mails werden nicht persönlich bearbeitet, Ihre Service Desk-Mitarbeiter werden jedoch über Ticketänderungen benachrichtigt, die sich aus den E-Mails ergeben.

- **DefaultTicketOwners@meinedomain.com**. Dieser E-Mail-Alias wird für Folgendes verwendet:
  - Um den Service Desk-Mitarbeitern die Kommunikation untereinander zu ermöglichen
  - Um automatisierte E-Mail-Benachrichtigungen über neue und offene Tickets durch die Appliance zu senden

1. Erstellen Sie Support@**meinedomain**.com als gültige E-Mail-Adresse auf Ihrem POP3-E-Mail-Server.
2. Konfigurieren Sie DefaultTicketOwners@**meinedomain**.com als E-Mail-Alias für die Service Desk-Mitarbeiter und fügen Sie diesem alle E-Mail-Adressen Ihrer Service Desk-Mitarbeiter hinzu. Dies ist ein allgemeiner E-Mail-Alias, den Ihre Service Desk-Mitarbeiter für die Kommunikation untereinander verwenden.
3. Falls Sie einen externen, von der Appliance genutzten SMTP-Server verwenden wollen, konfigurieren Sie diesen auf der Seite *Netzwerkeinstellungen* in der Systemverwaltungskonsole. Siehe Netzwerkeinstellungen der Appliance ändern.

   TIPP: Falls Sie POP3 für Service Desk-Ticket-E-Mails verwenden möchten, können Sie die POP3-Einstellungen auf der Warteschlangenebene konfigurieren.

4. **Optional**. Konfigurieren Sie die E-Mail-Voreinstellungen des Service Desk. Siehe E-Mail-Voreinstellungen konfigurieren.
5. Falls Sie für jede Warteschlange unterschiedliche SMTP- oder POP3-Einstellungen verwenden wollen, können Sie diese auf Warteschlangenebene angeben. Siehe Warteschlangen-spezifische E-Mail-Einstellungen konfigurieren.

E-Mail-Voreinstellungen konfigurieren

Sie können Voreinstellungen für die an Service Desk-Benutzer und -Mitarbeiter gesendeten und von diesen empfangenen E-Mails erstellen und konfigurieren.

Standardmäßig ist das Service Desk zur Verwendung eines internen SMTP-Servers zum Senden Ticket-bezogener E-Mails konfiguriert. Sie können optional einen externen SMTP-Server verwenden, müssen diesen jedoch in den Netzwerkeinstellungen der Appliance konfigurieren. Weitere Informationen hierzu finden Sie unter Netzwerkeinstellungen der Appliance ändern.

1. Rufen Sie die Seite *Service Desk, E-Mail-Voreinstellungen* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Service Desk** und anschließend auf **Konfiguration**.
   c. Klicken Sie im Fensterbereich **Konfiguration** im Abschnitt *E-Mail-Konfiguration* auf **Service Desk E-Mail-Voreinstellungen konfigurieren**.
2. Auf der Seite *Service Desk, E-Mail-Voreinstellungen* aktivieren Sie im Abschnitt *Ausgehende E-Mail* das Kontrollkästchen *Text „Antwort über dieser Zeile“ in ausgehende E-Mail-Kommunikation einschließen*.

   Es wird empfohlen, diese Funktion zu verwenden, um zu verhindern, dass die gesamte E-Mail-Kette zu jedem Kommentar hinzugefügt wird.
3. Geben Sie den Text an, der im E-Mail-Betreff erkannt werden soll. Wenn beim Service Desk eine auf ein Ticket bezogene E-Mail mit der entsprechenden Betreffzeile eingeht, wird diese E-Mail nicht weiter bearbeitet.
   a. Geben Sie im Abschnitt *Eingehende E-Mail* im Feld *E-Mails mit folgendem Text im Betreff ignorieren* die Worte ein, die Sie entdecken möchten. Sie können mehrere Einträge angeben,

die durch ein Semikolon voneinander getrennt sind. Beispiel: Abwesend;Fehlgeschlagene Mailzustellung.

4. Konfigurieren Sie die Schwellenwerte für alle eingehenden E-Mail-Benachrichtigungen während eines bestimmten Zeitraums. Wenn diese Schwellenwerte erreicht sind, sendet das Service Desk keine weiteren E-Mail-Benachrichtigungen.

> **HINWEIS:** Wenn der Gesamtschwellenwert erreicht wird, wird das Senden von Benachrichtigungen für alle Tickets unterbrochen. Wenn der Schwellenwert für ein einzelnes Ticket erreicht wird, wird das Senden von Benachrichtigungen nur für das betroffene Ticket unterbrochen. Wenn die Anzahl an E-Mail-Updates im vorgegebenen Zeitraum geringer als der konfigurierte Schwellenwert ist, wird das Senden von Benachrichtigungen fortgesetzt.

Option	Beschreibung
E-Mails gesamt	Die maximale Anzahl aller E-Mails, die das Service Desk empfängt und mit E-Mail-Benachrichtigungen beantwortet. Der Standardwert beträgt 100 E-Mails.
Innerhalb von x Minuten erhalten	Das Zeitintervall in Minuten, während derer die angegebene Anzahl von E-Mails empfangen werden. Der Standardwert beträgt eine Minute. Um diese Beschränkung aufzuheben, können Sie eine hohe Zahl wie 99999 einstellen.

5. Konfigurieren Sie die Schwellenwerte für eingehende E-Mail-Benachrichtigungen pro Ticket während eines bestimmten Zeitraums. Wenn diese Schwellenwerte erreicht sind, sendet das Service Desk keine weiteren E-Mail-Benachrichtigungen.

Option	Beschreibung
Gesamtzahl der E-Mails pro Ticket	Die maximale Anzahl aller E-Mails, die das Service Desk für jedes Ticket empfängt und mit E-Mail-Benachrichtigungen beantwortet. Der Standardwert beträgt 5 E-Mails pro Ticket.
Innerhalb von x Minuten erhalten	Geben Sie das Zeitintervall in Minuten ein, während dessen die angegebene Anzahl von E-Mails für jedes Ticket empfangen werden. Der Standardwert beträgt eine Minute. Um diese Beschränkung aufzuheben, stellen Sie eine hohe Zahl wie 99999 ein.

6. Klicken Sie auf **Speichern**.

Anschließend können Sie POP3-E-Mail-Konten für bestimmte Service Desk-Warteschlangen konfigurieren. Weitere Informationen hierzu finden Sie unter Warteschlangen-spezifische E-Mail-Einstellungen konfigurieren.

E-Mail-Auslöser und E-Mail-Vorlagen konfigurieren

Sie können Auslöser einrichten, die automatisch E-Mails von der Appliance senden und Vorlagen verwenden, um den Inhalt dieser E-Mail-Nachrichten festzulegen.

Im Abschnitt *E-Mail bei Ereignissen* legen Sie fest, welche Aktionen eine E-Mail an die verschiedenen Benutzer der Appliance auslösen. Der Inhalt der Nachrichten wird anhand von E-Mail-Vorlagen festgelegt.

Timing von E-Mail-Nachrichten

Die folgenden E-Mail-Ereignisse lösen bei der Appliance das sofortige Senden einer E-Mail aus:

- **Kommentar**: Das System sendet E-Mail-Benachrichtigungen für Kommentare, wenn Benutzer auf dem Ticketformular Kommentare hinzufügen und auf **Senden** klicken. Wenn Benutzer auf dem Ticketformular Kommentare hinzufügen und auf **Speichern** klicken, wird jedoch nur die Benachrichtigung *Alle Änderungen* gesendet.
- **Ticket abgeschlossen**: Wenn die Zufriedenheitsumfrage aktiviert ist, wird sofort nach dem Schließen von Tickets eine E-Mail versendet, die die Umfrage beschreibt.

Die folgenden E-Mail-Ereignisse lösen aus, dass die Appliance E-Mails in einem Intervall von einigen Minuten sendet, um eine übermäßige E-Mail-Anzahl zu vermeiden:

- Alle Änderungen
- Besitzeränderung
- Statusänderung
- Genehmigungsänderung
- Änderung der Lösung
- Eskalation
- SLA-Verstoß
- Neues Ticket per E-Mail

E-Mail-Auslöser konfigurieren

Sie können E-Mail-Auslöser für eine Warteschlange konfigurieren. Wenn Sie mehrere Warteschlangen haben, können Sie die E-Mail-Auslöser für jede Warteschlange individuell anpassen.

1. Rufen Sie die Seite *Warteschlangen-Detail* des Service Desks auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Service Desk** und anschließend auf **Konfiguration**.
   c. Klicken Sie im Fensterbereich **Konfiguration** auf **Warteschlangen**.
   d. Führen Sie eine der folgenden Aktionen aus, um die Seite mit den *Warteschlangendetails* anzuzeigen:
      - Klicken Sie auf den Namen einer Warteschlange.
      - Wählen Sie **Aktion auswählen** > **Neu**.
2. Klicken Sie auf der Seite *Warteschlangendetails* unter *E-Mail-Adresse* auf **E-Mail-Einstellungen für Warteschlange konfigurieren**, um die Seite *E-Mail-Einstellungen für Service Desk Warteschlange* anzuzeigen.
3. Wählen Sie auf der Seite *E-Mail-Einstellungen für Service Desk Warteschlange* im Abschnitt *E-Mail bei Ereignissen* die Optionen für das Senden von E-Mails aus, wenn die angegebenen Ereignisse eintreten. Jede Spalte entspricht einer Art von Service Desk-Benutzer(rolle) und jede Zeile entspricht einem Ticketereignis.

Service Desk-Benutzer(rolle)	Beschreibung
Besitzer	Die Person, die das Ticket lösen soll.

Service Desk-Benutzer(rolle)	Beschreibung
Absender	Die Person, deren Problem gelöst werden soll.
Genehmigt von	Die Person, die die Bearbeitung des Tickets genehmigen oder ablehnen kann.
Ticket CC	Eine oder mehrere E-Mail-Adressen, die im Feld *CC* des Tickets gespeichert sind.
Kategorie CC	Eine oder mehrere E-Mail-Adressen, die in der *CC-Liste* des *Kategoriewerts* des Tickets gespeichert sind. Siehe CC-Listen für Ticketkategorien konfigurieren.
Queue-Eigentümer	Ein oder mehrere Eigentümer der Ticketwarteschlange, wie vom Label *Eigentümer* angegeben. Dies gilt nur für die Ereignisse *Neues Ticket per E-Mail* und *Neues Ticket über Portal*.

Wenn ein Ticketereignis eintritt, werden an ausgewählte Rollen oder Benutzer E-Mails gesendet. Wenn Sie z. B. das Kontrollkästchen **Alle Änderungen** in der Spalte *Besitzer* aktivieren, wird bei jeder Ticketänderung eine E-Mail an den Ticketbesitzer gesendet. Für die Auslöser *Kommentar* und *Ticket abgeschlossen* werden sofort E-Mails versendet. Bei anderen Ticketänderungen werden E-Mails jedoch im Abstand von mehreren Minuten versendet, um eine E-Mail-Überlastung zu vermeiden.

HINWEIS: Wenn Benutzer die mobile App KACE GO auf ihrem Smartphone oder Tablet installiert haben, sendet das System Push-Benachrichtigungen für die ausgewählten Service Desk-Ticketereignisse.

Option	Beschreibung
Alle Änderungen	Eine beliebige Ticketinformation ist geändert worden.
Besitzeränderung	Das Ticketfeld *Besitzer* ist geändert worden.
Statusänderung	Das Ticketfeld *Status* ist geändert worden.
Kommentar	Im Abschnitt *Kommentare* des Tickets sind Informationen, Anhänge oder Screenshots hinzugefügt worden. Das System sendet E-Mail-Benachrichtigungen für Kommentare, wenn Benutzer auf dem Ticketformular Kommentare hinzufügen und auf **Senden** klicken. Wenn Benutzer auf dem Ticketformular Kommentare hinzufügen und auf **Speichern** klicken, wird jedoch nur die Benachrichtigung *Alle Änderungen* gesendet.
Genehmigungsänderung	Der Genehmigungsstatus des Tickets ist geändert worden.
Änderung der Lösung	Die Ticketauflösung ist geändert worden.

Option	Beschreibung
Eskalation	Das Ticket ist nicht innerhalb der durch die Ticketpriorität definierten Eskalationszeit aufgelöst worden.
SLA-Verstoß	Das Ticket ist nicht bis zum Fälligkeitsdatum aufgelöst worden.
Ticket abgeschlossen	Das Ticketfeld *Status* ist auf **Abgeschlossen** geändert worden. Dieses Ereignis wird für die Zusendung einer Zufriedenheitsumfrage an die Absender verwendet. Siehe Verwenden der Zufriedenheitsumfrage.
Neues Ticket per E-Mail	Ein Benutzer sendet eine E-Mail-Nachricht an den Service Desk und es wird ein Ticket erstellt.
Neues Ticket per E-Mail	Ein Ticket wird über die **Benutzerkonsole** erstellt.

4. Klicken Sie auf **Speichern**.

Verwandte Themen

Konfigurieren des Mobilgerätezugriffs

E-Mail-Vorlagen konfigurieren

Sie können die E-Mail-Vorlagen konfigurieren, die der Service Desk zum Generieren von E-Mail-Nachrichten für eine Warteschlange verwendet. Wenn Sie mehrere Warteschlangen haben, können Sie die E-Mail-Vorlagen für jede Warteschlange separat anpassen.

1. Rufen Sie die Seite *Warteschlangen-Detail* des Service Desks auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Service Desk** und anschließend auf **Konfiguration**.
   c. Klicken Sie im Fensterbereich **Konfiguration** auf **Warteschlangen**.
   d. Führen Sie eine der folgenden Aktionen aus, um die Seite mit den *Warteschlangendetails* anzuzeigen:
   - Klicken Sie auf den Namen einer Warteschlange.
   - Wählen Sie **Aktion auswählen** > **Neu**.
2. Klicken Sie auf der Seite *Warteschlangendetails* unter *E-Mail-Adresse* auf **E-Mail-Einstellungen für Warteschlange konfigurieren**, um die Seite *E-Mail-Einstellungen für Service Desk Warteschlange* anzuzeigen.
3. Klicken Sie auf der Seite *E-Mail-Einstellungen der Service Desk-Warteschlange* im Abschnitt *E-Mail bei Ereignissen* auf **E-Mails anpassen**, um die Seite *Service Desk-E-Mail-Benachrichtigungen* anzuzeigen.
4. Ändern Sie auf der Seite *Service Desk-E-Mail-Benachrichtigungen* die folgenden E-Mail-Vorlagen nach Bedarf.

   HINWEIS: Wenn der Standardtext für eine der Vorlagen geändert wird, werden die E-Mail-Nachrichten nicht in verschiedene Sprachen übersetzt.

Ticketbezogene Vorlage	Beschreibung	Standardempfänger
Ticket eskaliert	Wird zum Senden regelmäßiger Benachrichtigungen gemäß der für die Ticketpriorität in der Warteschlange konfigurierten Eskalationszeit verwendet. Wenn z. B. Tickets mit der Priorität **Hoch** eine Eskalationszeit von 30 Minuten haben, wird diese E-Mail für Tickets hoher Priorität alle 30 Minuten gesendet, bis die Ticketpriorität geändert oder das Ticket abgeschlossen wird.	Besitzer, Ticket-CC-Liste und Ticketkategorie-CC-Liste
Aus E-Mail erstelltes Ticket	Wird zur Bestätigung verwendet, dass ein Ticket aus einer E-Mail erstellt worden ist.	Absender
Ticket geändert	Wird zur Benachrichtigung von Empfängern verwendet, wenn Ticketinformationen geändert oder hinzugefügt werden.	Besitzer und Ticket-CC-Liste
Kommentar übermittelt	Wird zur Benachrichtigung von Empfängern verwendet, dass Kommentare zu Tickets hinzugefügt worden sind.	Besitzer, Absender, Genehmiger, Ticket-CC-Liste und Ticketkategorie-CC-Liste
Ticket abgeschlossen	Wird nach dem Abschluss von Tickets für die Zusendung einer Zufriedenheitsumfrage an die Absender verwendet. Siehe Verwenden der Zufriedenheitsumfrage.	Absender

Ticket manuell per E-Mail senden	Wird für Nachrichten verwendet, die mit der Aktion *Ticket per E-Mail senden* auf der Seite *Details zum Ticket* weitergeleitet werden.
	TIPP: Wenn Sie HTML/Markdown verwenden, muss das Token "$ticket_fields_visible" mit dem Tag `<pre>` umschlossen werden, um zu verhindern, dass Formatierungen wie Zeilenumbrüche verworfen werden. Beispiel:
	`<pre>`
	`$ticket_fields_visible</`
	`pre>`
		Manuelle Eingabe durch den Absender

Ticketbezogene Vorlage	Beschreibung	Standardempfänger
Verstoß gegen SLA	Wird zur Benachrichtigung von Empfängern verwendet, dass ein Ticket über das auf der Grundlage der SLA-Einstellungen (Service Level Agreement, Service Level-Vereinbarung) und der Ticketpriorität berechnete Fälligkeitsdatum hinaus geöffnet geblieben ist.	Kein(e). Auf der Seite *Warteschlangen-Detail* konfigurierbar

Fehlerbezogene Vorlage	Beschreibung	Empfänger
Fehler beim Erstellen des Tickets aus E-Mail	Wird zur Benachrichtigung von Absendern verwendet, dass das Ticket aus einem anderen Grund als **unbekannte E-Mail-Adresse** nicht erstellt werden konnte.	Absender
Antwort von unbekannter E-Mail-Adresse	Wird zur Benachrichtigung von Absendern verwendet, dass das Ticket nicht erstellt werden konnte, weil die E-Mail-Adresse des Absenders unbekannt ist.	Absender

In allen E-Mail-Vorlagen verwendete Token

Token	Beschreibung
$helpdesk_email	Die mit der Service Desk-Warteschlange verknüpfte E-Mail-Adresse. Diese Adresse wird auf der Seite *Warteschlangen-Detail* konfiguriert.
$helpdesk_name	Der Name der Service Desk-Warteschlange. Dieser Name wird auf der Seite "Warteschlangen-Detail" konfiguriert.
$userui_url	Ein Link zur **Benutzerkonsole**. Für den Zugriff auf die **Benutzerkonsole** sind die Anmeldeinformationen erforderlich.

In ticketbezogenen E-Mail-Vorlagen verwendete Token

Token	Beschreibung
$change_desc	Eine formatierte Repräsentation der Änderungen, die bei der letzten Speicherung des Tickets durchgeführt worden sind, einschließlich Feldänderungen und Kommentare.
$last_attachment	Der zuletzt zum Ticket hinzugefügte Anhang.
$last_comment	Der zuletzt zum Ticket hinzugefügte Kommentar.
$mobile_ticket_url	Ein Link zum Ticket KACE GO Mobile App. Wenn dieser Link in einer E-Mail auf einem Android

Token	Beschreibung
	oder iOS Mobilgerät angezeigt wird, öffnet er das zugehörige Ticket in der KACE GO Mobile App.
$process_description	Die Prozessbeschreibung. Sie kann wichtige Voraussetzungen enthalten, die die Benutzer abschließen müssen, bevor Sie fortfahren können, ein Ticket basierend auf einer Prozessvorlage zu erstellen.
$process_name	Der Name der Prozessvorlage.
$process_status	Der Status der Prozessvorlage, wie Genehmigung erforderlich, Zeitlimit für Genehmigung überschritten, Genehmigung empfangen, Genehmigung abgelehnt, Prozess abgebrochen und Prozess abgeschlossen.
$process_type	Der Prozesstyp. In einer Standardinstallation ist nur der *Service Desk* Prozesstyp enthalten. Sie können falls erforderlich neue Prozesstypen erstellen. Sie können beispielsweise einen Prozesstyp für den Zugriff auf eine bestimmte Anwendung oder eine Gruppe von Anwendungen erstellen. Weitere Informationen hierzu finden Sie unter Prozesstypen definieren.
$summary	Die aktuelle Zusammenfassung des Tickets.
$ticket_approver_email	Die E-Mail-Adresse des Ticketgenehmigers. Diese Adresse ist besonders für E-Mail-Benachrichtigungen vom Typ *Kommentare* nützlich.
$ticket_approver_name	Der Name des Ticketgenehmigers. **HINWEIS:** Der Genehmigername und die Kontaktinformationen werden aus dem mit den Feldern des Tickets verknüpften Benutzerdatensatz abgeleitet.
$ticket_approver_phone_home	Kontaktinformationen für den Ticketgenehmiger.
$ticket_approver_phone_mobile	Kontaktinformationen für den Ticketgenehmiger.
$ticket_approver_phone_pager	Kontaktinformationen für den Ticketgenehmiger.
$ticket_approver_phone_work	Kontaktinformationen für den Ticketgenehmiger.
$ticket_custom_X_label $ticket_custom_X_value	Label und Wert für ein benutzerdefiniertes Feld, wobei **X** die Indexnummer des benutzerdefinierten Felds repräsentiert. Wenn z. B. eine Warteschlange ein Ticketfeld mit dem Label *CUSTOM_5* enthält und das Feld mit dem Label *Standortname* konfiguriert wird, ersetzt das System `$ticket_custom_5_label` mit dem Text `Standortname`. Das Token

Token	Beschreibung
	`$ticket_custom_5_value` wird mit dem Ticketwert ersetzt, der für das Feld *Standortname* gespeichert worden ist, z. B. *Topeka* oder *Albuquerque*. Standardmäßig werden alle Ticketwarteschlangen mit 15 benutzerdefinierten Feldern konfiguriert. Diese Anzahl kann jedoch nach Bedarf erhöht werden. **HINWEIS:** Jede Warteschlange kann unterschiedliche benutzerdefinierte Felder und E-Mail-Vorlagen-Konfigurationen haben.
$ticket_due_date	Das im Ticket gespeicherte Fälligkeitsdatum. Administratoren können gegebenenfalls automatische Fälligkeitsdaten durch manuelle Fälligkeitsdaten außer Kraft setzen.
$ticket_escalation_minutes	Die Uhrzeit zwischen regelmäßigen Benachrichtigungen in Minuten. Diese Uhrzeit wird durch die für die Ticketpriorität in der Warteschlange konfigurierte Eskalationszeit bestimmt. Wenn z. B. Tickets mit der Priorität **Hoch** eine Eskalationszeit von 30 Minuten haben, wird diese E-Mail für Tickets hoher Priorität alle 30 Minuten gesendet, bis die Ticketpriorität geändert oder das Ticket abgeschlossen wird. Dieses Token wird in der Regel in der E-Mail-Vorlage "Ticket eskaliert" verwendet, um die Empfänger über die Häufigkeit der E-Mail-Benachrichtigungen zu informieren.

$ticket_fields_visible	Enthält alle Ticketfelder, die für den Benutzer sichtbar sind, der das Ticket per E-Mail weiterleitet.
	TIPP: Wenn Sie HTML/Markdown verwenden, muss das Token "$ticket_fields_visible" mit dem Tag `<pre>` umschlossen werden, um zu verhindern, dass Formatierungen wie Zeilenumbrüche verworfen werden. Beispiel:
	`<pre>$ticket_fields_visible</pre>`

$ticket_history	Der vollständige Ticketverlauf. **HINWEIS:** Bei einigen Tickets können die Verlaufsinformationen sehr detailliert und für das Versenden per E-Mail zu groß werden. Wenn nicht der gesamte Verlauf benötigt wird, können Sie `$ticket_history_X` zur Beschränkung der Anzahl der einzubeziehenden Datensätze verwenden.
$ticket_history_X	Eine angegebene Anzahl von Datensätzen im Ticketverlauf. `X` gibt die Anzahl der einzubeziehenden Datensätze beginnend mit dem zuletzt erstellten Datensatz an.

Token	Beschreibung
$ticket_id	Ein dem Ticket zugewiesener eindeutiger Bezeichner, der auch als Ticketnummer bezeichnet wird. Die Identifizierung von Tickets durch die Benutzer erfolgt hauptsächlich anhand dieses Bezeichners.
$ticket_number	Eine formatierte Version der Ticket-ID. Diese Version beginnt mit `TICK`, gefolgt von mindestens fünf Ziffern. Ein Ticket mit der ID `4321` wird z. B. als `TICK:04321` angezeigt. Dieses Format ist besonders in Betreffzeilen von E-Mails nützlich, um zu gewährleisten, dass sich E-Mail-Antworten auf die korrekten Tickets beziehen.
$ticket_owner_email	Die E-Mail-Adresse des dem Ticket zugewiesenen Service Desk-Administrators.
$ticket_owner_name	Der Name des dem Ticket zugewiesenen Service Desk-Administrators. **HINWEIS:** Der Besitzername und die Kontaktinformationen werden aus dem mit den Feldern des Tickets verknüpften Benutzerdatensatz abgeleitet.
$ticket_owner_phone_home	Die Kontaktinformationen des dem Ticket zugewiesenen Service Desk-Administrators.
$ticket_owner_phone_mobile	Die Kontaktinformationen des dem Ticket zugewiesenen Service Desk-Administrators.
$ticket_owner_phone_pager	Die Kontaktinformationen des dem Ticket zugewiesenen Service Desk-Administrators.
$ticket_owner_phone_work	Die Kontaktinformationen des dem Ticket zugewiesenen Service Desk-Administrators.
$ticket_priority	Die dem Ticket zugewiesene Priorität. Standardwerte sind "Hoch", "Mittel" und "Niedrig".
$ticket_resolution	Informationen darüber, was zur Auflösung des Tickets unternommen wurde, gemäß der Beschreibung im Ticketfeld *Auflösung*.
$ticket_status	Der Status des Tickets. Standardwerte sind "Neu", "Eröffnet", "Abgeschlossen", "Weitere Infos erforderlich", "Erneut geöffnet", "Warten - überfällig", "Warten auf Kunde" und "Warten auf Drittanbieter".
$ticket_submitter_email	Die E-Mail-Adresse des Absenders.
$ticket_submitter_name	Der Name des Absenders.

Token	Beschreibung
	HINWEIS: Der Absendername und die Kontaktinformationen werden aus dem mit den Feldern des Tickets verknüpften Benutzerdatensatz abgeleitet.
$ticket_submitter_phone_home	Kontaktinformationen für den Absender.
$ticket_submitter_phone_mobile	Kontaktinformationen für den Absender.
$ticket_submitter_phone_pager	Kontaktinformationen für den Absender.
$ticket_submitter_phone_work	Kontaktinformationen für den Absender.
$ticket_title	Der Titel des Tickets entsprechend der Anzeige auf der Seite *Details zum Ticket*.
$ticket_url	Ein Link zum Ticket in der **Benutzerkonsole**. Für den Zugriff auf die **Benutzerkonsole** sind die Anmeldeinformationen erforderlich.
$ticket_http_url	Ein Link zum Ticket in der **Benutzerkonsole**. Dieses Format wird zur Gewährleistung der Abwärtskompatibilität auf älteren Systemen verwendet. Für den Zugriff auf die **Benutzerkonsole** sind die Anmeldeinformationen erforderlich.
$ticket_https_url	Ein sicherer Link zum Ticket in der **Benutzerkonsole**. Verwenden Sie dieses Token, wenn auf Ihrer Appliance SSL aktiviert ist. Dadurch wird gewährleistet, dass per E-Mail versendete Links ordnungsgemäß funktionieren.
$userui_url	Ein Link zur Startseite der **Benutzerkonsole**. Für den Zugriff auf die **Benutzerkonsole** sind die Anmeldeinformationen erforderlich.

Token, die in E-Mail-Vorlagen für zusammengeführte Tickets verwendet werden

Token	Beschreibung
$ticket_merged_number	Die Nummer des zusammengeführten Tickets
$ticket_merged_title	Der Titel des zusammengeführten Tickets entsprechend der Anzeige auf der Seite *Details zum Ticket*.
$ticket_merged_changer_name	Der Name des Benutzers, der die Tickets zusammengeführt hat.
$ticket_merged_url	Ein Link zum zusammengeführten Ticket in der **Benutzerkonsole**. Für den Zugriff auf die **Benutzerkonsole** sind die Anmeldeinformationen erforderlich.

In fehlerbezogenen E-Mail-Vorlagen verwendete Token

Token	Beschreibung
$error_text	Dient zur Angabe eines Problems bei der Verarbeitung der gesendeten Token. Dieser Fehler erscheint, wenn: • das System eine Variable nicht erkennt • eine Variable erkannt wird, aber der Benutzer nicht über die Berechtigung zum Ändern des Felds verfügt • die Variable versucht, den Genehmigungsstatus zu ändern, aber der Benutzer nicht der Genehmiger ist
$quoted_mail	Der Inhalt der ursprünglichen E-Mail-Nachricht.
$subject	Der Betreff der ursprünglichen E-Mail-Nachricht.

HINWEIS: Ungültige Token in E-Mail-Nachrichten werden ignoriert und nicht ersetzt. Wenn Sie z. B. ein unbekanntes Token wie `$today` hinzufügen, wird es ignoriert und in der E-Mail-Nachricht als `$today` angezeigt.

5. **Optional**: Erstellen Sie für jede Vorlage HTML-basierte Inhalte, anstelle von Nur-Text-Inhalten.
   a. Wählen Sie **Als HTML senden**, um eine einfache HTML-basierte E-Mail statt Nur-Text zu verwenden.

      Ein HTML-Editor mit einer umfassenden Reihe von Bearbeitungsoptionen zum Formatieren Ihrer Inhalte, wie Schaltflächen für fettgedruckten Text, Hyperlinks, Listen oder Textfarbe, wird angezeigt.

   b. Verwenden Sie die Steuerelemente im Editor zum Formatieren des Vorlageninhalts. Beispiel:

   - Um Fettdruck auf eine Textfolge anzuwenden, wählen Sie diese im Editor aus und klicken auf B.
   - Um Bilder hinzuzufügen, klicken Sie auf , und geben Sie die URL der Bilddatei oder einen lokalen Dateipfad an, oder legen Sie das Bild einfach in dem angegebenen Bereich ab.
     - Sie können Screenshots auch kopieren und direkt in das Textfeld einfügen.
     - Alle Bilder, die Sie auf diese Weise einfügen, werden als Dateianhänge zum Ticket hinzugefügt. Sie sind gegebenenfalls auch in der E-Mail-Kommunikation enthalten.
     - Wenn Sie ein Bild aus dem Textfeld löschen, wird der zugehörige Dateianhang nicht entfernt. Dateianhänge können Sie im Abschnitt *Anlage* der Ticket-Seite verwalten. Weitere Informationen hierzu finden Sie unter Screenshots und Anhänge zu Service-Desk-Tickets hinzufügen oder aus ihnen löschen.
   - Um externe Links hinzuzufügen, klicken Sie auf .
   - Um extern gehostete Videos einzubetten, klicken Sie auf .

   c. Um schnell ein Token hinzuzufügen, klicken Sie auf $, und wählen Sie in der angezeigten Liste das entsprechende Token aus.

   Weitere Informationen zu den einzelnen Token finden Sie in Schritt 4.

6. Klicken Sie auf **Speichern**.

Anweisungen zur Konfiguration der Appliance für die Verwendung von SMTP-E-Mails finden Sie unter Konfigurieren von SMTP-E-Mail-Servern.

CC-Listen für Ticketkategorien konfigurieren

Sie können Benutzer bzw. Benutzergruppen automatisch benachrichtigen, wenn in angegebenen Kategorien, z. B. Hardware, Software oder Netzwerk, Tickets abgelegt werden. Fügen Sie dazu die entsprechenden E-Mail-Adressen zum Wert *CC-Liste* jeder einzelnen Ticketkategorie hinzu.

Die Konfiguration der Werte *CC-Liste* ist hilfreich, wenn Sie Benutzer bzw. Benutzergruppen benachrichtigen möchten, wenn Tickets in Kategorien abgelegt werden, die sie interessieren. Zum Beispiel könnten Sie alle Systemadministratoren zur *CC-Liste* der Kategorie "Netzwerk" hinzufügen, damit diese bei Netzwerkproblemen benachrichtigt werden.

Wenn Sie mehrere Warteschlangen haben, konfigurieren Sie die Werte der *CC-Liste* der Ticketkategorie für jede Warteschlange separat.

1. Rufen Sie die Seite *Warteschlangen-Detail* des Service Desks auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Service Desk** und anschließend auf **Konfiguration**.
   c. Klicken Sie im Fensterbereich **Konfiguration** auf **Warteschlangen**.
   d. Führen Sie eine der folgenden Aktionen aus, um die Seite mit den *Warteschlangendetails* anzuzeigen:
   - Klicken Sie auf den Namen einer Warteschlange.
   - Wählen Sie **Aktion auswählen** > **Neu**.
2. Aktivieren Sie im Abschnitt *E-Mail bei Ereignissen* alle Kontrollkästchen in der Spalte *Kategorie CC*. Siehe E-Mail-Auslöser konfigurieren.
3. Klicken Sie auf **Speichern**.
4. Klicken Sie im Abschnitt *Standardwerte für Tickets* auf **Diese Werte anpassen**.
5. Fügen Sie im Abschnitt *Kategoriewerte* den Einträgen der *CC-Liste* E-Mail-Adressen hinzu:
   a. Klicken Sie in einer Kategoriezeile auf die Schaltfläche **Bearbeiten**. .
   b. Geben Sie im Feld *CC-Liste* eine Standard-E-Mail-Adresse für die Kategorie ein. Trennen Sie E-Mail-Adressen durch Kommas. Verwenden Sie zum Eingeben mehrerer E-Mail-Adressen gegebenenfalls einen Verteiler.
   c. Klicken Sie am Ende der Zeile auf **Speichern**.
   d. Wiederholen Sie den Vorgang, um Einträge der *CC-Liste* für weitere Kategorien hinzuzufügen.
6. Klicken Sie unten auf der Seite auf **Speichern**.

Erstellen Sie eine Standard-E-Mail-Adresse für Ticketbesitzer. Siehe Konto "DefaultTicketOwners" erstellen.

E-Mail-Adressen automatisch zu Ticket-CC-Listenfeldern hinzufügen

Sie können angeben, dass Service Desk E-Mail-Adressen automatisch zum Feld *CC-Liste* von Tickets hinzufügen soll, wenn diese Adressen in den Feldern *An* und *Cc* von per E-Mail gesendeten oder aktualisierten Tickets enthalten sind.

Wenn diese Einstellung aktiviert ist, werden in den Feldern *An* und *Cc* enthaltene E-Mail-Adressen automatisch zum Feld *CC-Liste* von Tickets hinzugefügt, wenn diese Adressen nicht in der *System-E-Mail-Ausschlussliste* enthalten sind. Siehe Adressen aus Ticket-CC-Listenfeldern ausschließen.

HINWEIS: Wenn Ihr Service Desk auf einer Appliance mit Version 6.3 oder früher erstellt worden ist, ist diese Einstellung standardmäßig deaktiviert. Wenn die Organisationskomponente auf Ihrem System aktiviert ist und Sie eine neue Organisation erstellen, wird die Einstellung jedoch standardmäßig aktiviert. Auch auf neuen KACE SMAs mit Version 6.4 oder höher ist die Einstellung aktiviert.

1. Rufen Sie die Seite *Einstellungen* des Service Desks auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Service Desk** und anschließend auf **Konfiguration**.
   c. Klicken Sie im Fensterbereich *Konfiguration* auf **Einstellungen**.
2. Aktivieren Sie im Abschnitt *Eingehende E-Mail* das Kontrollkästchen neben *E-Mail-Adressen aus CC-Liste zum Ticket hinzufügen*.
3. Klicken Sie auf **Speichern**.

Konfigurieren Sie die E-Mail-Ausschlussliste, um zu verhindern, dass Service Desk automatisch unerwünschte E-Mail-Adressen zum Feld *CC-Liste* von Tickets hinzufügt. Siehe Adressen aus Ticket-CC-Listenfeldern ausschließen.

Adressen aus Ticket-CC-Listenfeldern ausschließen

Service Desk kann automatisch E-Mail-Adressen zu Feldern der *CC-Liste* hinzufügen, wenn Tickets werden per E-Mail gesendet oder aktualisiert werden. Bestimmte Adressen wie Verteilerlisten und allgemeine E-Mail-Adressen im Unternehmen sollten nicht automatisch hinzugefügt werden, weil sie das E-Mail-Aufkommen nur unnötig belasten. Damit Service Desk keine unerwünschten E-Mail-Adressen hinzufügt, können Sie angeben, welche E-Mail-Adressen ausgeschlossen werden sollen.

Die E-Mail-Ausschlussliste ist eine Einstellung auf Appliance-Ebene. Wenn die Organisationskomponente auf der Appliance aktiviert ist, wird die E-Mail-Ausschlussliste auf alle Organisationen und Service Desk-Warteschlangen angewendet.

HINWEIS: Die Service Desk-Warteschlangen zugeordneten E-Mail-Adressen werden niemals automatisch zu Feldern der *CC-Liste* hinzugefügt, weil das Senden von Nachrichten an diese Adressen zur versehentlichen Eröffnung neuer Tickets führen könnte. Sie müssen diese Adressen nicht zur Ausschlussliste hinzuzufügen.

1. Rufen Sie die Seite *Einstellungen* des Service Desks auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Service Desk** und anschließend auf **Konfiguration**.
   c. Klicken Sie im Fensterbereich *Konfiguration* auf **Einstellungen**.
2. Klicken Sie im Abschnitt *Eingehende E-Mail* auf **E-Mail-Ausschlussliste des Systems definieren**, um die gleichnamige Seite *E-Mail-Ausschlussliste des Systems definieren* anzuzeigen.
3. Zum Hinzufügen einer E-Mail-Adresse zur Liste klicken Sie auf "Hinzufügen": +.
4. Im Dialogfeld *E-Mail hinzufügen* geben Sie eine E-Mail-Adresse ein und klicken auf **Speichern**.

   Die E-Mail-Adresse wurde in die Ausschlussliste aufgenommen.

Verhindern von E-Mail-Schleifen

Wenn Tickets per E-Mail eingereicht oder aktualisiert werden, sendet das Service Desk Ticket-Benachrichtigungen an die jeweiligen Parteien. Falls jedoch ein Benutzer, der eine solche E-Mail-Antwort mit einer automatischen *Abwesenheits*-Antwort erhält, reagiert das Service Desk mit einer weiteren Ticket-Aktualisierung und einer weiteren E-Mail-Benachrichtigung, wodurch potenziell eine endlose E-Mail-Schleife entstehen kann.

Sie können verhindern, dass das Service Desk bei Eingang einer Abwesenheits-Antwort E-Mails bearbeitet. Weiterhin können Sie das Senden von E-Mail-Benachrichtigungen stoppen, wenn eine hohe Anzahl eingehender E-Mails erkannt wird, die sich auf Tickets beziehen. Alle E-Mails, die bewirken, dass dass das Service Desk keine weiteren E-Mail-Benachrichtigungen versendet, werden protokolliert.

1. Rufen Sie die Seite *Service Desk, E-Mail-Voreinstellungen* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Service Desk** und anschließend auf **Konfiguration**.
   c. Klicken Sie im Fensterbereich **Konfiguration** im Abschnitt *E-Mail-Konfiguration* auf **Service Desk E-Mail-Voreinstellungen konfigurieren**.
2. Geben Sie den Text an, der im E-Mail-Betreff erkannt werden soll. Wenn beim Service Desk eine auf ein Ticket bezogene E-Mail mit der entsprechenden Betreffzeile eingeht, wird diese E-Mail nicht weiter bearbeitet.
   a. Geben Sie im Abschnitt *Eingehende E-Mail* im Feld *E-Mails mit folgendem Text im Betreff ignorieren* die Worte ein, die Sie entdecken möchten. Sie können mehrere Einträge angeben, die durch ein Semikolon voneinander getrennt sind. Beispiel: Abwesend;Fehlgeschlagene Mailzustellung.
3. Konfigurieren Sie die Schwellenwerte für alle eingehenden E-Mail-Benachrichtigungen während eines bestimmten Zeitraums. Wenn diese Schwellenwerte erreicht sind, sendet das Service Desk keine weiteren E-Mail-Benachrichtigungen.

   HINWEIS: Wenn der Gesamtschwellenwert erreicht wird, wird das Senden von Benachrichtigungen für alle Tickets unterbrochen. Wenn der Schwellenwert für ein einzelnes Ticket erreicht wird, wird das Senden von Benachrichtigungen nur für das betroffene Ticket unterbrochen. Wenn die Anzahl an E-Mail-Updates im vorgegebenen Zeitraum geringer als der konfigurierte Schwellenwert ist, wird das Senden von Benachrichtigungen fortgesetzt.

Option	Beschreibung
E-Mails gesamt	Die maximale Anzahl aller E-Mails, die das Service Desk empfängt und mit E-Mail-Benachrichtigungen beantwortet. Der Standardwert beträgt 100 E-Mails.
Innerhalb von x Minuten erhalten	Das Zeitintervall in Minuten, während derer die angegebene Anzahl von E-Mails empfangen werden. Der Standardwert beträgt eine Minute. Um diese Beschränkung aufzuheben, können Sie eine hohe Zahl wie 99999 einstellen.

4. Konfigurieren Sie die Schwellenwerte für eingehende E-Mail-Benachrichtigungen pro Ticket während eines bestimmten Zeitraums. Wenn diese Schwellenwerte erreicht sind, sendet das Service Desk keine weiteren E-Mail-Benachrichtigungen.

Option	Beschreibung
Gesamtzahl der E-Mails pro Ticket	Die maximale Anzahl aller E-Mails, die das Service Desk für jedes Ticket empfängt und mit E-Mail-Benachrichtigungen beantwortet. Der Standardwert beträgt 5 E-Mails pro Ticket.
Innerhalb von x Minuten erhalten	Geben Sie das Zeitintervall in Minuten ein, während dessen die angegebene Anzahl von E-Mails für jedes Ticket empfangen werden. Der Standardwert beträgt eine Minute. Um diese Beschränkung aufzuheben, stellen Sie eine hohe Zahl wie 99999 ein.

5. Klicken Sie auf **Speichern**.

Konfigurieren der Cache-Lebensdauer für Service Desk-Widgets

Auf der Seite *Dashboard* verfügbare Service Desk-Widgets bieten einen Einblick in die allgemeine Aktivität Ihrer Service Desk-Tickets. Sie können beispielsweise die Anzahl der aktiven Tickets sortiert nach Kategorie oder Warteschlange anzeigen. Aus Leistungsgründen werden zugrundeliegende Daten für die Service Desk-Widgets für einen festgelegten Zeitraum lokal im Cache gespeichert. Der Standardwert lautet 30 Minuten. Dieser Wert kann nach Bedarf erhöht werden. Sie können eine Datenaktualisierung für ein bestimmtes Widget erzwingen, indem Sie auf das Aktualisierungssymbol im Widget klicken.

Weitere Informationen zu *Dashboard*-Widgets finden Sie unter Informationen zu Dashboard-Widgets.

1. Rufen Sie die Seite *Einstellungen* des Service Desks auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Service Desk** und anschließend auf **Konfiguration**.
   c. Klicken Sie im Fensterbereich *Konfiguration* auf **Einstellungen**.
2. Geben Sie unter *Service Desk Dashboard Widgets* im Feld *Cache-Speicherdauer* die Zeit in Minuten an, während der die Daten, die die Service Desk-Dashboard-Widgets ausfüllen, in der Datenbank gespeichert werden. Das Minimum beträgt 30 Minuten.
3. Klicken Sie auf **Speichern**.

Erstellen und Verwalten von Organisationen

Wenn die Komponente **Organisation** auf Ihrer Appliance aktiviert ist, können Sie separate Organisationen mit separaten Inventaren und Einstellungen erstellen und verwalten, um Ihre geschäftlichen Anforderungen zu erfüllen.

TIPP: Wenn die Organisationskomponente auf Ihrer Appliance aktiviert ist, die Dropdown-Liste jedoch nicht oben rechts in der **Administratorkonsole** neben den Anmeldeinformationen zu sehen ist, gibt es zwei Möglichkeiten: Entweder ist die Option Schneller Wechsel nicht aktiviert oder Ihre Benutzerrolle hat keine Berechtigung zur Verwaltung von Organisationen.

TIPP: Siehe Schnellen Wechsel von Organisationen und verknüpften Appliance aktivieren.

Informationen zu Organisationen

Organisationen sind all die logischen Instanzen einer Appliance, die auf einer einzelnen Appliance ausgeführt werden. Jede Organisation wird von einer eigenen Datenbank unterstützt und Sie verwalten das Inventar jeder Organisation und andere Komponenten getrennt voneinander.

In einer schulischen Umgebung könnten Sie beispielsweise eine Organisation für Lehrer und eine andere für Schüler erstellen. Dann könnten Sie den einzelnen Organisationen automatisch verwaltete Geräte zuweisen und diese separat verwalten. Weiterhin können Sie Administratoren und Benutzern organisationsspezifische Rollen zuweisen, um deren Zugang zur **Administratorkonsole** und **Benutzerkonsole** der Appliance zu regeln. Administratoren in einer Organisation müssten dann die Geräte und Inventarelemente in der anderen Organisation nicht anzeigen. Sie können pro Appliance bis zu 50 Organisationen hinzufügen.

Informationen zum Konfigurieren allgemeiner Organisationseinstellungen für die Appliance finden Sie unter Allgemeine Appliance-Einstellungen bei aktivierter Organisationskomponente konfigurieren.

Informationen zur Standardorganisation

Die Organisation mit dem Namen **Standard** ist die einzige Organisation, die bei der ersten Einrichtung der Appliance verfügbar ist. Neue Geräte, die nicht über einen Filter einer Organisation zugewiesen werden, werden der Standardorganisation zugewiesen.

Sie können die Standardorganisation umbenennen und ihre Einstellungen nach Bedarf ändern. Siehe Organisationen hinzufügen oder bearbeiten.

Verfolgen von Änderungen an Organisationseinstellungen

Wenn Verlaufsabonnements zur Aufbewahrung von Informationen konfiguriert wurden, können Sie Details zu den an Einstellungen, Assets und Objekten vorgenommenen Änderungen anzeigen.

Diese Informationen beinhalten auch das Datum der Änderung und den Benutzer, der diese vorgenommen hat. Dies kann bei der Fehlerbehebung nützlich sein. Siehe Informationen zu den Verlaufseinstellungen.

Verwalten von Organisationsrollen und Benutzerrollen

Wenn die Organisationskomponente in Ihrer Appliance aktiviert ist, stehen zwei Arten von Rollen zur Verfügung: Organisationsrollen, die auf Organisationen angewendet werden, und Benutzerrollen, die auf einzelne Benutzerkonten angewendet werden.

Wenn die Organisationskomponente in Ihrer Appliance aktiviert ist, stehen zwei Arten von Rollen zur Verfügung: Organisationsrollen, die auf Organisationen angewendet werden, und Benutzerrollen, die auf einzelne Benutzerkonten angewendet werden.

In diesem Abschnitt werden die standardmäßigen Organisations- und Benutzerrollen beschrieben und die Verwaltung von Organisationsrollen erläutert. Informationen zum Verwalten von Benutzerrollen finden Sie unter Informationen zu Benutzerkonten und Benutzerauthentifizierung.

Verfügbare Standardrollen

Standardrollen bieten eine Vielzahl von Berechtigungseinstellungen für Organisationen und Benutzer.

Folgende Optionen sind standardmäßig verfügbar:

Rolle	Beschreibung
Organisationsrollen	Organisationsrollen sind Berechtigungsgruppen, die Organisationen zugewiesen werden, und anhand derer die Berechtigungen festgelegt werden, die für die Benutzer in den jeweiligen Organisationen verfügbar sind. Wird einer Organisation beispielsweise eine Organisationsrolle zugewiesen, bei der die Registerkarte *Verteilung* ausgeblendet ist, können die Benutzer in dieser Organisation, einschließlich des Admin-Benutzers, nicht auf die Registerkarte *Verteilung* zugreifen. **HINWEIS:** Organisationsrollen sind nur in Appliances mit aktivierter Organisationskomponente verfügbar.
Standardrolle	Die Standardrolle im Abschnitt über Organisationsrollen verfügt über Schreib- und Leseberechtigungen für alle Registerkarten. Sie können die Standardrolle zwar nicht bearbeiten oder löschen, aber stattdessen zusätzliche Organisationsrollen erstellen.
Benutzerrollen	Benutzern zugewiesene Rollen, um deren Zugang zur **Administratorkonsole** und **Benutzerkonsole** zu steuern. Wenn die Organisationskomponente in Ihrer Appliance aktiviert ist, sind die zu diesen Rollen verfügbaren Berechtigungen von der Organisationsrolle abhängig, die einer Organisation zugewiesen ist.
Administrator	Dies ist die Benutzerrolle mit den umfassendsten Berechtigungen in der Appliance. Benutzer mit der **Administrator**rolle können standardmäßig Informationen und Einstellungen anzeigen und ändern. Hierzu zählt auch das Hoch- oder Herabstufen anderer Benutzer durch Ändern ihrer Rollen. Die **Administrator**rolle kann weder geändert noch gelöscht werden. Weisen Sie diese Rolle nur vertrauenswürdigen Administratoren zu. Mitarbeiter, denen die **Administratorrolle** zugewiesen wurde, sind berechtigt, Service-Desk-Tickets auf der Registerkarte *Tickets* in der **Administratorkonsole** zu verwalten und zu ändern, obwohl sie selbst möglicherweise keine Tickets besitzen dürfen.

Rolle	Beschreibung
	Benutzer mit der **Administrator**rolle können außerdem die Sicherheits-, Skripterstellungs- und Verteilungsfunktionen zur Auflösung von Service-Desk-Tickets verwenden und die Probleme anschließend in der Knowledge Base dokumentieren. Die Rolle des **Administrators** interagiert vor allem über die **Administratorkonsole** mit der Appliance.
Kein Zugriff	Benutzer mit dieser Rolle können sich nicht bei der **Administratorkonsole** oder **Benutzerkonsole** anmelden.
Administrator mit Leseberechtigung	Diese Rolle berechtigt Inhaber dazu, Informationen oder Einstellungen in der Appliance anzuzeigen, jedoch nicht dazu, sie zu ändern. Sie eignet sich für Mitarbeiter mit Überwachungsfunktion, wie beispielsweise Vorgesetzte. Diese Rolle interagiert vor allem über die **Administratorkonsole** mit der Appliance.
Nur Benutzerkonsole	Diese Rolle ist für Appliance-Benutzer gedacht. Sie enthält standardmäßig die Berechtigung, Service-Desk-Tickets zu erstellen, anzuzeigen oder zu ändern. Diese Rolle interagiert ausschließlich über die **Benutzerkonsole** mit der Appliance.

Organisationsrollen hinzufügen und bearbeiten

Sie können Organisationsrollen nach Bedarf hinzufügen oder bearbeiten.

Bevor Sie Organisationen erstellen, sollten Sie die Organisationsrollen erstellen, die Sie diesen Organisationen zuweisen möchten, wie in diesem Abschnitt beschrieben. Anhand von Organisationsrollen werden die Berechtigungen festgelegt, die für Benutzer in Organisationen verfügbar sind.

1. Rufen Sie die Seite *Detail zur Rolle der Organisation* auf:
   a. Melden Sie sich bei der Systemadministratorkonsole der Appliance an: `http://`**appliance_hostname**`/system`. Oder wählen Sie in der Dropdown-Liste rechts oben auf der Seite den Eintrag **System** aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Organisationen** und anschließend auf **Rollen**.
   c. Führen Sie eine der folgenden Aktionen aus, um die Seite *Detail zur Rolle der Organisation* anzuzeigen:
   - Klicken Sie auf den Namen einer Rolle.
   - Wählen Sie **Aktion auswählen** > **Neu**.

   HINWEIS: Die Standardrolle können Sie nicht bearbeiten.

2. Geben Sie die folgenden Informationen an:

Option	Beschreibung
Name	(Erforderlich) Geben Sie einen Namen für die Rolle ein.
Beschreibung	(Optional) Geben Sie eine Beschreibung für die Rolle ein.

3. So weisen Sie Berechtigungen in der Administratorkonsole zu:
   - **Klicken Sie in der Administratorkonsole im Abschnitt** *Berechtigungen* **auf einen Komponentennamen, um ihn zu erweitern, oder klicken Sie auf Alle erweitern, um alle Komponenten zu erweitern.**
   - **Um allen Abschnitten dieselbe Zugriffsebene zuzuweisen, wählen Sie Alle schreiben, Alle lesen oder Alle ausblenden aus.**
   - **Um verschiedenen Abschnitten unterschiedliche Zugriffsebenen zuzuweisen, wählen Sie die Option Benutzerdefiniert aus und wählen anschließend in der Dropdown-Liste neben dem jeweiligen Abschnittsnamen eine Zugriffsebene aus.**
4. So weisen Sie Berechtigungen in der Benutzerkonsole zu:
   - **Klicken Sie in der Benutzerkonsole im Abschnitt** *Berechtigungen* **auf den Link für die Benutzerkonsole, um den Abschnitt der Berechtigungen zu erweitern.**
   - **Um allen Abschnitten der Benutzerkonsole dieselbe Zugriffsebene zuzuweisen, wählen Sie Alle schreiben, Alle lesen oder Alle ausblenden aus.**
   - **Um verschiedenen Abschnitten unterschiedliche Zugriffsebenen zuzuweisen, wählen Sie die Option Benutzerdefiniert aus und wählen anschließend in der Dropdown-Liste neben dem jeweiligen Abschnittsnamen eine Zugriffsebene aus.**
5. Klicken Sie auf **Speichern**.

   HINWEIS: Wenn Sie für **Allgemein** die Berechtigung **Ausblenden** und unter **Einstellungen** die Option *Benutzerauthentifizierung* zuweisen, wird die *Systemsteuerung* ausgeblendet.

Die Rolle wird auf der Seite *Rollen* angezeigt. Wenn Sie eine Organisation hinzufügen, wird die Rolle in der Dropdown-Liste *Rolle* angezeigt. Siehe Hinzufügen, Bearbeiten und Löschen von Organisationen.

Organisationsrollen duplizieren

Wenn Sie eine Organisationsrolle duplizieren, werden deren Eigenschaften in die neue Rolle kopiert. Wenn Sie Rollen erstellen möchten, die bereits bestehenden Rollen ähnlich sind, können Sie durch das Duplizieren von Rollen Zeit sparen.

1. Rufen Sie die Seite *Detail zur Rolle der Organisation* auf:
   a. Melden Sie sich bei der Systemadministratorkonsole der Appliance an: `http://`**appliance_hostname**`/system`. Oder wählen Sie in der Dropdown-Liste rechts oben auf der Seite den Eintrag **System** aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Organisationen** und anschließend auf **Rollen**.
   c. Klicken Sie auf den Namen einer Rolle.
2. Klicken Sie unten auf der Seite auf **Duplizieren**, um die Organisationsdetails zu duplizieren.

   Die Seite wird aktualisiert.
3. Geben Sie die folgenden Informationen an:

Option	Beschreibung
Name	(Erforderlich) Geben Sie einen Namen für die Rolle ein.

Option	Beschreibung
Beschreibung	(Optional) Geben Sie eine Beschreibung für die Rolle ein.

4. So weisen Sie Berechtigungen in der Administratorkonsole zu:
   - **Klicken Sie in der Administratorkonsole im Abschnitt** *Berechtigungen* **auf einen Komponentennamen, um ihn zu erweitern, oder klicken Sie auf Alle erweitern, um alle Komponenten zu erweitern.**
   - **Um allen Abschnitten dieselbe Zugriffsebene zuzuweisen, wählen Sie Alle schreiben, Alle lesen oder Alle ausblenden aus.**
   - **Um verschiedenen Abschnitten unterschiedliche Zugriffsebenen zuzuweisen, wählen Sie die Option Benutzerdefiniert aus und wählen anschließend in der Dropdown-Liste neben dem jeweiligen Abschnittsnamen eine Zugriffsebene aus.**
5. So weisen Sie Berechtigungen in der Benutzerkonsole zu:
   - **Klicken Sie in der Benutzerkonsole im Abschnitt** *Berechtigungen* **auf den Link für die Benutzerkonsole, um den Abschnitt der Berechtigungen zu erweitern.**
   - **Um allen Abschnitten der Benutzerkonsole dieselbe Zugriffsebene zuzuweisen, wählen Sie Alle schreiben, Alle lesen oder Alle ausblenden aus.**
   - **Um verschiedenen Abschnitten unterschiedliche Zugriffsebenen zuzuweisen, wählen Sie die Option Benutzerdefiniert aus und wählen anschließend in der Dropdown-Liste neben dem jeweiligen Abschnittsnamen eine Zugriffsebene aus.**
6. Klicken Sie auf **Speichern**.

Rollen löschen

Mit Ausnahme der Standardrolle können Sie Organisationsrollen nach Bedarf löschen. Die Standardrolle und Rollen, die einer Organisation zugewiesen sind, können Sie jedoch nicht löschen.

Die folgenden Rollen können nicht gelöscht werden:

- die Standardrolle
- alle Rollen, die einer Organisation zugewiesen sind
- alle Rollen mit einem verknüpften Label

1. Rufen Sie die Liste *Rollen* auf:
   a. Melden Sie sich bei der Systemadministratorkonsole der Appliance an: `http://`**appliance_hostname**`/system`. Oder wählen Sie in der Dropdown-Liste rechts oben auf der Seite den Eintrag **System** aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Organisationen** und anschließend auf **Rollen**.
2. Aktivieren Sie das Kontrollkästchen neben mindestens einer Rolle.
3. Wählen Sie **Aktion auswählen** > **Löschen** und klicken Sie dann zum Bestätigen auf **Ja**.

Hinzufügen, Bearbeiten und Löschen von Organisationen

Sie können Organisationen nach Bedarf hinzufügen, bearbeiten oder löschen. Darüber hinaus können Sie die Standardorganisation umbenennen und ihre Einstellungen ändern.

Organisationen hinzufügen oder bearbeiten

Sie können pro Appliance bis zu 50 Organisationen hinzufügen oder bearbeiten.

Wenn Sie Organisationen hinzufügen, müssen Sie diesen Organisationsrollen zuweisen. Sie können dazu die Standardrolle verwenden. Wenn Sie jedoch eine benutzerdefinierte Organisationsrolle verwenden möchten, sollten Sie diese Rolle noch vor der neuen Organisation hinzufügen. Siehe Organisationsrollen hinzufügen und bearbeiten.

1. Rufen Sie die Seite *Organisationsdetail* auf:
   a. Melden Sie sich bei der Systemadministratorkonsole der Appliance an: `http://`**appliance_hostname**`/system`. Oder wählen Sie in der Dropdown-Liste rechts oben auf der Seite den Eintrag **System** aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Organisationen** und anschließend auf **Organisationen**.
   c. Führen Sie eine der folgenden Aktionen aus, um die Seite *Organisationsdetail* anzuzeigen:
   - Klicken Sie auf den Namen einer Organisation.
   - Wählen Sie **Aktion auswählen** > **Neu**.
2. Wenn Sie eine Organisation hinzufügen, geben Sie folgende Informationen ein und klicken Sie auf **Speichern**.

Option	Beschreibung
Name	Geben Sie einen Namen für die Organisation ein. Sie können den Namen gegebenenfalls später ändern. Wenn die Option *Schneller Wechsel* aktiviert ist, wird dieser Name in der Dropdown-Liste oben rechts auf der Seite angezeigt. Siehe Schnellen Wechsel von Organisationen und verknüpften Appliance aktivieren.
Beschreibung	Eine Beschreibung der Organisation. Sie können die Beschreibung gegebenenfalls später ändern.
Rolle	Die Benutzerrolle, die Sie der Organisation zuweisen möchten. Sie können die Auswahl gegebenenfalls später ändern. **HINWEIS:** Die Rolle erstellen Sie unter **Organisationen** > **Rollen**.
Client-Drop-Größe	Ein Dateigrößenfilter für den Client-Drop-Speicherort der Organisation. Der Client-Drop-Speicherort ist ein Speicherbereich (Samba-Freigabe) für die Organisation auf der Appliance. Dieser Speicherbereich dient zum Hochladen großer Dateien, z. B. von Installationsprogrammen für Anwendungen und Appliance-Sicherungsdateien, auf die Appliance. Das Hochladen von Dateien auf den Client-Drop-Speicherort ist eine Alternative zum Hochladen von Dateien über die **Administratorkonsole** mit dem Standard-HTTP-Mechanismus, bei dem es bei großen Dateien zu Browser-Timeouts kommen kann.

Option	Beschreibung
	Der Filter *Client-Drop-Größe* bestimmt, ob auf den Client-Drop-Speicherort der Organisation hochgeladene Dateien in der Liste *Client-Drop-Datei hochladen und verknüpfen* auf der Seite *Softwaredetail* angezeigt werden. Wenn der Filter „Client-Drop-Größe“ z. B. auf 1 GB eingestellt ist, werden in der Liste *Client-Drop-Datei hochladen und verknüpfen* Dateien angezeigt, die 1 GB oder größer sind. Dateien, die kleiner als 1 GB sind, werden in der Liste nicht angezeigt. Anwendungsdateien werden vom Client-Drop-Speicherort der Organisation zu dem entsprechenden Bereich verschoben, wenn die Datei auf der Seite *Softwaredetail* ausgewählt und gespeichert wird. Am Client-Drop-Speicherort abgelegte Appliance-Sicherungsdateien werden automatisch als Appliance-Sicherungsdateien erkannt und innerhalb von fünf Minuten auf der Seite *Sicherungseinstellungen* für die Auswahl verfügbar. Wenn Sie mehrere Organisationen haben, verfügt jede Organisation über ihren eigenen Client-Drop-Speicherort und eine eigene Filtereinstellung „Client-Drop-Größe“. Siehe Dateien kopieren und auf dem Client-Drop-Speicherort der Appliance ablegen.

3. Fügen Sie die folgenden Informationen hinzu, bearbeiten Sie diese oder zeigen Sie sie an:

Option	Beschreibung
Name	Ändern die den Namen der Organisation nach Bedarf. Wenn die Option *Schneller Wechsel* aktiviert ist, wird dieser Name in der Dropdown-Liste oben rechts auf der Seite angezeigt. Siehe Schnellen Wechsel von Organisationen und verknüpften Appliance aktivieren.
Gebietsschema	Die für die **Administratorkonsole** und **Benutzerkonsole** der Organisation zu verwendende Sprache.
Name des virtuellen Hosts	Ein eindeutiger Domänenname für die Organisation. Wenn dieses Feld konfiguriert ist und Sie sich vom angegebenen Standort aus bei der Appliance anmelden, wählt die Appliance diese Organisation automatisch aus, und Sie müssen nur Ihre Benutzeranmeldeinformationen angeben. Wenn Sie die SAML-Anmeldung (Security Assertion Markup Language) verwenden, werden Sie vom konfigurierten virtuellen Hostnamen direkt beim Identitätsanbieter (Identity Provider, IdP) dieser Organisation angemeldet. Weitere Informationen zur SAML-Anmeldung finden Sie unter SAML für die einmalige Anmeldung konfigurieren.

Option	Beschreibung
Virtual Host IP (IP des virtuellen Hosts)	Eine eindeutige IP-Adresse für diese Organisation. Wenn dieses Feld konfiguriert ist und Sie sich vom angegebenen Standort aus bei der Appliance anmelden, wählt die Appliance diese Organisation automatisch aus, und Sie müssen nur Ihre Benutzeranmeldeinformationen angeben. Wenn Sie die SAML-Anmeldung verwenden, werden Sie von der konfigurierten IP-Adresse des virtuellen Hosts direkt beim IdP (beim Identitätsanbieter) der Organisation angemeldet. Weitere Informationen zur SAML-Anmeldung finden Sie unter SAML für die einmalige Anmeldung konfigurieren.
Beschreibung	Eine Beschreibung der Organisation. Sie können die Beschreibung gegebenenfalls später ändern.
Datenbankname	(Schreibgeschützt) Zeigt den Namen der Datenbank an, welche die Organisation verwendet.
Benutzer für Berichterstellung	(Schreibgeschützt) Der zur Erstellung von Berichten verwendete Benutzername. Der Benutzername für die Berichterstellung ermöglicht Zugriff auf die Datenbank (und damit weitere Berichterstellungstools), jedoch ohne Schreibzugriff für den Benutzer.
Kennwort für Berichterstellung	Das Benutzerkennwort für Berichte. Dieses Kennwort wird nur vom Berichterstellungssystem und MySQL verwendet.
Rolle	Die Benutzerrolle, die Sie der Organisation zuweisen möchten. Sie können die Auswahl gegebenenfalls später ändern. **HINWEIS:** Die Rolle erstellen Sie unter **Organisationen** > **Rollen**.
Client-Drop-Größe	Ein Dateigrößenfilter für den Client-Drop-Speicherort der Organisation. Der Client-Drop-Speicherort ist ein Speicherbereich (Samba-Freigabe) für die Organisation auf der Appliance. Dieser Speicherbereich dient zum Hochladen großer Dateien, z. B. von Installationsprogrammen für Anwendungen und Appliance-Sicherungsdateien, auf die Appliance. Das Hochladen von Dateien auf den Client-Drop-Speicherort ist eine Alternative zum Hochladen von Dateien über die **Administratorkonsole** mit dem Standard-HTTP-Mechanismus, bei dem es bei großen Dateien zu Browser-Timeouts kommen kann. Der Filter *Client-Drop-Größe* bestimmt, ob auf den Client-Drop-Speicherort der Organisation hochgeladene Dateien in der Liste *Client-Drop-Datei hochladen und verknüpfen* auf der Seite

Option	Beschreibung
	Softwaredetail angezeigt werden. Wenn der Filter „Client-Drop-Größe“ z. B. auf 1 GB eingestellt ist, werden in der Liste *Client-Drop-Datei hochladen und verknüpfen* Dateien angezeigt, die 1 GB oder größer sind. Dateien, die kleiner als 1 GB sind, werden in der Liste nicht angezeigt. Anwendungsdateien werden vom Client-Drop-Speicherort der Organisation zu dem entsprechenden Bereich verschoben, wenn die Datei auf der Seite *Softwaredetail* ausgewählt und gespeichert wird. Am Client-Drop-Speicherort abgelegte Appliance-Sicherungsdateien werden automatisch als Appliance-Sicherungsdateien erkannt und innerhalb von fünf Minuten auf der Seite *Sicherungseinstellungen* für die Auswahl verfügbar. Wenn Sie mehrere Organisationen haben, verfügt jede Organisation über ihren eigenen Client-Drop-Speicherort und eine eigene Filtereinstellung „Client-Drop-Größe“. Siehe Dateien kopieren und auf dem Client-Drop-Speicherort der Appliance ablegen.
Filter	Die Filter, die Sie verwenden möchten, um der Organisation neue Geräte zuzuweisen, wenn diese sich bei der Appliance anmelden Um mehrere Filter auszuwählen, verwenden Sie **STRG**+Klicken oder **Befehlstaste**+Klicken.
Geräte	(Schreibgeschützt) Zeigt die Zahl der einer Organisation zugewiesenen Geräte an.

4. Legen Sie die folgenden Einstellungen fest:

> **HINWEIS:** Um die Auslastung der Appliance zu reduzieren, sollten Sie die Anzahl der Agenten-Verbindungen auf 500 pro Stunde begrenzen. Die Anzahl der Verbindungen, die neben den Inventarisierungs-, Skripterstellungs- und Erfassungsintervallen angezeigt wird, gilt nur für die aktuelle Organisation. Wenn die Organisationskomponente in Ihrer Appliance aktiviert ist, sollte die Gesamtzahl der Agenten-Verbindungen für alle Organisationen maximal 500 pro Stunde betragen.

Option	Empfohlene Einstellung	Anmerkungen
Agentenprotokollierung	Aktiviert	Gibt an, ob die Appliance Skriptergebnisse speichert, die von Agenten auf verwalteten Geräten übermittelt wurden. Agenten-Protokolle können in der Datenbank bis zu 1GB Speicherplatz benötigen. Wenn Speicherplatz keine Rolle spielt, aktivieren Sie die *Agentenprotokollierung*, um alle Protokollinformationen für vom Agenten verwaltete Geräte zu speichern. Diese Protokolle können bei der Fehlerbehebung nützlich sein. Um Speicherplatz zu sparen und eine schnellere

Option	Empfohlene Einstellung	Anmerkungen
		Kommunikation mit dem Agenten zu ermöglichen, deaktivieren Sie die *Agentenprotokollierung*.
Agent Debug Trace	Aktiviert	Wenn ausgewählt, ermöglicht Ihnen diese Option, den Debug-Verlauf des Agenten aufzuzeichnen. Anhand dieser Informationen können Administratoren die Leistung des Agenten überwachen und häufige Probleme diagnostizieren.
Agenten-Inventar	12 Stunden	Die Häufigkeit, mit der Agenten auf verwalteten Geräten das Inventar melden. Diese Informationen werden im Abschnitt *Inventar* angezeigt.
Inventar ohne Agent	1 Tag	Die Häufigkeit, mit Geräte ohne Agent Inventar melden. Diese Informationen werden im Abschnitt *Inventar* angezeigt.
Kataloginventarisierung	24 Stunden	Die Häufigkeit, mit der verwaltete Geräte der Seite *Softwarekatalog* das Inventar melden sollen.
Erfassung der Nutzung	4 Stunden	Die Häufigkeit, mit der verwaltete Geräte der Appliance Erfassungsinformationen melden sollen. Damit dies möglich ist, muss die Erfassung auf Geräten und in Anwendungen aktiviert sein.
Skriptaktualisierung	4 Stunden	Die Häufigkeit, mit der Agenten auf den verwalteten Geräten aktualisierte Skriptkopien anfordern sollen, die auf verwalteten Geräten verfügbar sind. Dieses Intervall hat keine Auswirkungen darauf, wie häufig ein Skript ausgeführt wird.
Maximale Download-Geschwindigkeit	Nach Bedarf	Die maximale Download-Geschwindigkeit, nach Bedarf. Wählen Sie aus den verfügbaren Optionen.
Prozess-Zeitüberschreitung	1 Stunde	Die maximale Dauer, während der der Agent-Prozess vor dem Beenden ausgeführt wird. Weitere Details finden Sie unter https://support.quest.com/kb/177093/how-to-allow-more-time-for-a-

Option	Empfohlene Einstellung	Anmerkungen
		kace-script-to-run-before-it-times-out-.
Warten auf Startaufgaben deaktivieren	Deaktiviert	Ist diese Option ausgewählt, wird der Agent bei der Ausführung von Startaufgaben gestoppt.
Warten auf Anmeldeaufgaben deaktivieren	Deaktiviert	Ist diese Option ausgewählt, wird der Agent bei der Ausführung von Anmeldeaufgaben gestoppt.

5. Geben Sie im Abschnitt *Agent Status Icon Settings (Einstellungen des Agentenstatussymbols)* folgende Einstellungen an:

Option	Empfohlene Einstellung	Anmerkungen
Agentenstatus-Symbol für Gerät	Aktiviert	Wenn ausgewählt, ermöglicht Ihnen diese Option, den Agentenstatus für verwaltete Geräte anzuzeigen.
Agent auf Gerät im Snooze-Modus	Aktiviert	Wenn diese Option ausgewählt ist, können Sie die Aktivität des Agenten auf verwalteten Geräten über die Taskleiste (Windows) oder die Menüleiste (Mac OS) vorübergehend aussetzen. **HINWEIS:** Einige kritische Hintergrundaufgaben können weiterhin ausgeführt werden, einschließlich Inventarisierung, Replikationsaufgaben und dringende Warnungen.
Max. Snooze-Anzahl für Agent (pro Tag)	1 Snooze	Gibt an, wie oft Sie die Snooze-Funktion für den Agenten auf verwalteten Geräten pro Tag verwenden können.
Agent Status Icon Shortcuts (Verknüpfungen für das Agentenstatussymbol)	Nach Bedarf	Verwenden Sie diesen Abschnitt, um Links im Menü "KACE Agent" auf von Agenten verwalteten Geräten anzuzeigen. Sie können bis zu zehn Links angeben. Standard-URI-Links (Uniform Resource Identifier) werden unterstützt, wie z. B. `https`-, `ssh`- und `ftp`-URLs. So fügen Sie einen Link hinzu: a. Klicken Sie auf +. b. Geben Sie in die Spalte *Anzeigename* den Text ein, der im Menü angezeigt

Option	Empfohlene Einstellung	Anmerkungen
		werden soll. Zum Beispiel *My FTP link (Mein FTP-Link)*. c. Geben Sie in die Spalte "URL" die vollständig qualifizierte URL-Adresse ein. Zum Beispiel `https://www.quest.com/`. Die URL unterstützt die folgenden Ersetzungsvariablen: ◦ $(KACE_SYS_DIR) ◦ $(KACE_MAC_ADDRESS) ◦ $(KACE_IP_ADDRESS) ◦ $(KACE_SERVER_URL) ◦ $(KACE_SERVER) ◦ $(KACE_COMPANY_NAME) ◦ $(KACE_KUID) ◦ $(KACE_APP_DIR) ◦ $(KACE_DATA_DIR) ◦ $(KACE_AGENT_VERSION) Vollständige Informationen zu diesen und anderen Ersetzungsvariablen finden Sie unter Token-Ersetzungsvariablen. Mithilfe der Spaltenüberschriften können Sie die Liste sortieren. Im Menü "KACE Agent" werden die Links in der Reihenfolge angezeigt, in der sie auf dieser Seite aufgeführt sind.

HINWEIS: Alle Änderungen, die Sie in diesem Abschnitt vornehmen, werden erst wirksam, nachdem der KACE Agent auf dem verwalteten Gerät erneut eine Verbindung zur Appliance herstellt, entweder durch einen Neustart jedes einzelnen Agenten oder der Appliance.

6. Geben Sie im Abschnitt *Benachrichtigen* die Mitteilung für die Agenten-Kommunikation ein:

Option	Empfohlene Einstellung	Anmerkungen
Meldung auf der Begrüßungsseite des Agenten	Standardtext: **KACE Systemverwaltungs-Appliance** `überprüft die Aktualisierungen für die Konfigurations- und Verwaltungssoftware auf Ihrem PC. Bitte warten...`	Die Meldung, die Benutzern angezeigt wird, wenn Agenten Aufgaben ausführen, z.B. die Ausführung von Skripten auf ihren Geräten.
Agenten-Splash-Bitmap	Nach Bedarf	Der Pfad zu einer vorhandenen .bmp-Datei, die

Option	Empfohlene Einstellung	Anmerkungen
		Sie als Splash-Logo verwenden möchten.
Start-Splash deaktivieren	Deaktiviert	Ist diese Option ausgewählt, wird der Agent bei der Anzeige des Start-Splash-Logos gestoppt.
Anmelde-Splash deaktivieren	Deaktiviert	Ist diese Option ausgewählt, wird der Agent bei der Anzeige des Anmelde-Splash-Logos gestoppt.

7. Legen Sie im Abschnitt *Einstellungen für die Verarbeitung ohne Agent* die Kommunikationseinstellungen für Geräte ohne Agent fest:

Option	Beschreibung
SSH-Timeout	Die Zeit in Sekunden, nach der eine Verbindung geschlossen wird, wenn keine Aktivität stattfindet.
SNMP-Timeout	Die Zeit in Sekunden, nach der eine Verbindung geschlossen wird, wenn keine Aktivität stattfindet.
Wiederholungsversuche	Die Anzahl der Verbindungsversuche.
WinRM-Timeout	Die Zeit in Sekunden, nach der eine Verbindung geschlossen wird, wenn keine Aktivität stattfindet.
VMware-Timeout	Die Zeitspanne in Sekunden, die auf eine Verbindung zum VMware vSphere API Service gewartet wird, der auf einem VMware-Host ausgeführt wird.

8. Legen Sie im Abschnitt *Einstellungen für die Verarbeitung ohne Agent* die Kommunikationseinstellungen für Geräte ohne Agent fest:

Option	Beschreibung
SSH-Timeout	Die Zeit in Sekunden, nach der eine Verbindung geschlossen wird, wenn keine Aktivität stattfindet.
SNMP-Timeout	Die Zeit in Sekunden, nach der eine Verbindung geschlossen wird, wenn keine Aktivität stattfindet.
Wiederholungsversuche	Die Anzahl der Verbindungsversuche.
WinRM-Timeout	Die Zeit in Sekunden, nach der eine Verbindung geschlossen wird, wenn keine Aktivität stattfindet.
VMware-Timeout	Die Zeitspanne in Sekunden, die auf eine Verbindung zum VMware vSphere API Service gewartet wird, der auf einem VMware-Host ausgeführt wird.

9. Klicken Sie auf **Speichern**.

Die Organisation wird hinzugefügt. Wenn der schnelle Wechsel aktiviert ist und das Kennwort für das Standard-**Administratorkonto** für das System und die Organisationen übereinstimmen, können Sie mithilfe der Dropdown-Liste oben rechts auf der Seite zwischen Organisationen und dem System wechseln. Damit neue Organisationen in der Liste angezeigt werden, müssen Sie sich von der **Administratorkonsole** abmelden und dann erneut anmelden. Wenn die Option "Organisationsauswahl bei Anmeldung erforderlich" auf Systemebene aktiviert ist, ist die Organisation in der Dropdown-Liste auf der Administratoranmeldeseite unter `http://appliance_hostname/admin` verfügbar, wobei **appliance_hostname** für den Hostnamen Ihrer Appliance steht.

HINWEIS: Für neue Organisationen ist das Kennwort für das Standard-**Administratorkonto** das Gleiche wie das Kennwort des Standard-**Administratorkontos** auf Systemebene. Dieses wird automatisch zugewiesen. Zum Ändern des Kennworts des **Administratorkontos** müssen Sie das Administratorbenutzerkonto bearbeiten.

HINWEIS: Beachten Sie jedoch, dass Organisationen mit unterschiedlichen Kennwörtern für das **Administratorkonto** nicht für den **schnellen Wechsel** über die Dropdown-Liste in der oberen rechten Ecke der Seite verfügbar sind.

Weitere Informationen zu den Einstellungen auf Systemebene finden Sie unter Allgemeine Appliance-Einstellungen bei aktivierter Organisationskomponente konfigurieren.

Verwandte Themen

Verwalten von Organisationsfiltern

Appliance-Protokolle anzeigen

Verwalten von Benutzerkonten für Organisationen

Zweifaktor-Authentifizierung für Organisationen konfigurieren

Die Zwei-Faktor-Authentifizierung (2FA) bietet mehr Sicherheit für Benutzer, die sich im Gerät anmelden, indem sie einen zusätzlichen Schritt für den Anmeldevorgang hinzufügt. Sie vertraut auf die Google Authenticator-App, um Verifizierungscodes zu generieren. Die App generiert in regelmäßigen Abständen einen neuen sechsstelligen Code. Wenn diese Option aktiviert ist, werden die Endbenutzer bei jeder Anmeldung aufgefordert, den aktuellen Verifizierungscode einzugeben.

Um die Google Authenticator-App herunterzuladen, besuchen Sie eine der folgenden Websites:

- **Android-Geräte**: https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2
- **iOS-Geräte:** https://itunes.apple.com/ca/app/google-authenticator/id388497605?mt=8

Sie können 2FA-Zugriff auf die **Administratorkonsole** und **Benutzerkonsole** für eine oder mehrere Organisationen mit der **Systemverwaltungskonsole** aktivieren oder deaktivieren, wie unten beschrieben. Alternativ können Sie 2FA-Zugriff auf die **Administratorkonsole** und **Benutzerkonsole** für alle Benutzer in einer Organisation über die Seite *Zweifaktor-Authentifizierung* in der **Administratorkonsole** aktivieren. Weitere Informationen hierzu finden Sie unter Zweifaktor-Authentifizierung für alle Benutzer aktivieren.

1. Rufen Sie die Listenseite *Organisationen* auf:
   a. Melden Sie sich bei der Systemadministratorkonsole der Appliance an: `http://`**appliance_hostname**`/system`. Oder wählen Sie in der Dropdown-Liste rechts oben auf der Seite den Eintrag **System** aus.

   b. Klicken Sie in der linken Navigationsleiste auf **Organisationen** und anschließend auf **Organisationen**.
2. Wählen Sie auf der Listenseite *Organisation* eine oder mehrere Organisationen aus, für die Sie 2FA konfigurieren möchten.
3. Um 2FA für alle Benutzer in den ausgewählten Organisationen in der Administratorkonsole zu aktivieren, klicken Sie auf **Aktion auswählen** > **Zweifaktor-Authentifizierung** > **Verwaltungsportal** > **Für alle Benutzer erforderlich**.
4. Um 2FA für alle Benutzer in den ausgewählten Organisationen in der Administratorkonsole zu deaktivieren, klicken Sie auf **Aktion auswählen** > **Zweifaktor-Authentifizierung** > **Verwaltungsportal** > **Nicht erforderlich**.
5. Um 2FA für alle Benutzer in den ausgewählten Organisationen in der Benutzerkonsole zu aktivieren, klicken Sie auf **Aktion auswählen** > **Zweifaktor-Authentifizierung** > **Benutzerportal** > **Für alle Benutzer erforderlich**.
6. Um 2FA für alle Benutzer in den ausgewählten Organisationen in der Benutzerkonsole zu deaktivieren, klicken Sie auf **Aktion auswählen** > **Zweifaktor-Authentifizierung** > **Benutzerportal** > **Nicht erforderlich**.

Organisationen löschen

Sie können Organisationen nach Bedarf löschen. Wenn auf Ihrer Appliance jedoch nur eine Organisation vorhanden ist, können Sie diese erst löschen, nachdem Sie eine weitere hinzugefügt haben. Auf der Appliance muss immer mindestens eine Organisation verfügbar sein.

1. Rufen Sie die Seite *Organisationsdetail* auf:
   a. Melden Sie sich bei der Systemadministratorkonsole der Appliance an: `http://`**appliance_hostname**`/system`. Oder wählen Sie in der Dropdown-Liste rechts oben auf der Seite den Eintrag **System** aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Organisationen** und anschließend auf **Organisationen**.
   c. Klicken Sie auf den Namen einer Organisation.
2. Wählen Sie **Aktion auswählen** > **Löschen** und klicken Sie dann zum Bestätigen auf **Ja**.

Die Organisation wird zusammen mit den Informationen in der Organisationsdatenbank von der Appliance entfernt.

Für die Benutzerkonsole und Organisationsberichte verwendete Logos anpassen

Sie können das Logo ändern, das in der **Benutzerkonsole** und in Organisationsberichten angezeigt wird, damit es mit dem Branding Ihres Unternehmens übereinstimmt.

Die **Benutzerkonsole** und die Berichte, die Sie ausführen, wenn Sie über die **Administratorkonsole** bei einer Organisation angemeldet sind, verwenden standardmäßig das Quest Logo. Informationen zum Hochladen Ihres eigenen Logos finden Sie im Abschnitt *Logo-Überschreibungen* unter Allgemeine Appliance-Einstellungen ohne aktivierte Organisationskomponente konfigurieren.

Verwalten von Benutzerkonten für Organisationen

Organisationsbenutzerkonten ermöglichen Benutzern auf Grundlage der ihrem Konto zugewiesenen Rolle den Zugriff auf Funktionen der **Administratorkonsole**, **Benutzerkonsole** und des Service Desks.

Sie können LDAP-Server zur Benutzerauthentifizierung verwenden oder Sie können Benutzerkonten manuell hinzufügen und bearbeiten. Siehe:

- Verwalten von Organisationsbenutzerkonten
- Verwalten von Benutzerkonten auf Systemebene
- Verwenden eines LDAP-Servers zur Benutzerauthentifizierung

> **VORSICHT: Gehen Sie vorsichtig vor, wenn Sie das Kennwort für das Standard-Administratorkonto einer Organisation ändern. Organisationen mit unterschiedlichen Kennwörtern für das Administratorkonto sind nicht für den schnellen Wechsel über die Dropdown-Liste in der oberen rechten Ecke der Seite verfügbar.**
>
> **VORSICHT: Siehe Schnellen Wechsel von Organisationen und verknüpften Appliance aktivieren.**

Verwalten von Organisationsfiltern

Organisationfilter dienen zum Zuweisen von Geräten an Organisationen bei der Inventarerfassung von Geräten.

Organisationsfilter ähneln Labels, sie dienen jedoch einem bestimmten Zweck: Organisationfilter weisen bei der Inventarerfassung von Geräten diese automatisch an Organisationen zu.

Es gibt zwei Arten von Organisationsfiltern:

- **Datenfilter**: Weist Geräte basierend auf Suchkriterien automatisch Organisationen zu. Bei der Inventarerfassung von Geräten werden diese der Organisation zugewiesen, wenn sie den Kriterien entsprechen. Dieser Filter ähnelt Smart Labels dahingehend, dass er Geräte automatisch Organisationen zuweist, wenn sie den angegebenen Kriterien entsprechen.
- **LDAP-Filter**: Weisen Geräte basierend auf LDAP- oder Active Directory-Interaktionen automatisch Organisationen zu. Bei der Inventarerfassung von Geräten wird die Abfrage an den LDAP-Server gesendet. Wenn Geräte den Kriterien entsprechen, werden sie automatisch der Organisation zugewiesen.

Informationen zum Hinzufügen und Bearbeiten von Organisationsfiltern finden Sie unter:

- Datenfilter für Organisationen hinzufügen oder bearbeiten
- LDAP-Filter für Organisationen hinzufügen oder bearbeiten

Nachdem Sie einen Filter hinzugefügt haben, können Sie diesen der Organisation auf der Seite *Organisationsdetail* zuordnen. Siehe Hinzufügen, Bearbeiten und Löschen von Organisationen.

So funktionieren Organisationsfilter:

Für eine Organisation können mehrere Filter verwendet werden, ein Filter kann jedoch nicht mehreren Organisationen zugewiesen werden.

Organisationsfilter werden gemäß den folgenden Regeln ausgeführt:

- Bei der Inventarerfassung von Geräten wird mindestens ein Filter dafür ausgeführt. Wenn mehrere Filter vorhanden sind, werden diese entsprechend der **Reihenfolge** oder **Auswertungsreihenfolge** in den Filterdetails ausgeführt.
- Wenn Geräte den Kriterien entsprechen, werden sie der Organisation zugewiesen.
- Wenn Geräte den Kriterien nicht entsprechen, werden sie der Standardorganisation zugewiesen. Ein Administrator kann Geräte dann später manuell von der Standard- in eine andere Organisation verschieben. Siehe Geräte umleiten.

Datenfilter für Organisationen hinzufügen oder bearbeiten

Sie können Datenfilter für Organisationen hinzufügen oder bearbeiten, um Geräte automatisch Organisationen zuzuweisen.

1. Rufen Sie die Seite *Detail zu Organisationsfilter* auf:
   a. Melden Sie sich bei der Systemadministratorkonsole der Appliance an: `http://`**appliance_hostname**`/system`. Oder wählen Sie in der Dropdown-Liste rechts oben auf der Seite den Eintrag **System** aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Organisationen** und anschließend auf **Filter**.
   c. Führen Sie eine der folgenden Aktionen aus, um die Seite *Detail zu Organisationsfilter* anzuzeigen:
   - Klicken Sie auf den Namen eines Filters.
   - Wählen Sie **Aktion auswählen** > **Neuer Datenfilter**.
2. Geben Sie die folgenden Informationen an:

Option	Beschreibung
Aktiviert	Gibt an, ob der Filter aktiviert ist. Filter müssen aktiviert werden, bevor sie angewendet werden können.
Name	Name des Filters Dieser Name wird in der Liste *Organisationsfilter* angezeigt.
Beschreibung	Eine Beschreibung des Filters
Reihenfolge	Die Ausführungsreihenfolge des Filters Filter werden entsprechend der angegebenen Nummer ausgeführt. Kleine Zahlen werden vor großen Zahlen ausgeführt.

3. Wählen Sie im Abschnitt **Gerät-Filterkriterien** die Filterkriterien aus:
   a. Wählen Sie ein Geräteattribut in der Dropdown-Liste ganz links in der obersten Zeile aus.

   Beispiel: **IP-Adresse**.

   TIPP: Die Appliance unterstützt sowohl IPv6- (Internet Protocol Version 6) als auch IPv4-Adressen.

   b. Wählen Sie in der zweiten Dropdown-Liste eine Bedingung aus.

   Beispiel: **Enthält**.

   c. Geben Sie im Textfeld einen Wert für das Attribut ein.

   Wenn Sie beispielsweise Geräte eines bestimmten IP-Adressbereichs wie dem gesamten Subnetz 67.18.250.255 finden möchten, verwenden Sie das Prozentzeichen (%) folgendermaßen als Platzhalter: 67.18.250.%.

   d. **Optional**: Wenn Sie Attribute hinzufügen möchten, wählen Sie einen Operator wie etwa [**UND**] aus der linken Dropdown-Liste in der zweiten Zeile aus.

   Die Felder in der Zeile werden aktiviert.

   e. **Optional**: Um dem Abschnitt mit Kriterien Zeilen hinzuzufügen, klicken Sie auf **Kriterium hinzufügen**.

Eine weitere Zeile wird angezeigt.

4. Klicken Sie auf **Speichern**.

LDAP-Filter für Organisationen hinzufügen oder bearbeiten

Sie können LDAP-Filter hinzufügen, um Geräte automatisch Organisationen anhand von LDAP-Kriterien zuzuweisen.

HINWEIS: Falls der LDAP-Server Anmeldeinformationen für die Anmeldung als Administrator erfordert (also für eine nicht anonyme Anmeldung), geben Sie diese Anmeldeinformationen an. Wenn Benutzername und Kennwort nicht angegeben werden, wird der Struktur-Lookup nicht ausgeführt. Jeder LDAP-Filter kann eine Verbindung zu einem anderen LDAP-Server herstellen.

1. Rufen Sie die Seite *Detail zu Organisationsfilter* auf:
   a. Melden Sie sich bei der Systemadministratorkonsole der Appliance an: `http://`**appliance_hostname**`/system`. Oder wählen Sie in der Dropdown-Liste rechts oben auf der Seite den Eintrag **System** aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Organisationen** und anschließend auf **Filter**.
   c. Führen Sie eine der folgenden Aktionen aus, um die Seite *Detail zu Organisationsfilter* anzuzeigen:
   - Klicken Sie auf den Namen eines LDAP-Filters.
   - Wählen Sie **Aktion auswählen** > **Neuer LDAP-Filter**.
2. Geben Sie die folgenden Informationen an:

Option	Beschreibung
Aktiviert	Gibt an, ob der Filter aktiviert ist. Filter müssen aktiviert werden, bevor sie angewendet werden können.
Name	Name des Filters Dieser Name wird in der Liste *Organisationsfilter* angezeigt.
Beschreibung	Eine Beschreibung des Filters
Auswertungsreihenfolge	Die Ausführungsreihenfolge des Filters Filter werden entsprechend der angegebenen Nummer ausgeführt. Kleine Zahlen werden vor großen Zahlen ausgeführt.

3. Geben Sie LDAP-Kriterien an:

Option	Beschreibung
LDAP-Server	Die IP-Adresse oder der Hostname des LDAP-Servers. Wenn die IP-Adresse ungültig ist, wartet die Appliance auf ein Timeout, sodass bei der Verwendung der LDAP-Authentifizierung Verzögerungen bei der Anmeldung entstehen. **HINWEIS:** Wenn die Verbindung über SSL hergestellt wird, verwenden Sie die IP-Adresse oder den Hostnamen. Beispiel: ldaps://hostname.

Option	Beschreibung
Port	Die LDAP-Port-Nummer, in der Regel 389 (LDAP) oder 636 (sicheres LDAP).
Basis-DN	Die LDAP-Kriterien für das Filtern des Hauptstandorts von Geräten. Diese Kriterien legen einen Standort oder Container in der LDAP- oder Active Directory-Struktur fest und sollten alle Geräte umfassen, die identifiziert werden sollen. Geben Sie eine genaue Kombination aus OUs, DCs oder CNs an, die Ihren Kriterien entsprechen, die von links (sehr genau) bis rechts (sehr allgemein) reichen. Dieser Pfad beispielsweise würde zu einem Container mit den Geräten führen, die Sie identifizieren möchten: `OU=computers,DC=company,DC=com`.
Erweiterte Suche	Der Suchfilter. Beispiel: `(&(objectCategory=Computer) (sAMAccountName=KBOX_COMPUTER_NAME))`
LDAP-Anmeldung	Die Anmeldeinformationen, die erforderlich sind, damit die Appliance sich beim LDAP-Server anmelden und Konten lesen kann. Beispiel: `LDAP Login:CN=service_account,CN=Users,DC=company,DC=com`. Ohne Angabe eines Benutzernamens erfolgt ein anonymer Zugriffsversuch. Jedes LDAP-Label kann eine Verbindung zu einem anderen LDAP- oder Active Directory-Server herstellen.
LDAP-Kennwort	Das Kennwort des Kontos, mit dem sich die Appliance beim LDAP-Server anmeldet.

Während der Filterverarbeitung ersetzt die Appliance alle als "KBOX_" definierten Variablen durch ihre entsprechenden Laufzeitwerte.

Derzeit unterstützte Variablen für Organisationsgerätefilter:

```
KBOX_COMPUTER_NAME
KBOX_COMPUTER_DESCRIPTION
KBOX_COMPUTER_MAC
KBOX_COMPUTER_IP
KBOX_USER
KBOX_USER_DOMAIN
KBOX_DOMAINUSER
```

Wenn der externe Server Anmeldeinformationen für die Anmeldung als Administrator benötigt (auch als nicht-anonyme Anmeldung bezeichnet), geben Sie diese Anmeldeinformationen an. Wenn Sie keinen LDAP-Benutzernamen angeben, erfolgt ein anonymer Zugriffsversuch. Jeder LDAP-Filter kann eine Verbindung zu einem anderen LDAP/AD-Server herstellen.

HINWEIS: Ersetzen Sie alle als "KBOX_" definierten Variablen durch reale Werte. Klicken Sie auf **Testen**, um die Ergebnisse zu überprüfen.

4. Klicken Sie auf **Speichern**.

Organisationsfilter testen

Sie können Organisationsfilter testen, um sicherzustellen, dass sie die erwarteten Ergebnisse liefern.

1. Rufen Sie die Liste mit den *Geräten* der Organisation auf:
   a. Melden Sie sich bei der Systemadministratorkonsole der Appliance an: `http://`**appliance_hostname**`/system`. Oder wählen Sie in der Dropdown-Liste rechts oben auf der Seite den Eintrag **System** aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Organisationen** und anschließend auf **Geräte**.
2. Klicken Sie rechts auf der Seite über der Tabelle auf die Registerkarte **Organisationsfilter testen**.
3. Wählen Sie einen Filter aus der Dropdown-Liste **Filter auswählen** aus.
4. Klicken Sie auf **Testen**.

   Die Testergebnisse werden angezeigt. Sie können die in der Liste angezeigten Geräte ggf. erneut filtern. Siehe Geräte filtern.

   HINWEIS: Werden in den Testergebnissen keine Geräte aufgeführt, gibt es entweder keine Geräte, die den Kriterien entsprechen, oder die Kriterien sind ungültig. Informationen zum Bearbeiten der Kriterien finden Sie unter Datenfilter für Organisationen hinzufügen oder bearbeiten.

Organisationsfilter löschen

Sie können Organisationsfilter löschen, die keiner Organisation zugeordnet sind.

1. Rufen Sie die Liste *Organisationen* auf:
   a. Melden Sie sich bei der Systemadministratorkonsole der Appliance an: `http://`**appliance_hostname**`/system`. Oder wählen Sie in der Dropdown-Liste rechts oben auf der Seite den Eintrag **System** aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Organisationen** und anschließend auf **Organisationen**.
2. Wenn der Filter einer Organisation zugeordnet ist:
   a. Klicken Sie auf den Namen einer Organisation, um die Seite *Organisationsdetail* anzuzeigen.
   b. Klicken Sie im Feld *Filter* auf das **x** neben dem Filter, den Sie löschen möchten.
   c. Klicken Sie unten auf der Seite auf **Speichern**.

   Filter werden erst aktualisiert, nachdem Sie auf **Speichern** geklickt haben.

   Der Filter ist der Organisation nicht mehr zugeordnet.
3. Klicken Sie auf **Organisationen > Filter**, um die Seite *Organisationsfilter* anzuzeigen.
4. Gehen Sie beim Löschen von Filtern folgendermaßen vor:
   - **Aktivieren Sie das Kontrollkästchen neben mindestens einem Filter und wählen Sie Aktion auswählen > Löschen.**
   - **Klicken Sie auf den verknüpften Namen eines Filters und dann auf der Seite** *Detail zu Organisationsfilter* **auf Löschen.**
5. Klicken Sie zur Bestätigung auf **Ja**.

Verwalten von Geräten in Organisationen

Sie können Geräte, die Organisationen zugewiesen sind, suchen, filtern, und umleiten.

Verwenden der erweiterten Suche

Wenn Sie eine genauere Suche durchführen möchten, als dies mit Stichwörtern möglich ist, können Sie die erweiterte Suche verwenden. Hierbei können Sie für jedes Feld im Inventardatensatz Werte angeben und die gesamte Inventarliste nach diesen Werten durchsuchen.

Sie können zum Beispiel nach BIOS-Informationen suchen, wenn Sie wissen möchten, auf welchen Geräten eine bestimmte BIOS-Version installiert ist, um nur bei diesen ein Upgrade durchzuführen. Siehe Auf Seitenebene mit erweiterten Optionen suchen.

TIPP: Sie können Filter auf die in den Suchergebnissen angezeigten Geräte anwenden.

Geräte filtern

Wenn Sie über Organisationsfilter verfügen, können Sie Geräte filtern, um zu überprüfen, dass die Filter richtig angewendet werden.

1. Rufen Sie die Liste mit den *Organisationsgeräten* auf:
   a. Melden Sie sich bei der Systemadministratorkonsole der Appliance an: `http://`**appliance_hostname**`/system`. Oder wählen Sie in der Dropdown-Liste rechts oben auf der Seite den Eintrag **System** aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Organisationen** und anschließend auf **Geräte**.
2. Aktivieren Sie das Kontrollkästchen neben einem oder mehreren Geräten.
3. Wählen Sie **Aktion auswählen** > **Filter anwenden**.

   Die ausgewählten Geräte werden gegen die vorhandenen Filter abgeglichen. Wenn Geräte Organisationen neu zugeordnet werden, wird der neue Organisationsname neben dem alten Organisationsnamen in der Spalte *Organisation* angezeigt.

Geräte umleiten

Sie können Geräte Organisationen nach Bedarf erneut zuweisen oder manuell zuweisen.

Beispiel: Ein Gerät, das Organisation **A** zugweisen wurde, kann manuell an Organisation **B** umgeleitet werden, sodass es im Inventar von Organisation **B** angezeigt wird.

1. Rufen Sie die Liste mit den *Organisationsgeräten* auf:
   a. Melden Sie sich bei der Systemadministratorkonsole der Appliance an: `http://`**appliance_hostname**`/system`. Oder wählen Sie in der Dropdown-Liste rechts oben auf der Seite den Eintrag **System** aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Organisationen** und anschließend auf **Geräte**.
2. Aktivieren Sie das Kontrollkästchen neben einem oder mehreren Geräten.
3. Wählen Sie **Aktion auswählen** > **Zuweisen** und wählen Sie dann einen Organisationsnamen aus, um die ausgewählten Geräte der Organisation neu zuzuweisen.

Informationen zu Gerätedetails

Die Seite *Gerätedetails* im Abschnitt *Organisationen* auf Systemebene enthält Details zu Geräten, die Organisationen zugewiesen sind.

Rufen Sie zum Öffnen der Seite *Gerätedetails* im Abschnitt *Organisationen* die Systemebene der Appliance auf und wählen Sie **Organisationen** > **Geräte** aus. Wählen Sie anschließend einen Gerätenamen in der Liste aus. Weitere Informationen zu Gerätedetails finden Sie unter Verwalten von Inventarinformationen.

Ausführen von Berichten für Einzelorganisationen sowie von konsolidierten Berichten

Wenn die Organisationskomponente auf Ihrer Appliance aktiviert ist und Sie über mehrere Organisationen verfügen, können Sie Berichte für Einzelorganisationen für die einzelnen Organisationen getrennt ausführen. Zusätzlich können Sie auch konsolidierte Berichte ausführen, die Informationen für alle Organisationen in einem einzigen Bericht zusammenfassen.

Informationen zur Berichterstellung finden Sie unter Erstellen von Berichten.

Importieren und Exportieren von Appliance-Ressourcen

Sie können auf einer Appliance Ressourcen zwischen Organisationen übertragen. Wenn Sie über mehrere Appliances verfügen, können Sie auch Ressourcen zwischen den Appliances übertragen.

Informationen zum Importieren und Exportieren von Anwendungsressourcen

Ressourcen wie verwaltete Installationen und Smart Labels können importiert oder exportiert und so zwischen Organisationen und Appliances ausgetauscht werden.

Wenn Sie mehrere KACE SMAs haben, können Sie Ressourcen zwischen ihnen mithilfe der integrierten Samba Freigabeverzeichnisse der Appliances übertragen. Wenn auf Ihrer Appliance die Organisationskomponente aktiviert wurde, können Sie außerdem Ressourcen zwischen Organisationen übertragen. Dies ist hilfreich für Ressourcen wie Skripte, die für eine Organisation erstellt wurden, aber auch für andere Organisationen nützlich sein können.

Sie können folgende Ressourcen importieren bzw. exportieren:

- Benachrichtigungen
- Verwaltete Installationen
- Berichte
- Skripte
- Smart Labels
- Software
- Service Desk-Prozesse, Ticketwarteschlangen und Ticketregeln

Übertragen von Ressourcen zwischen Appliances mithilfe von Samba Freigabeverzeichnissen

Mithilfe von Samba Freigabeverzeichnissen als Staging-Bereiche können Sie Ressourcen zwischen Appliances übertragen.

Exportieren Sie dazu die Ressourcen aus einer Appliance und importieren Sie sie in eine andere Appliance.

Ressourcen aus einer Appliance exportieren

Exportieren Sie Ressourcen aus einer Appliance, um sie für den Import in andere Appliances verfügbar zu machen.

1. Melden Sie sich bei der Administratorkonsole der Appliance an, auf der sich die Ressourcen befinden.
2. Aktivieren Sie die Samba Dateifreigabe.

   Siehe Dateifreigabe auf Systemebene aktivieren.
3. Rufen Sie die Liste der *freigegebenen Ressourcen* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie auf der linken Navigationsleiste auf **Einstellungen** und anschließend auf **Ressourcen**.
   c. Klicken Sie im *Ressourcenbereich* auf **Exportieren**.
4. **Optional**: Sie können die Liste filtern. Verwenden Sie hierzu rechts auf der Seite über der Tabelle die Dropdown-Liste *Anzeigen nach* und das Feld *Suchen*.

   Wählen Sie beispielsweise eine Ressource aus der Dropdown-Liste *Anzeigen nach* aus, um nur diese Ressourcenkategorie anzuzeigen, oder geben Sie einen Begriff in das Feld *Suchen* ein, um Elemente anzuzeigen, die diesem Begriff entsprechen.
5. Aktivieren Sie das Kontrollkästchen neben einer oder mehreren Ressourcen.
6. Führen Sie einen der folgenden Schritte aus:
   - **Aktion auswählen > Auf lokale Freigabe exportieren**
   - **Aktion auswählen > Auf Netzwerkfreigabe exportieren**

   HINWEIS: Wählen Sie **Auf Netzwerkfreigabe exportieren**, um die Daten an einem freigegebenen Speicherort im Netzwerk zu speichern, auf den von anderen Geräten zugegriffen werden kann. Wählen Sie **Auf lokale Freigabe exportieren**, um die Daten an einem Speicherort auf einem Gerät zu speichern, auf den nur von diesem Gerät aus zugegriffen werden kann.
7. **Optional**: Geben Sie auf der Seite *Exportierte Ressource(n) mit Anmerkungen versehen* ggf. zusätzliche Informationen im Feld **Hinweis** ein.
8. Klicken Sie auf **Speichern**.

   Die exportierten Ressourcen werden zunächst auf der Seite *Ressourcen-Weitergabestatus* mit dem *Status Neue Anforderung* angezeigt.

Wenn der Export abgeschlossen ist, wird der *Status* in *Abgeschlossen* geändert. Die exportierten Ressourcen sind auf der Samba Dateifreigabe zum Import verfügbar. Siehe Ressourcen in Organisationen importieren.

Die meisten Import- und Exportaufgaben dauern nur einen Moment. Sehr große Ressourcen nehmen mehr Zeit in Anspruch.

Ressourcen in eine Appliance importieren

Sie können Ressourcen bei Bedarf in Appliances importieren.

Sie haben Ressourcen aus einer Appliance exportiert. Siehe Übertragen von Ressourcen zwischen Appliances mithilfe von Samba Freigabeverzeichnissen.

1. Führen Sie einen der folgenden Schritte aus, um den Speicherort des Samba Freigabeverzeichnisses anzuzeigen:
   - **Wenn die Organisationskomponente auf Ihrer Appliance aktiviert ist, wählen Sie Einstellungen > Sicherheitseinstellungen aus.**
   - **Wenn die Organisationskomponente in Ihrer Appliance aktiviert ist, wählen Sie auf der Seite rechts oben aus der Dropdown-Liste eine Organisation aus und wählen dann Einstellungen > Allgemeine Einstellungen.**
2. Kopieren Sie die Ressourcen mithilfe eines Drittanbieter-Dienstprogramms zum Kopieren von Dateien aus der Samba Freigabe der **exportierenden** Appliance in die Samba Freigabe der **importierenden** Appliance.
3. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
4. Wählen Sie auf der **importierenden** Appliance **Einstellungen** > **Ressourcen**, um den Bereich *Ressourcen* anzuzeigen.
5. Klicken Sie auf **Import**, um die Seite *Import Appliance Resources (Appliance-Ressourcen importieren)* zu öffnen, auf der alle für den Import verfügbaren Appliance-Ressourcen angezeigt werden.
6. Wählen Sie **Aktion auswählen** > **Von Netzwerkfreigabe importieren**, um die Seite *Ressourcen aus Samba Verzeichnis importieren* anzuzeigen.
7. Wählen Sie die Ressourcen aus, die importiert werden sollen, und klicken Sie auf **Ressourcen importieren**.

   Die importierten Ressourcen werden auf der Seite *Ressourcen-Manager-Warteschlange* mit dem *Status Neue Anforderung* angezeigt.

Wenn der Import abgeschlossen ist, wird der *Status* in *Abgeschlossen* geändert. Die importierten Ressourcen sind verfügbar und werden auf den jeweiligen Registerkarten, beispielsweise *Berichterstellung*, angezeigt.

Die meisten Import- und Exportaufgaben dauern nur einen Moment. Sehr große Ressourcen nehmen mehr Zeit in Anspruch.

Übertragen von Ressourcen zwischen Organisationen

Falls die Organisationskomponente in Ihrer Appliance aktiviert ist, können Sie Ressourcen zwischen Organisationen übertragen, indem Sie sie aus einer Organisation exportieren und anschließend in andere Organisationen importieren.

Ressourcen aus Organisationen exportieren

Exportieren Sie Ressourcen aus Organisationen, um sie für den Import in andere Organisationen verfügbar zu machen.

1. Wählen Sie in der oberen rechte Ecke der Seite die Organisation aus, aus der Sie Ressourcen exportieren möchten.
2. Rufen Sie die Liste *Ressourcen exportieren* auf:
   a. Klicken Sie auf der linken Navigationsleiste auf **Einstellungen** und anschließend auf **Ressourcen**.
   b. Klicken Sie im *Ressourcenbereich* auf **Exportieren**.

   Auf der Seite *Ressourcen exportieren* werden alle Ressourcen für Organisationen angezeigt, die für den Export verfügbar sind.
3. Aktivieren Sie das Kontrollkästchen neben einer oder mehreren Ressourcen.
4. Wählen Sie **Aktion auswählen** > **Auf lokale Freigabe exportieren** oder **Auf Netzwerkfreigabe exportieren**, um das Dialogfeld *Exportierte Ressource(n) mit Anmerkungen versehen* anzuzeigen.
5. **Optional**: Geben Sie eventuelle zusätzliche Informationen in das Feld *Hinweise* ein.
6. Klicken Sie auf **Speichern**.

   Die exportierte Ressource wird zunächst auf der Seite *Ressourcen-Manager-Warteschlange* mit dem *Status Neue Anforderung* angezeigt.

Wenn der Export abgeschlossen ist, wird der *Status* in *Abgeschlossen* geändert. Die exportierten Ressourcen sind in Ihrer Appliance für andere Organisationen zum Import verfügbar. Anleitungen dazu finden Sie unter Ressourcen in Organisationen importieren.

Die meisten Import- und Exportaufgaben dauern nur einen Moment. Sehr große Ressourcen nehmen mehr Zeit in Anspruch.

Ressourcen in Organisationen importieren

Sie können Ressourcen bei Bedarf in Organisationen importieren.

Sie haben Ressourcen aus einer Organisation exportiert. Siehe Übertragen von Ressourcen zwischen Organisationen.

Um Appliance-Ressourcen aus einer anderen Appliance zu importieren, befolgen Sie die Anweisungen unter Übertragen von Ressourcen zwischen Appliances mithilfe von Samba Freigabeverzeichnissen.

1. Wählen Sie aus der Dropdown-Liste in der oberen rechten Ecke der Seite die Organisation aus, in die Sie Ressourcen importieren möchten.
2. Rufen Sie die Liste der *Importressourcen* auf:
   a. Klicken Sie auf der linken Navigationsleiste auf **Einstellungen** und anschließend auf **Ressourcen**.
   b. Klicken Sie im *Ressourcenbereich* auf **Importieren**.
3. Aktivieren Sie das Kontrollkästchen neben einer oder mehreren Ressourcen.
4. Wählen Sie **Aktion auswählen** > **Von lokaler Freigabe importieren**.

   Die importierte Ressource wird auf der Seite *Ressourcen-Weitergabestatus* mit dem *Status Neue Anforderung* angezeigt.

Wenn der Import abgeschlossen ist, wird der *Status* in *Abgeschlossen* geändert. Die importierten Ressourcen sind verfügbar und werden auf den jeweiligen Registerkarten, beispielsweise *Berichterstellung*, angezeigt.

Die meisten Import- und Exportaufgaben dauern nur einen Moment. Sehr große Ressourcen nehmen mehr Zeit in Anspruch.

Verwalten exportierter Ressourcen auf Systemebene

Wenn die Organisationskomponente in der Appliance aktiviert ist, können Sie exportierte oder freigegebene Ressourcen auf Systemebene verwalten.

Dies bietet Zugriff auf Ressourcen, die von einer beliebigen Organisation in der Appliance exportiert oder für die Freigabe verfügbar gemacht wurden.

Freigegebene Ressourcen anzeigen oder löschen

Wenn die Organisationskomponente auf Ihrer Appliance aktiviert ist, können Sie die Ressourcen anzeigen, die aus einer beliebigen Organisation in der Appliance exportiert wurden.

1. Rufen Sie die Liste *Freigegebene Ressourcen* auf:
   a. Melden Sie sich bei der Systemadministratorkonsole der Appliance an: `http://`**appliance_hostname**`/system`. Oder wählen Sie in der Dropdown-Liste rechts oben auf der Seite den Eintrag **System** aus.
   b. Klicken Sie auf der linken Navigationsleiste auf **Einstellungen** und anschließend auf **Ressourcen**.
   c. Klicken Sie auf **Freigegeben**.
2. So löschen Sie eine Ressource:
   a. Aktivieren Sie das Kontrollkästchen neben einer oder mehreren Ressourcen.
   b. Wählen Sie **Aktion auswählen** > **Löschen** und klicken Sie dann zum Bestätigen auf **Ja**.

Freigegebene Ressourcen von der lokalen Appliance in Netzwerkstandorte verschieben

Wenn die Organisationskomponente auf Ihrer Appliance aktiviert ist, können Sie freigegebene Ressourcen von der lokalen Appliance in eine Netzwerkfreigabe verschieben.

1. Rufen Sie die Liste *Freigegebene Ressourcen* auf:
   a. Melden Sie sich bei der Systemadministratorkonsole der Appliance an: `http://`**appliance_hostname**`/system`. Oder wählen Sie in der Dropdown-Liste rechts oben auf der Seite den Eintrag **System** aus.
   b. Klicken Sie auf der linken Navigationsleiste auf **Einstellungen** und anschließend auf **Ressourcen**.
   c. Klicken Sie auf **Freigegeben**.
2. Wählen Sie **Aktion auswählen** > **Auf Netzwerkfreigabe exportieren** und klicken Sie dann zum Bestätigen auf **Ja**.

Status von Ressourcenexporten anzeigen oder löschen

Wenn die Organisationskomponente auf Ihrer Appliance aktiviert ist, können Sie den Status der Ressourcen anzeigen, die von einer beliebigen Organisation auf Systemebene exportiert wurden.

Die Statusinformationen werden nach 24 Stunden automatisch gelöscht, sie können den Status allerdings auch bei Bedarf manuell löschen.

1. Rufen Sie die Liste *Ressourcen-Weitergabestatus* auf:

a. Melden Sie sich bei der Systemadministratorkonsole der Appliance an: `http://`**appliance_hostname**`/system`. Oder wählen Sie in der Dropdown-Liste rechts oben auf der Seite den Eintrag **System** aus.
b. Klicken Sie auf der linken Navigationsleiste auf **Einstellungen** und anschließend auf **Ressourcen**.
c. Klicken Sie im *Ressourcenbereich* auf **Status**.

2. So löschen Sie einen Status
   a. Aktivieren Sie das Kontrollkästchen neben einem Status.
   b. Wählen Sie **Aktion auswählen > Löschen** und klicken Sie dann zum Bestätigen auf **Ja**.

Verwalten des Inventars

Mit der Appliance können Sie Geräte, Software, Prozesse und Dienste im Inventar verwalten.

Verwenden des Bestandsaufnahme-Dashboards

Das Bestandsaufnahme-Dashboard bietet einen Überblick über verwaltete Geräte für die ausgewählte Organisation (falls zutreffend) oder das Gerät.

Wenn auf der Appliance die Organisationskomponente aktiviert ist und Sie bei der Administratorkonsole angemeldet sind (`http://`**appliance_hostname**`/admin`), zeigt das Bestandsaufnahme-Dashboard Informationen zur ausgewählten Organisation an.

Sie können auf das *Bestandsaufnahme-Dashboard* zugreifen, wenn eine oder mehrere Rollen, die mit Ihrem Benutzerkonto verknüpft sind, Zugriff auf dieses Dashboard haben. Wenn Sie es ausblenden möchten, bearbeiten Sie Ihre Benutzerrollen nach Bedarf. Weitere Informationen hierzu finden Sie unter Benutzerrollen hinzufügen oder bearbeiten.

TIPP: Die Appliance aktualisiert die Übersichtswidgets regelmäßig. Um die meisten Widgets zu aktualisieren, klicken Sie auf die Schaltfläche **Aktualisieren** in der oberen rechten Seite: . Um die meisten einzelne Widgets zu aktualisieren, zeigen Sie mit dem Mauszeiger auf das Widget und klicken Sie oberhalb des Widgets auf die Schaltfläche **Aktualisieren**. Einige Widgets erfordern möglicherweise zusätzliche Schritte.

Informationen über die Bestandsaufnahme-Dashboard-Widgets

Die Bestandsaufnahme-Dashboard-Widgets bieten einen Überblick über verwaltete Geräte für die ausgewählte Organisation oder Appliance.

In diesem Abschnitt werden die im *Bestandsaufnahme-Dashboard* verfügbaren Widgets beschrieben. Wenn die Organisationskomponente in Ihrer Appliance aktiviert ist, zeigen die Widgets die Informationen für die ausgewählte Organisation auf Administratorebene und die Informationen für das Gerät auf Systemebene.

Dieses Dashboard bietet einen groben Überblick über Ihre Gerätenutzung. Verwenden Sie es, um schnell den Status Ihrer Geräte zu überprüfen und nach Indikatoren zu suchen, mit denen Sie Ihr Geräteinventar verbessern können. Sie können sich beispielsweise auf die Festplattenkapazität des Geräts konzentrieren und Ressourcen neu zuweisen, wo sie am dringendsten benötigt werden.

Widget	Beschreibung
Geräteberichte	Dieses Widget enthält Links zu häufig verwendeten Inventarberichten. Verwenden Sie sie, um schnell einen bestimmten Bericht zu erstellen, z. B. *Geräte nach Speicher*, *Geräte nach Betriebssystem* und andere.

Widget	Beschreibung
Verbindungen	Dieses Widget zeigt die Anzahl der Verbindungen zum Webserver der Appliance an. Eine hohe Anzahl zeigt an, dass der Server stark ausgelastet ist, wodurch sich die Reaktionszeit der Appliance verschlechtern kann. Wenn für Ihre Appliance die Organisationskomponente aktiviert ist, zeigt das Widget Informationen für die jeweils ausgewählte Organisation an.
Geräteanmelderate	Diese Auswahl zeigt die Anzahl der Geräte an, die sich während der letzten 60 Minuten mit der Appliance verbunden haben. Wenn die Organisationskomponente in Ihrer Appliance aktiviert ist, ist dieses Widget auf Systemebene verfügbar.
Provisionierung	Dieses Widget zeigt den Status von Provisionierungs- oder Installationsaufgaben des KACE Agenten an. Wenn für Ihre Appliance die Organisationskomponente aktiviert ist, zeigt das Widget Informationen für die jeweils ausgewählte Organisation an.
Verknüpfungen	Dieses Widget enthält Links zu häufig verwendeten Inventarseiten und -assistenten. Verwenden Sie sie, um schnell zu bestimmten Seiten zu navigieren, wie z. B. zum Assistent für die Agenten-Provisionierung, zur Seite *Ermittlungszeitpläne* und andere.
Anzahl der Agent-Versionen	Dieses Widget zeigt die Anzahl der Agenten für jede Version an. Diese Informationen können während eines Upgrades nützlich sein.
Bestandszählungen	Dieses Widget zeigt die Anzahl der Geräte an, die mit jeder Geräteverwaltungsmethode verknüpft sind, z. B. „Agentenverwaltung“, „ohne Agent“ und andere. Außerdem wird die Anzahl der Agenten angezeigt, die in den letzten acht Stunden aktualisiert wurden.
Geräte nach Datenträgerkapazität	Dieses Widget zeigt eine Ringdiagramm an, in dem die einzelnen „Tortenstücke“ des Diagramms den freien Speicherplatz in Prozent auf den verwalteten Geräten angeben. Durch Klicken auf den Widget-Titel wird ein Bericht mit Links zu den zugeordneten Geräten angezeigt. Wenn Sie mit der Maus über die einzelnen „Tortenstücke“ des Diagramms fahren, kann der prozentuale Anteil an verwalteten Geräten angezeigt werden, die über den ausgewählten prozentualen Anteil an freiem Speicherplatz verfügen. Wenn Sie beispielsweise über das rote „Tortenstück“ im Diagramm fahren, zeigt das Widget den Prozentsatz an Geräten an, deren freier Speicherplatz unter 25 % liegt.

Widget	Beschreibung
Verwaltete Betriebssysteme	Dieses Widget zeigt den Prozentsatz der verwalteten Geräte an, die mit dem jeweiligen Betriebssystem laufen. Wenn für Ihre Appliance die Organisationskomponente aktiviert ist, zeigt dieses Widget die Anzahl der Geräte für die jeweils ausgewählte Organisation als Prozentsatz an.
Provisionierte Plattformen	Dieses Widget zeigt den Prozentsatz der installierten Betriebssysteme auf durch den Agenten verwalteten Geräten. Wenn für Ihre Appliance die Organisationskomponente aktiviert ist, zeigt das Widget Informationen für die jeweils ausgewählte Organisation an.
Geräte nach Hersteller	Dieses Widget zeigt die wichtigsten Gerätehersteller aus dem Geräteinventar an. Wenn für Ihre Appliance die Organisationskomponente aktiviert ist, zeigt dieses Widget die Anzahl der Geräte für die jeweils ausgewählte Organisation als Prozentsatz an.
Geräte nach Modell	Dieses Widget zeigt die wichtigsten Gerätemodelle aus dem Geräteinventar an. Wenn für Ihre Appliance die Organisationskomponente aktiviert ist, zeigt dieses Widget die Anzahl der Geräte für die jeweils ausgewählte Organisation als Prozentsatz an.
Geräte nach Speicher	Dieses Widget zeigt ein Balkendiagramm an, in dem jeder Balken für eine Reihe von Geräten steht, auf denen eine angegebene RAM-Größe installiert ist.
Geräte nach Prozessor	Dieses Widget zeigt ein Balkendiagramm an, in dem jeder Balken für eine Reihe von Geräten steht, die eine bestimmte Prozessorkonfiguration aufweisen.
Geräte nach Untertyp	Dieses Widget zeigt ein Ringdiagramm an, in dem die Abschnitte des Diagramms den Prozentsatz der verwalteten Geräte nach Geräte-Untertyp angeben.
VMware-Geräteanzahl	Dieses Widget zeigt die Anzahl der einzelnen VMware-Gerätetypen an, z. B. vCenter, ESXi-Hosts, virtuelle Maschinen und bereitgestellte virtuelle Maschinen. Wenn Sie auf den Titel des Widgets klicken, wird die Seite mit der *Geräteliste* angezeigt.
VMware-Geräteberichte	Dieses Widget enthält Links zu fünf beliebten VMware-Inventarberichten. Wenn Sie auf den Titel des Widgets klicken, wird die Seite mit der Liste der *Berichte* angezeigt, auf der der Filter für die *virtuelle Infrastruktur* angewendet wird.
VMware ESXi-Gerät nach Status	Dieses Widget zeigt ein Ringdiagramm an, das den aktuellen Status von ESXi-Geräten darstellt. Es gibt vier mögliche Werte: *OK*, *Warnung*, *Fehler* und *Unbekannt*. Wenn Sie auf den Widget-Titel klicken, wird ein neuer VMware-Bestandsbericht angezeigt,

Widget	Beschreibung
	in dem alle ESXi-Geräte nach aktuellem Status aufgelistet sind.
Anzahl der VMware ESXi-Versionen	Dieses Widget zeigt die Anzahl der fünf wichtigsten ESXi-Versionen an. Wenn Sie auf den Widget-Titel klicken, wird ein neuer VMware-Bestandsbericht angezeigt, der alle ESXi-Geräte nach Version auflistet.

Dashboard „Bestand“ anpassen

Sie können das Dashboard anpassen und Widgets nach Bedarf ein- oder ausblenden.

1. Rufen Sie das *Dashboard* auf.
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Inventar** und anschließend auf **Dashboard**.
2. Fahren Sie mit dem Mauszeiger über das Widget und verwenden Sie anschließend die folgenden Schaltflächen:
   - : Die Informationen im Widget aktualisieren
   - : Die Informationen zum Widget anzeigen
   - : Das Widget ausblenden
   - : Die Größe des Widgets ändern
   - : Das Widget an eine andere Position auf der Seite ziehen.
3. Klicken Sie auf die Schaltfläche **Anpassen** in der oberen rechten Ecke der Seite, um die verfügbaren Widgets anzuzeigen.
4. Um ein Widget anzuzeigen, das derzeit ausgeblendet ist, klicken Sie auf **Installieren**.

Verwenden der Geräteerkennung

Mithilfe der Geräteerkennung können Sie mit Ihrem Netzwerk verbundene Geräte ermitteln und Informationen zu diesen Geräten abrufen.

Auf der Grundlage der Erkennungsergebnisse können Sie Geräte mit Labels versehen oder dem Inventar hinzufügen.

Informationen zu Geräteerkennung und -verwaltung

Zu den Geräten, die erkannt werden können, gehören Laptops, Desktops, Server, Mobilgeräte, virtuelle Geräte, Drucker, Netzwerkgeräte, Drahtloszugriffspunkte, Router, Switches und mehr.

Diese Geräte können auch dann erkannt werden, wenn sie nicht über den KACE Agent verfügen. Sie können Erkennungsscans nach Bedarf durchführen oder die Ausführung von Scans zu bestimmten Zeiten planen.

Die Erkennungsergebnisse zeigen die Verfügbarkeit sowie Details von Geräten an. Nachdem Geräte erkannt wurden, können Sie dem Inventar Geräte wie folgt hinzufügen:

- **Durch Installieren des KACE Agent auf Geräten**. Der KACE Agent kann auf Geräten unter Windows, Red Hat®, SUSE® und Ubuntu® sowie auf Mac® Geräten installiert werden. Siehe Provisionierung des KACE Agent.
- **Durch Aktivieren der Verwaltung ohne Agent auf Geräten**. Die Verwaltung ohne Agent ist besonders bei Geräten nützlich, auf denen der KACE Agent nicht installiert werden kann, beispielsweise bei Geräten mit nicht unterstützten Betriebssystemen. Siehe Geräte ohne Agent verwalten.

Nachverfolgen von Änderungen an Erkennungseinstellungen

Wenn Verlaufsabonnements zur Aufbewahrung von Informationen konfiguriert wurden, können Sie Details zu den an Einstellungen, Assets und Objekten vorgenommenen Änderungen anzeigen.

Diese Informationen beinhalten auch das Datum der Änderung und den Benutzer, der diese vorgenommen hat. Dies kann bei der Fehlerbehebung nützlich sein. Siehe Informationen zu den Verlaufseinstellungen.

Erkennen von Geräten im Netzwerk

Zur Erkennung von Geräten können Sie einen Erkennungszeitplan erstellen und Ihr Netzwerk durchsuchen. Im Erkennungszeitplan sind die während des Scans zu verwendenden Protokolle, der zu überprüfende IP-Adressbereich sowie die Scan-Häufigkeit festgelegt.

Je nachdem, welches Ergebnis Sie mit dem Erkennungsscan erzielen möchten und mit welchen Geräten Sie arbeiten, können Sie aus verschiedenen Erkennungsscantypen wählen.

- **Schnelle "Was und wo"-Erkennung**: Siehe Erkennungszeitplan für die Durchführung eines schnellen „Was und wo“-Scans in Ihrem Netzwerk hinzufügen.
- **Gründliche Erkennung**: Verwenden Sie diesen Erkennungstyp, um mehr Geräteinformationen zu erhalten als bei der "Was und wo"-Erkennung. Siehe Erkennungszeitplan für einen umfassenden Scan von verwalteten Windows, Mac, Linux und UNIX Computern hinzufügen.
- **Externe Integrationserkennung**: Eine andere Art der gründlichen Erkennung, die auf bestimmte Computer mit anderen Betriebssystemen als Windows, Mac OS X oder Linux ausgelegt ist. Weitere Informationen finden Sie unter:
  - Hinzufügen eines Erkennungszeitplans für ein KACE Cloud Mobile Device Manager-Gerät
  - Erkennungszeitplan für ein G-Suite-Gerät hinzufügen
  - Erkennungszeitplan für ein Workspace ONE-Gerät hinzufügen
- **Nicht-Computer-Erkennung**: Siehe Hinzufügen eines Erkennungszeitplans für SNMP-fähige computerfremde Geräte.

Sie können in einem oder in mehreren Subnetzen nach Geräten suchen. Außerdem können Sie einen Scan definieren, der nach Geräten sucht, die einen bestimmten Port überwachen.

Wenn Sie Erkennungszeitpläne erstellen, sollten Sie den Umfang des Scans (Anzahl der überprüften IP-Adressen) und die Scan-Tiefe (Anzahl der überprüften Attribute) gegeneinander abwägen, um das Netzwerk und die Appliance nicht zu überlasten. Wenn Sie zum Beispiel häufig eine große Anzahl von IP-Adressen überprüfen müssen, sollten Sie die Anzahl der Ports, TCP/IP-Verbindungen usw. verhältnismäßig klein halten. Ein Subnetz sollte maximal alle paar Stunden überprüft werden.

Erkennungszeitplan für die Durchführung eines schnellen „Was und wo“-Scans in Ihrem Netzwerk hinzufügen

Verwenden Sie einen der verfügbaren Zeitpläne, um schnell Ermittlungsergebnisse abzurufen, die die Verfügbarkeit von Geräten anzeigen.

Dieser Erkennungstyp scannt Ihr Netzwerk nach beliebigen Gerätetypen: verwaltete Computer oder computerfremde Geräte.

Wenn Sie einen Nmap-Erkennungszeitplan hinzufügen möchten, müssen Sie einige Punkte beachten. Siehe Bei der Nmap-Erkennung zu berücksichtigende Aspekte.

1. Rufen Sie die Seite *Detail zum Erkennungszeitplan* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Inventar** und anschließend auf **Erkennungszeitpläne**.
   c. Wählen Sie **Aktion auswählen** > **Neu**.
2. Wählen Sie den *Erkennungstyp* aus, um das Formular mit den entsprechenden Optionen anzuzeigen.

   Abhängig vom ausgewählten Typ werden die folgenden Optionen vor dem Abschnitt *Benachrichtigen* angezeigt:

   - **Ping**. Erkennungsoptionen für *DNS-Lookup* und *Ping* werden angezeigt.
   - **Socket**. Erkennungsoptionen für *DNS-Lookup* und *Socket* werden angezeigt.
   - **Active Directory**. Erkennungsoptionen für *DNS-Lookup* und *Active Directory* werden angezeigt.
   - **Externe Integration [KACE Cloud Mobile Device Manager, G Suite, Workspace ONE]**. Erkennungsoptionen für *KACE Cloud Mobile Device Manager*, *G Suite* und *Workspace ONE* werden angezeigt.

     HINWEIS: Geräte, die durch externe Integration erkannt werden, wie KACE Mobile Device Manager-, G Suite- oder Workspace ONE-Geräte, werden nicht auf das Lizenzlimit der Appliance angerechnet.
   - **Authentifiziert [WinRM, SNMP, SSH, VMware, Hyper-V]**. Erkennungsoptionen für *DNS Lookup*, *Relay*, *WinRM, Hyper-V, VMM*, *SNMP*, *SSH* und *VMware* werden angezeigt.
   - **Nmap**. Erkennungsoptionen für *DNS-Lookup* und *Nmap* werden angezeigt.
   - **Benutzerdefiniert**. Erkennungsoptionen für *DNS Lookup*, *Ping*, **Nmap**, *WinRM*, *SNMP*, *SSH* und *VMware* Erkennungsoptionen werden angezeigt.
3. Geben Sie im Feld *Name* einen Namen für den Scan ein:

   Dieser Name wird auf der Seite *Erkennungszeitpläne* angezeigt.
4. Geben Sie im Feld *IP-Adressbereich* den zu scannenden IP-Adressbereich ein. Verwenden Sie Bindestriche, um einzelne Bereiche von IP-Adressklassen anzugeben. Geben Sie beispielsweise 192.168.2-5.1-200 ein, um nach allen IP-Adressen von 192.168.2-5.1 bis einschließlich 192.168.2-5.200 zu suchen.

   TIPP: Die Appliance unterstützt sowohl IPv6- (Internet Protocol Version 6) als auch IPv4-Adressen.

VORSICHT: Ein Maximum von 25.000 IP-Adressen wird unterstützt. Wenn Sie einen IP-Bereich angeben, der mehr als 25.000 Adressen enthält, wird eine Warnmeldung angezeigt, wenn Sie versuchen, den Provisionierungszeitplan zu speichern.

5. Wählen Sie die Erkennungsoptionen aus. Die angezeigten Optionen sind abhängig vom ausgewählten Erkennungstyp:

Option	Element	Beschreibung
DNS-Lookup		Aktiviert die Erkennung, um den Namen des Geräts zu ermitteln. Das DNS-Lookup ist wichtig, wenn Gerätenamen in den Erkennungsergebnissen und Inventarlisten angezeigt werden sollen. Sie können die Optionen für DNS-Lookup für die jeweiligen Erkennungstypen auswählen.
	DNS-Server für Lookup	Die IP-Adresse oder der Hostname des DNS-Servers **TIPP:** Die Appliance unterstützt sowohl IPv6- (Internet Protocol Version 6) als auch IPv4-Adressen.
	Timeout	Die Zeit in Sekunden, nach der das Zeitlimit für DNS-Lookup abläuft. Wenn während dieser Zeit keine Adresse gefunden wird, tritt ein Timeout des Vorgangs auf.
Relay		Aktivieren Sie einen KACE Agent, der als Tunnel für den WinRM-, SSH- und SNMP-Datenverkehr zum Agent-Verbindungsprotokoll für WinRM-, SSH- und SNMP-Ermittlungspläne, agentenlose Bestandsaufnahme und Agentenbereitstellung agiert.
	Relay-Gerät	Geben Sie das Gerät an, das als Relay für die agentenlose Geräteinventarisierung verwendet werden soll. Ein Relay-Gerät, das während der Ermittlung verwendet wird, wenn ein neues Gerät von den Ermittlungsergebnissen automatisch durch ein neues Gerät bereitgestellt wird. Ausgewählte Relay-Geräte sind auf den folgenden Seiten aufgeführt: • Auf der Seite *Details zur Geräteverbindung ohne Agent*, wenn ein neues

Option	Element	Beschreibung
		Gerät automatisch aus Ermittlungsergebnissen bereitgestellt wird. Weitere Informationen zu dieser Seite finden Sie unter Verwaltung ohne Agent durch manuelle Eingabe von Geräteinformationen aktivieren. • Auf der Seite *Detail zum Provisionierungszeitplan*, wenn das Agent-Provisioning aus Ermittlungsergebnissen initiiert wird. Weitere Informationen hierzu finden Sie unter KACE Agent auf einem Gerät oder auf mehreren Geräten installieren. • Auf der Seite *Details zur Geräteverbindung ohne Agent*, wenn ein neues Gerät automatisch aus Ermittlungsergebnissen bereitgestellt wird. Weitere Informationen zu dieser Seite finden Sie unter Verwaltung ohne Agent durch manuelle Eingabe von Geräteinformationen aktivieren.
Ping		Führt im Rahmen des Netzwerk-Scans einen Ping-Test durch. Bei diesem Test sendet die Appliance einen Ping-Test, um zu ermitteln, ob ein System reagiert.
Socket		Bei Auswahl dieser Option wird ein Verbindungstest während des Netzwerk-Scans durchgeführt. Während dieses Tests sendet die Appliance ein Paket an den Port, um zu bestimmen, ob der Port geöffnet ist.
	TCP-Port-Liste	Aktiviert einen Port-Scan unter Verwendung von TCP (Transmission Control Protocol). Trennen Sie die einzelnen Port-Nummern jeweils mit einem Komma.

Option	Element	Beschreibung
	UDP-Port-Liste	Aktiviert einen Port-Scan unter Verwendung von UDP (User Datagram Protocol). Trennen Sie die einzelnen Port-Nummern jeweils mit einem Komma.
Active Directory		Veranlasst, dass die Appliance nach Geräteinformationen auf einem Active Directory-Server sucht. Bei Active Directory-Scans wird der Status als ein ungefährer Prozentsatz angegeben anstatt als Anzahl überprüfter Geräte.
	Use Secure LDAP (LDAPS) (Secure LDAP (LDAPS) verwenden)	Ermöglicht der Appliance die Verwendung eines sicheren Ports für die LDAP-Kommunikation.
	Berechtigter Benutzer	Der Benutzername des Administratorkontos auf dem Active Directory-Server. Beispiel: benutzername@beispiel.com.
	Kennwort des berechtigten Benutzers	Das Kennwort des Administratorkontos auf dem Active Directory-Server.
	Suchkontext	Die Kriterien für die Suche nach Geräten. Diese Kriterien geben einen Speicherort oder Container in der Active Directory-Struktur an, der durchsucht werden soll. Geben Sie eine genaue Kombination aus OUs, DCs oder CNs an, die Ihren Kriterien entsprechen, die von links (sehr genau) bis rechts (sehr allgemein) reichen. Beispiel: DC=company,DC=com
KACE Cloud Mobile Device Manager		Mit dieser Option können Sie auf mobile Geräte wie Smartphones und Tablets zugreifen, die mit dem KACE Cloud Mobile Device Manager (MDM) verbunden sind. Sie benötigen einen Mandantennamen und einen Geheimschlüssel von KACE Cloud MDM, um auf die damit verknüpften Geräte zuzugreifen.
	Mandantenname	Der Name des Mandanten im KACE Cloud MDM, der mit den Geräten verknüpft ist, die Sie verwalten möchten.

Option	Element	Beschreibung
	Anmeldeinformationen	Die Details des Kontos, das für die Verbindung mit dem KACE Cloud MDM-Gerät verwendet wird. Wählen Sie vorhandene Anmeldeinformationen in der Dropdown-Liste aus oder wählen Sie **Neue Anmeldeinformationen hinzufügen** aus, um neue Anmeldeinformationen nach Bedarf hinzuzufügen. Weitere Informationen hierzu finden Sie unter Geheimschlüssel-Anmeldeinformationen hinzufügen und bearbeiten.
	Automatische Provisionierung von Geräten	Bei Verwendung dieser Option werden alle beim nächsten Scan erkannten mobilen Geräte dem Inventar hinzugefügt. **HINWEIS:** Verwenden Sie diese Option mit Bedacht, um eine unerwartet umfangreiche Erweiterung Ihres Inventars zu vermeiden.
G Suite		Bei Verwendung von G-Suite-Geräten benötigt die Appliance Anmeldeinformationen, um über die Admin SDK-API auf eine Google Apps-Domain zugreifen zu können. Sie benötigen eine Client-ID und einen geheimen Client-Schlüssel von Google, um einen Genehmigungscode für die Appliance generieren zu können.
	Chrome-Geräte ermitteln	Wenn aktiviert, werden Chrome-Geräte beim nächsten Scan ermittelt.
	Mobile Geräte ermitteln	Wenn aktiviert, werden mobile Geräte der G Suite beim nächsten Scan ermittelt.
	Anmeldeinformationen	Die Details des Kontos, das für die Verbindung mit dem Chrome-Gerät verwendet wird. Wählen Sie vorhandene Anmeldeinformationen in der Dropdown-Liste aus oder wählen Sie **Neue Anmeldeinformationen hinzufügen** aus, um neue Anmeldeinformationen nach Bedarf hinzuzufügen. Das

Option	Element	Beschreibung
		ausgewählte Anmeldeprofil muss über einen Genehmigungscode verfügen, der mit dem entsprechenden Gerätetyp verknüpft werden kann. Wenn Sie beispielsweise mobile Geräte der G Suite ermitteln möchten, können Sie kein Anmeldeprofil verwenden, dessen Genehmigungscode für Chrome-Geräte generiert wurde. Weitere Informationen hierzu finden Sie unter Hinzufügen und Bearbeiten von Google OAuth-Anmeldeinformationen.
	Automatische Provisionierung von Geräten	Bei Verwendung dieser Option werden alle beim nächsten Scan erkannten Geräte vom Typ „Chrome“ und mobile Geräte dem Inventar hinzugefügt. **HINWEIS:** Verwenden Sie diese Option mit Bedacht, um eine unerwartet umfangreiche Erweiterung Ihres Inventars zu vermeiden.
Workspace ONE		VMware® Workspace ONE® ist eine Mobilitätsverwaltungsplattform auf Unternehmensebene, die es Ihnen erlaubt, eine große Zahl unterschiedlicher Gerätetypen zu verwalten.
	Host	Der Host-Name der Workspace ONE-Verwaltungskonsole.
	REST API-Schlüssel	Der REST-API-Schlüssel der in der Workspace ONE-Verwaltungskonsole verfügbar ist. Der Schlüssel muss angegeben werden, damit die Integration von Workspace ONE über API-Aufrufe aktiviert wird.
	Anmeldeinformationen	Die Details des Dienstkontos, die erforderlich sind, um eine Verbindung zum Gerät herzustellen und Befehle auszuführen Wählen Sie vorhandene Anmeldeinformationen in der Dropdown-Liste aus oder wählen Sie **Neue Anmeldeinformationen**

Option	Element	Beschreibung
		hinzufügen aus, um neue Anmeldeinformationen nach Bedarf hinzuzufügen. Siehe Hinzufügen und Bearbeiten von Benutzer-/Kennwort-Anmeldeinformationen.
	Automatische Provisionierung von Geräten	Bei Verwendung dieser Option werden alle beim nächsten Scan erkannten Geräte vom Typ "Workspace ONE" dem Inventar hinzugefügt. **HINWEIS:** Verwenden Sie diese Option mit Bedacht, um eine unerwartet umfangreiche Erweiterung Ihres Inventars zu vermeiden.
WinRM, Hyper-V, VMM		WinRM ist der Verbindungstyp für Windows Geräte.
	Timeout	Die Zeit (maximal 60 Sekunden), nach der eine inaktive Verbindung getrennt wird.
	Kerberos voraussetzen	Bei Verwendung dieser Option ist eine Kerberos-Authentifizierung erforderlich. Wenn Kerberos nicht verfügbar ist, wird NTLM nicht als Alternative verwendet. Für die Verwendung von Kerberos muss in der Erkennungskonfiguration auch DNS-Lookup aktiviert sein. Darüber hinaus muss in den lokalen Netzwerkeinstellungen der Appliance auch der DNS-Server angegeben werden.
	Nach Hyper-V und Virtual Machine Manager suchen	Wenn diese Option ausgewählt ist, importiert die Appliance eine Microsoft Hyper-V- oder System Center Virtual Machine Manager-Infrastruktur mit agentenloser Verwaltung. Weitere Informationen zu dieser Funktion finden Sie unter .
	Port	Ohne Angabe in diesem Feld wird der Standardport 5985 verwendet.
	Anmeldeinformationen	Die Details des Dienstkontos, die erforderlich sind, um

Option	Element	Beschreibung
		eine Verbindung zum Gerät herzustellen und Befehle auszuführen Wählen Sie vorhandene Anmeldeinformationen in der Dropdown-Liste aus oder wählen Sie **Neue Anmeldeinformationen hinzufügen** aus, um neue Anmeldeinformationen nach Bedarf hinzuzufügen. Siehe Hinzufügen und Bearbeiten von Benutzer-/Kennwort-Anmeldeinformationen.
SNMP		SNMP (Simple Network Management Protocol) ist ein Protokoll zum Überwachen von verwalteten Geräten in einem Netzwerk.
	SNMP - vollständiger Durchlauf	Aktiviert auf Geräten einen vollständigen Durchlauf von Daten in der MIB (Management Information Base). Wenn diese Option deaktiviert ist, führt die Appliance einen „Bulk GET“-Vorgang durch, bei dem drei Haupt-OIDs (Objektbezeichner) durchsucht werden. Beachten Sie, dass ein vollständiger Durchlauf pro Gerät bis zu 20 Minuten dauern kann. „Bulk GET“ dauert standardmäßig etwa eine Sekunde und erfasst sämtliche Informationen, die zur Erkennung erforderlich sind. **WICHTIG: Beim SNMP-Inventardurchlauf werden auf Windows-Geräten keine nicht-englischen Zeichen unterstützt. Werden nicht-englische Zeichen erkannt, meldet die SNMP-Inventarisierung einen Fehler und beendet das Laden von Inventarinformationen.**
	Timeout	Die Zeit (in Sekunden), nach der der Scan endet, falls keine Reaktion erfolgt.
	Maximale Anzahl Versuche	Die Anzahl der Verbindungsversuche.

Option	Element	Beschreibung
	Anmeldeinformationen (SNMPV1/V2):	Die Details der SNMP v1/v2-Anmeldeinformationen, die erforderlich sind, um eine Verbindung zum Gerät herzustellen und Befehle auszuführen. Wählen Sie vorhandene Anmeldeinformationen in der Dropdown-Liste aus oder wählen Sie **Neue Anmeldeinformationen hinzufügen** aus, um neue Anmeldeinformationen nach Bedarf hinzuzufügen. Siehe Hinzufügen und Bearbeiten von SNMP-Anmeldeinformationen.
	Anmeldeinformationen (SNMPV3):	Die Details der SNMP v3-Anmeldeinformationen, die erforderlich sind, um eine Verbindung zum Gerät herzustellen und Befehle auszuführen. Wählen Sie vorhandene Anmeldeinformationen in der Dropdown-Liste aus oder wählen Sie **Neue Anmeldeinformationen hinzufügen** aus, um neue Anmeldeinformationen nach Bedarf hinzuzufügen. Siehe Hinzufügen und Bearbeiten von SNMP-Anmeldeinformationen.
SSH		Verwenden Sie das SSH-Protokoll mit Authentifizierung. **WICHTIG: Sobald ein Erkennungszeitplan gespeichert wurde, können Sie SSH-Authentifizierung nicht mehr in SNMP-Authentifizierung ändern.**
	Timeout	Die Zeit (maximal fünf Minuten), nach der eine inaktive Verbindung getrennt wird.
	SSH2-Verbindung versuchen	Aktiviert das SSH2-Protokoll zur Verbindung und Kommunikation mit Geräten. Verwenden Sie SSH2, wenn Sie eine sicherere

Option	Element	Beschreibung
		Gerätekommunikation wünschen (empfohlen).
	Anmeldeinformationen	Die Details des Dienstkontos, die erforderlich sind, um eine Verbindung zum Gerät herzustellen und Befehle auszuführen Wählen Sie vorhandene Anmeldeinformationen in der Dropdown-Liste aus oder wählen Sie **Neue Anmeldeinformationen hinzufügen** aus, um neue Anmeldeinformationen nach Bedarf hinzuzufügen. Siehe Hinzufügen und Bearbeiten von Benutzer-/Kennwort-Anmeldeinformationen.
VMware	Timeout	Die Zeit, nach der der Scan endet, falls keine Reaktion erfolgt.
	Anmeldeinformationen	Die Details des Dienstkontos, die erforderlich sind, um eine Verbindung zum Gerät herzustellen und Befehle auszuführen Wählen Sie vorhandene Anmeldeinformationen in der Dropdown-Liste aus oder wählen Sie **Neue Anmeldeinformationen hinzufügen** aus, um neue Anmeldeinformationen nach Bedarf hinzuzufügen. Siehe Hinzufügen und Bearbeiten von Benutzer-/Kennwort-Anmeldeinformationen.
Nmap		**HINWEIS:** Das gleichzeitige Ausführen mehrerer der vier Nmap-Erkennungstypen ist zwar möglich, aber nicht empfehlenswert. Mögliche Folgen sind eine Verlängerung der Ausführungszeit sowie falsche Ergebnisse bei der Betriebssystemerkennung.
	Timeout	Die Zeit, nach der der Scan endet, falls keine Reaktion erfolgt.
	Schneller Scan	Ermöglicht das schnelle Scannen von 100 häufig verwendeten Ports

Option	Element	Beschreibung
		durch die die Appliance. Ist diese Option deaktiviert, werden alle verfügbaren TCP-Ports gescannt, was wesentlich länger dauern kann als der schnelle Scan.
	Nmap-Betriebssystemerkennung (bestmögliche Vermutung)	Hiermit wird es der Appliance ermöglicht, das Betriebssystem des Geräts auf der Basis von Fingerabdruck- und Port-Informationen zu ermitteln. Diese Option kann die für den Scan erforderliche Zeit erhöhen.
	TCP-Port-Scan	Ermöglicht einen Transmission Control Protocol-basierten Port-Scan von 1000 häufig verwendeten TCP-Ports. Wenn diese Option deaktiviert ist und UPD ausgewählt wird, führt die Appliance einen UDP-Scan durch. Wenn sowohl TCP als auch UDP deaktiviert sind, führt die Appliance einen TCP-Scan durch. Bei Verwendung dieser Option empfiehlt es sich, den Wert für *Timeout* auf 10 Minuten festzulegen, um das Fehlerrisiko zu senken. Kombinieren Sie diesen Scan nicht mit der Option *Schneller Scan*. Andernfalls werden lediglich 100 häufig verwendete Ports gescannt.
	UDP-Port-Scan	Ermöglicht einen User Datagram Protocol-basierten Port-Scan von bis zu 1000 UDP-Ports. UDP-Scans sind in der Regel weniger zuverlässig und haben eine geringere Prozessorverarbeitungszeit als TCP-Scans, da bei TCP ein Handshake zur Kommunikation mit Geräten erforderlich ist, bei UDP jedoch nicht. UDP-Scans können jedoch mehr Zeit in Anspruch nehmen als TCP-Scans, da UDP zur Erkennung von Ports mehrere Pakete sendet, während TCP nur ein einziges Paket sendet. Bei Verwendung dieser Option empfiehlt es sich, den Wert für *Timeout* auf 30 Minuten

Option	Element	Beschreibung
		festzulegen, um das Fehlerrisiko zu senken. Kombinieren Sie diesen Scan nicht mit der Option *Schneller Scan*. Andernfalls werden lediglich 100 häufig verwendete Ports gescannt. Wenn diese Option deaktiviert ist, führt die Appliance keine Port-Scans mithilfe von UDP durch.

6. **Optional**: Geben Sie eine E-Mail-Adresse ein, um sich bei Abschluss des Erkennungsscans benachrichtigen zu lassen. Die E-Mail enthält den Namen des Erkennungszeitplans.
7. Legen Sie den Scan-Zeitplan fest:

TIPP: Zum Verwalten des Scan-Inventars ohne Überprüfen legen Sie den Zeitplan der Scan-Konfiguration auf **Keine**.

Option	Beschreibung
Kein(e)	Die Ausführung erfolgt im Zusammenhang mit einem Ereignis anstatt zu einem bestimmten Datum oder zu einem bestimmten Zeitpunkt.
jede Stunde	Der Vorgang wird im angegebenen Intervall durchgeführt.
Täglich/an einem bestimmten Tag um HH:MM	Die Erfassung wird täglich zu einem bestimmten Zeitpunkt oder an einem bestimmten Wochentag um eine bestimmte Uhrzeit ausgeführt.
Ausführen am n-ten jedes Monats/eines bestimmten Monats um HH:MM	Die Erfassung wird jeden Monat oder in einem bestimmten Monat an einem festgelegten Datum zu einer festgelegten Uhrzeit ausgeführt.
Ausführen am n-ten Wochentag **jedes Monats/ eines bestimmten Monats um HH:MM**	Die Erfassung wird jeden Monat oder in einem bestimmten Monat an einem festgelegten Wochentag zu einer festgelegten Uhrzeit ausgeführt.

Benutzerdefiniert	Führen Sie die Erfassung nach einem benutzerdefinierten Zeitplan aus.
	Verwenden Sie das Standard-5-Feld-Cron-Format (das erweiterte Cron-Format wird nicht unterstützt):
	`* * * * *`
	`| | | | +————Wochentag (0-6) (Sonntag=0)`
	`| | | +————Monat (1-12)`
	`| | +————Monatstag (1-31)`
	`| +————Stunde (0-23)`
	`+————Minute (0-59)`

Option	Beschreibung
	Verwenden Sie bei der Angabe von Werten die folgenden Zeichen: • **Leerzeichen( )**: Die einzelnen Felder mit einem Leerzeichen trennen. • **Sternchen (*)**: Ein Sternchen repräsentiert den gesamten Wertebereich in einem Feld. Zum Beispiel repräsentiert ein Sternchen im Stundenfeld eine beliebige Stunde. • **Kommas (,)**: Mehrere Werte in einem Feld werden mit einem Komma getrennt. Zum Beispiel werden mit `0,6` im Feld „Wochentag“ Sonntag und Samstag angegeben. • **Bindestriche (-)**: Mit einem Bindestrich wird ein Wertebereich in einem Feld angegeben. Zum Beispiel entspricht `1-5` im Feld „Wochentag“ `1,2,3,4,5`, d. h. Montag bis Freitag. • **Schrägstriche (/)**: Die Angabe der Zeitabstände, mit denen eine Aktion wiederholt werden soll, erfolgt mit einem Schrägstrich. Zum Beispiel entspricht `*/3` im Feld Stunde `0,3,6,9,12,15,18,21`. Das Sternchen (`*`) gibt jede Stunde an, mit `/3` erfolgt aber eine Einschränkung auf durch drei teilbare Stunden. Beispiele: • `15 * * * * Jeden Tag 15 Minuten nach jeder vollen Stunde ausführen` • `0 22 * * * Jeden Tag um 22:00 Uhr ausführen` • `0 0 1 1,6 * Am 1. Januar und 1. Juni um 00:00 Uhr ausführen` • `30 8,12 * * 1-5 An Wochentagen um 08:30 Uhr und 12:30 Uhr ausführen` • `0 2 */2 * * Jeden zweiten Tag um 02:00 Uhr ausführen`
Aufgabenplan anzeigen	Klicken Sie, um den Aufgabenplan anzuzeigen. Im Dialogfeld *Aufgabenplan* wird eine Liste der geplanten Aufgaben angezeigt. Klicken Sie auf eine Aufgabe, um die Aufgabendetails anzuzeigen. Weitere Informationen hierzu finden Sie unter Aufgabenpläne anzeigen.

8. Klicken Sie auf **Speichern**.

Verwandte Themen

Informationen zu Erkennungsergebnissen

Erkennungsergebnisse anzeigen und durchsuchen

Laufenden Erkennungsscan anhalten

Erkennungszeitpläne löschen

Bei der Nmap-Erkennung zu berücksichtigende Aspekte

Für eine erfolgreiche Nmap-Erkennung müssen einige Punkte und Best Practices beachtet werden. Dadurch können Sie die Geschwindigkeit und Genauigkeit steigern und Probleme vermeiden.

Best Practices zum Steigern der Geschwindigkeit und Genauigkeit bei der Erkennung

So steigern Sie die Geschwindigkeit und Genauigkeit bei der Nmap-Erkennung:

- **Nicht DNS-Lookup verwenden**. *DNS-Lookup* kann den Scanvorgang um bis zu 500 Prozent verlangsamen, wenn für den DNS-Server eine ungültige oder nicht erreichbare IP-Adresse angegeben wurde.
- **Jeweils nur einen Erkennungstyp ausführen**. Sie können zwar mehrere Erkennungstypen gleichzeitig ausführen, möglicherweise verlängert sich dadurch jedoch die Ausführungszeit oder es werden falsche Ergebnisse bei der Betriebssystemerkennung zurückgegeben.
- **„Nmap-Betriebssystemerkennung (bestmögliche Vermutung)“ auswählen, wenn Sie unsicher sind, welchen Typ Sie ausführen sollen**. Diese Auswahloption vermittelt einen angemessenen Einblick in Ihre Subnetze. Mithilfe der bestmöglichen Vermutung wird mindestens ermittelt, welche Betriebssysteme sich auf welchen Geräten befinden. Wenn die Ergebnisse nicht Ihren Erwartungen entsprechen (weil beispielsweise das *Betriebssystem* einiger Geräte *nicht erkannt* wird), wiederholen Sie die Erkennung mit einem höheren Timeout-Wert.
- **Die Erkennung funktioniert über ein VPN nicht ordnungsgemäß**. Verwenden Sie eine andere Quelle für den Gerätezugriff.

Probleme, die die Erkennung beeinträchtigen können

Geräte, die zum Zeitpunkt des Scans offline sind oder auf die aus einem anderen Grund nicht zugegriffen werden kann, werden ignoriert, da sie scheinbar nicht vorhanden sind.

Sollten also Geräte vorhanden sein, die eigentlich hätten erkannt werden müssen, gibt es folgende Möglichkeiten:

- Das Gerät wird durch eine Firewall blockiert.
- Das Gerät blockiert aktiv Pings.
- Das Gerät ist offline (ohne Strom).
- Das Gerät verhindert durch verschiedene Methoden die Fingerabdruckerzeugung.

Einige Geräte (insbesondere Sicherheitsgeräte) machen sich unsichtbar oder täuschen das System, damit sie nicht erkannt werden.

Fehlerbehebung bei unbekannten Betriebssystemen

Falls das *Betriebssystem* auf der Listenseite mit den *Erkennungsergebnissen* als *unbekannt* angegeben wird, haben Sie folgende Möglichkeiten:

- Vergewissern Sie sich, dass in der Spalte *Nmap* das Nmap-Häkchen gesetzt ist. Andernfalls war das Gerät während des Scanvorgangs offline und das Betriebssystem konnte nicht ermittelt werden.
- Falls das Nmap-Häkchen gesetzt ist, das *Betriebssystem* aber trotzdem nicht erkannt wurde, ist dies meistens darauf zurückzuführen, dass die Ports, die Nmap zur Ermittlung des Gerätebetriebssystems verwendet, durch eine Firewall blockiert werden.

  Wenn Sie für den Scan beispielsweise nur die UDP-Ports 7 und 161 verwenden, wird das Gerät als online und mit gesetztem Nmap-Häkchen angezeigt. Das *Betriebssystem* wird jedoch *nicht erkannt*, da das Betriebssystem eines Geräts nicht allein über die UDP-Ports ermittelt werden kann.

Erkennungszeitplan für einen umfassenden Scan von verwalteten Windows, Mac, Linux und UNIX Computern hinzufügen

Mit Erkennungszeitplänen können Sie Ihr Netzwerk nach Geräten durchsuchen und Informationen zu Geräten erfassen. Nach der Erkennung der Geräte mit dem Erkennungstyp „Active Directory“ oder „Authentifiziert“ können Sie die erkannten Geräte dem Inventar hinzufügen.

1. Rufen Sie die Seite *Detail zum Erkennungszeitplan* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Inventar** und anschließend auf **Erkennungszeitpläne**.
   c. Wählen Sie **Aktion auswählen > Neu**.
2. Wählen Sie den *Erkennungstyp* aus, um das Formular mit den entsprechenden Optionen anzuzeigen.

   Abhängig vom ausgewählten Typ werden die folgenden Optionen vor dem Abschnitt *Benachrichtigen* angezeigt:

   - **Active Directory**. Erkennungsoptionen für *DNS-Lookup* und *Active Directory* werden angezeigt.
   - **Authentifiziert [WinRM, SNMP, SSH, VMware, Hyper-V]**. Erkennungsoptionen für *DNS Lookup*, *Relay*, *WinRM, Hyper-V, VMM*, *SNMP*, *SSH* und *VMware* werden angezeigt.
3. Geben Sie im Feld *Name* einen Namen für den Scan ein:

   Dieser Name wird auf der Seite *Erkennungszeitpläne* angezeigt.
4. Führen Sie im Feld *IP-Adressbereich* einen der folgenden Schritte aus:

   - **Wenn Sie den Erkennungstyp** *Active Directory* **auswählen, geben Sie die IP-Adresse des zu scannenden Active Directory-Servers ein.**
   - **Geben Sie einen IP-Adressbereich ein, der überprüft werden soll. Verwenden Sie Bindestriche, um individuelle IP-Adressklassenbereiche anzugeben. Geben Sie beispielsweise 192.168.2-5.1-200 ein, um nach allen IP-Adressen von 192.168.2-5.1 bis einschließlich 192.168.2-5.200 zu suchen.**

   TIPP: Die Appliance unterstützt sowohl IPv6- (Internet Protocol Version 6) als auch IPv4-Adressen.

   VORSICHT: Ein Maximum von 25.000 IP-Adressen wird unterstützt. Wenn Sie einen IP-Bereich angeben, der mehr als 25.000 Adressen enthält, wird eine Warnmeldung angezeigt, wenn Sie versuchen, den Provisionierungszeitplan zu speichern.
5. Wählen Sie die Erkennungsoptionen aus. Die angezeigten Optionen sind abhängig vom ausgewählten Erkennungstyp:

Option	Element	Beschreibung
DNS-Lookup		Aktiviert die Erkennung, um den Namen des Geräts zu ermitteln. Das DNS-Lookup ist wichtig, wenn Gerätenamen in den Erkennungsergebnissen und Inventarlisten angezeigt werden sollen. Sie können die Optionen

Option	Element	Beschreibung
		für DNS-Lookup für die jeweiligen Erkennungstypen auswählen.
	DNS-Server für Lookup	Die IP-Adresse oder der Hostname des DNS-Servers **TIPP:** Die Appliance unterstützt sowohl IPv6- (Internet Protocol Version 6) als auch IPv4-Adressen.
	Timeout	Die Zeit in Sekunden, nach der das Zeitlimit für DNS-Lookup abläuft. Wenn während dieser Zeit keine Adresse gefunden wird, tritt ein Timeout des Vorgangs auf.
Relay		Aktivieren Sie einen KACE Agent, der als Tunnel für den WinRM-, SSH- und SNMP-Datenverkehr zum Agent-Verbindungsprotokoll für WinRM-, SSH- und SNMP-Ermittlungspläne, agentenlose Bestandsaufnahme und Agentenbereitstellung agiert.
	Relay-Gerät	Geben Sie das Gerät an, das als Relay für die agentenlose Geräteinventarisierung verwendet werden soll. Ein Relay-Gerät, das während der Ermittlung verwendet wird, wenn ein neues Gerät von den Ermittlungsergebnissen automatisch durch ein neues Gerät bereitgestellt wird. Ausgewählte Relay-Geräte sind auf den folgenden Seiten aufgeführt: • Auf der Seite *Details zur Geräteverbindung ohne Agent*, wenn ein neues Gerät automatisch aus Ermittlungsergebnissen bereitgestellt wird. Weitere Informationen zu dieser Seite finden Sie unter Verwaltung ohne Agent durch manuelle Eingabe von Geräteinformationen aktivieren. • Auf der Seite *Detail zum Provisionierungszeitplan*, wenn das Agent-Provisioning aus

Option	Element	Beschreibung
		Ermittlungsergebnissen initiiert wird. Weitere Informationen hierzu finden Sie unter KACE Agent auf einem Gerät oder auf mehreren Geräten installieren. • Auf der Seite *Details zur Geräteverbindung ohne Agent*, wenn ein neues Gerät automatisch aus Ermittlungsergebnissen bereitgestellt wird. Weitere Informationen zu dieser Seite finden Sie unter Verwaltung ohne Agent durch manuelle Eingabe von Geräteinformationen aktivieren.
Active Directory		Veranlasst, dass die Appliance nach Geräteinformationen auf einem Active Directory-Server sucht. Bei Active Directory-Scans wird der Status als ein ungefährer Prozentsatz angegeben anstatt als Anzahl überprüfter Geräte.
	Use Secure LDAP (LDAPS) (Secure LDAP (LDAPS) verwenden)	Ermöglicht der Appliance die Verwendung eines sicheren Ports für die LDAP-Kommunikation.
	Berechtigter Benutzer	Der Benutzername des Administratorkontos auf dem Active Directory-Server. Beispiel: benutzername@beispiel.com.
	Kennwort des berechtigten Benutzers	Das Kennwort des Administratorkontos auf dem Active Directory-Server.
	Suchkontext	Die Kriterien für die Suche nach Geräten. Diese Kriterien geben einen Speicherort oder Container in der Active Directory-Struktur an, der durchsucht werden soll. Geben Sie eine genaue Kombination aus OUs, DCs oder CNs an, die Ihren Kriterien entsprechen, die von links (sehr genau) bis rechts (sehr allgemein) reichen. Beispiel: `DC=Unternehmen, DC=com`.

Option	Element	Beschreibung
WinRM, Hyper-V, VMM		WinRM ist der Verbindungstyp für Windows Geräte.
	Timeout	Die Zeit (maximal 60 Sekunden), nach der eine inaktive Verbindung getrennt wird.
	Kerberos voraussetzen	Bei Verwendung dieser Option ist eine Kerberos-Authentifizierung erforderlich. Wenn Kerberos nicht verfügbar ist, wird NTLM nicht als Alternative verwendet. Für die Verwendung von Kerberos muss in der Erkennungskonfiguration auch DNS-Lookup aktiviert sein. Darüber hinaus muss in den lokalen Netzwerkeinstellungen der Appliance auch der DNS-Server angegeben werden.
	Nach Hyper-V und Virtual Machine Manager suchen	Dieses Feld wird nur verwendet, wenn Sie eine Microsoft Hyper-V- oder System Center Virtual Machine Manager-Infrastruktur überwachen möchten. Stellen Sie sicher, dass diese Option deaktiviert ist. Weitere Informationen zu dieser Funktion finden Sie unter .
	Port	Ohne Angabe in diesem Feld wird der Standardport 5985 verwendet.
	Anmeldeinformationen	Die Details des Dienstkontos, die erforderlich sind, um eine Verbindung zum Gerät herzustellen und Befehle auszuführen Wählen Sie vorhandene Anmeldeinformationen in der Dropdown-Liste aus oder wählen Sie **Neue Anmeldeinformationen hinzufügen** aus, um nicht bereits aufgeführte Anmeldeinformationen hinzuzufügen. Siehe Hinzufügen und Bearbeiten von Benutzer-/Kennwort-Anmeldeinformationen.
SSH		Verwenden Sie das SSH-Protokoll mit Authentifizierung.

Option	Element	Beschreibung
		HINWEIS: Sobald ein Erkennungszeitplan gespeichert wurde, können Sie SSH-Authentifizierung nicht mehr in SNMP-Authentifizierung ändern.
	Timeout	Die Zeit (maximal fünf Minuten), nach der eine inaktive Verbindung getrennt wird.
	SSH2-Verbindung versuchen	Aktiviert das SSH2-Protokoll zur Verbindung und Kommunikation mit Geräten. Verwenden Sie SSH2, wenn Sie eine sicherere Gerätekommunikation wünschen (empfohlen).
	Anmeldeinformationen	Die Details des Dienstkontos, die erforderlich sind, um eine Verbindung zum Gerät herzustellen und Befehle auszuführen Wählen Sie vorhandene Anmeldeinformationen in der Dropdown-Liste aus oder wählen Sie **Neue Anmeldeinformationen hinzufügen** aus, um nicht bereits aufgeführte Anmeldeinformationen hinzuzufügen. Siehe Hinzufügen und Bearbeiten von Benutzer-/Kennwort-Anmeldeinformationen.

6. **Optional**: Geben Sie eine E-Mail-Adresse ein, um sich bei Abschluss des Erkennungsscans benachrichtigen zu lassen. Die E-Mail enthält den Namen des Erkennungszeitplans.
7. Legen Sie den Scan-Zeitplan fest:

TIPP: Zum Verwalten des Scan-Inventars ohne Überprüfen legen Sie den Zeitplan der Scan-Konfiguration auf **Keine**.

Option	Beschreibung
Kein(e)	Die Ausführung erfolgt im Zusammenhang mit einem Ereignis anstatt zu einem bestimmten Datum oder zu einem bestimmten Zeitpunkt.
jede Stunde	Der Vorgang wird im angegebenen Intervall durchgeführt.
Täglich/an einem bestimmten Tag um HH:MM	Die Erfassung wird täglich zu einem bestimmten Zeitpunkt oder an einem bestimmten Wochentag um eine bestimmte Uhrzeit ausgeführt.

Option	Beschreibung
Ausführen am n-ten jedes Monats/eines bestimmten Monats um HH:MM	Die Erfassung wird jeden Monat oder in einem bestimmten Monat an einem festgelegten Datum zu einer festgelegten Uhrzeit ausgeführt.
Ausführen am n-ten Wochentag **jedes Monats/ eines bestimmten Monats um HH:MM**	Die Erfassung wird jeden Monat oder in einem bestimmten Monat an einem festgelegten Wochentag zu einer festgelegten Uhrzeit ausgeführt.

Benutzerdefiniert	Führen Sie die Erfassung nach einem benutzerdefinierten Zeitplan aus.
	Verwenden Sie das Standard-5-Feld-Cron-Format (das erweiterte Cron-Format wird nicht unterstützt):
	`* * * * *`
	`| | | | +————————Wochentag (0-6) (Sonntag=0)`
	`| | | +————————Monat (1-12)`
	`| | +————————Monatstag (1-31)`
	`| +————————Stunde (0-23)`
	`+————————Minute (0-59)`
	Verwenden Sie bei der Angabe von Werten die folgenden Zeichen:
	• **Leerzeichen( )**: Die einzelnen Felder mit einem Leerzeichen trennen.
	• **Sternchen (*)**: Ein Sternchen repräsentiert den gesamten Wertebereich in einem Feld. Zum Beispiel repräsentiert ein Sternchen im Stundenfeld eine beliebige Stunde.
	• **Kommas (,)**: Mehrere Werte in einem Feld werden mit einem Komma getrennt. Zum Beispiel werden mit `0,6` im Feld „Wochentag“ Sonntag und Samstag angegeben.
	• **Bindestriche (-)**: Mit einem Bindestrich wird ein Wertebereich in einem Feld angegeben. Zum Beispiel entspricht `1-5` im Feld „Wochentag“ `1,2,3,4,5`, d. h. Montag bis Freitag.
	• **Schrägstriche (/)**: Die Angabe der Zeitabstände, mit denen eine Aktion wiederholt werden soll, erfolgt mit einem Schrägstrich. Zum Beispiel entspricht `*/3` im Feld Stunde `0,3,6,9,12,15,18,21`. Das Sternchen (`*`) gibt jede Stunde an, mit `/3` erfolgt aber eine Einschränkung auf durch drei teilbare Stunden.

Option	Beschreibung
	Beispiele: • `15 * * * *` Jeden Tag 15 Minuten nach jeder vollen Stunde ausführen • `0 22 * * *` Jeden Tag um 22:00 Uhr ausführen • `0 0 1 1,6 *` Am 1. Januar und 1. Juni um 00:00 Uhr ausführen • `30 8,12 * * 1-5` An Wochentagen um 08:30 Uhr und 12:30 Uhr ausführen • `0 2 */2 * *` Jeden zweiten Tag um 02:00 Uhr ausführen
Aufgabenplan anzeigen	Klicken Sie, um den Aufgabenplan anzuzeigen. Im Dialogfeld *Aufgabenplan* wird eine Liste der geplanten Aufgaben angezeigt. Klicken Sie auf eine Aufgabe, um die Aufgabendetails anzuzeigen. Weitere Informationen hierzu finden Sie unter Aufgabenpläne anzeigen.

8. Klicken Sie auf **Speichern**.

Verwandte Themen

Informationen zu Erkennungsergebnissen

Erkennungsergebnisse anzeigen und durchsuchen

Laufenden Erkennungsscan anhalten

Erkennungszeitpläne löschen

Client-ID und geheimen Client-Schlüssel für die Erkennung von Chrome-Geräten abrufen

Bei Verwendung von Chrome-Geräten benötigt die Appliance Anmeldeinformationen, um über die Admin SDK-API auf eine Google Apps-Domain zugreifen zu können. Sie benötigen eine Client-ID und einen geheimen Client-Schlüssel von Google, um einen Genehmigungscode für die Appliance generieren zu können.

- Sie verfügen über eine Domain vom Typ "Google Apps for Business" oder "Google Apps for Education" mit Unterstützung der Chrome-Geräteverwaltung.
- Sie verfügen über ein Google-Administratorkonto, das der Geschäfts- oder Bildungsdomain angehört. Dem Konto muss die Superuser-Rolle zugewiesen sein.
- Sie verfügen über ein Google-Konto, das im Rahmen dieses Verfahrens als Entwicklerkonto verwendet werden kann. Bei diesem Konto muss es sich nicht um das Administratorkonto handeln und es muss auch nicht der Geschäfts- oder Bildungsdomäne angehören.

Die Appliance kann Geräteinformationen zu Geräten und Benutzern aus einer Google Apps-Domain importieren, wenn sie Zugriff auf die Admin SDK-API hat. Der Anmeldeprozess umfasst das Einrichten eines Google-Projekts, das Aktivieren der Admin SDK API mithilfe dieses Projekts sowie das Erstellen einer Client-ID und eines geheimen Client-Schlüssels.

1. Melden Sie sich unter https://console.developers.google.com/ bei Ihrem Entwicklerkonto an.
2. Erstellen Sie ein Projekt.
   a. Klicken Sie auf der linken Navigationsleiste auf **Projekte**.

b. Klicken Sie auf **Projekt erstellen**, um das Dialogfeld *Neues Projekt* anzuzeigen.
c. Geben Sie einen Projektnamen ein.
d. Verwenden Sie die automatisch generierte *Projekt-ID* oder geben Sie eine eigene eindeutige ID ein.
e. Klicken Sie auf **Erstellen**.

Das *Projekt-Dashboard* für das neue Projekt erscheint.

3. Aktivieren Sie die Admin SDK API.
   a. Klicken Sie auf der linken Navigationsleiste auf **APIs und Authentifizierung**, um den Bereich zu erweitern, und klicken Sie anschließend auf **APIs**.
   b. Suchen Sie unter *APIs durchsuchen* nach *Admin SDK* und klicken Sie ganz rechts in der Zeile auf **AUS**, um den *Status* auf **EIN** zu stellen, und aktivieren Sie die API.
   c. Stimmen Sie den Servicebedingungen zu, nachdem Sie sie gelesen haben, und klicken Sie auf **Akzeptieren**.
4. Erstellen Sie eine OAuth-Client-ID und einen geheimen Client-Schlüssel.

   HINWEIS: Quest empfiehlt die Erstellung einer eigenen Client-ID für jede Appliance, die zur Erkennung von Chrome-Geräten konfiguriert ist.

   a. Klicken Sie auf der linken Navigationsleiste unter **APIs und Authentifizierung** auf **Anmeldedaten**.
   b. Klicken Sie im Abschnitt *OAuth* auf **Neue Client-ID erstellen**, um das gleichnamige Dialogfeld anzuzeigen.
   c. Klicken Sie auf **Zustimmungsbildschirm konfigurieren**, um das Dialogfeld *Zustimmungsbildschirm* anzuzeigen.
   d. Wählen Sie Ihre E-Mail aus der Dropdown-Liste *E-MAIL-ADRESSE* aus, geben Sie den Namen Ihres Produkts bei *PRODUKTNAME* ein und klicken Sie auf **Speichern**, um zum Dialogfeld *Neue Client-ID erstellen* zurückzukehren.
   e. Wählen Sie **Installierte Anwendung** aus.
   f. Wählen Sie bei *Installierter Anwendungstyp* die Option **Sonstige** aus und klicken Sie anschließend auf **Neue Client-ID erstellen**.

      Auf der Seite *Anmeldedaten* werden die erstellte *Client-ID* und der erstellte *geheime Client-Schlüssel* angezeigt.

   g. Notieren Sie sich die Client-ID und den geheimen Client-Schlüssel.

   Diese Werte benötigen Sie, wenn Sie in der Appliance die Autorisierungsanmeldeinformationen für die Erkennung von Chrome-Geräten konfigurieren.

Mit einem Erkennungszeitplan für Drittanbieter können Sie Ihr Netzwerk nach G Suite-Geräten durchsuchen und Informationen zu diesen Geräten erfassen. Siehe Erkennungszeitplan für ein G-Suite-Gerät hinzufügen.

Hinzufügen eines Erkennungszeitplans für ein KACE Cloud Mobile Device Manager-Gerät

Wenn Sie KACE Cloud Mobile Device Manager (MDM) für die Verwaltung des Zugriffs auf Smartphones und Tablets verwenden, können Sie verwaltete Mobilgeräte per Erkennungszeitplanung erkennen lassen. Mit einem externen Integrationszeitplan können Sie Ihr Netzwerk nach KACE Cloud MDM-Geräten durchsuchen und Informationen zu diesen Geräten erfassen.

HINWEIS: Mithilfe dieser Methode erkannte KACE Cloud MDM-Geräte werden nicht auf das Lizenzlimit der Appliance angerechnet.

1. Rufen Sie die Seite *Detail zum Erkennungszeitplan* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen*

aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.

b. Klicken Sie in der linken Navigationsleiste auf **Inventar** und anschließend auf **Erkennungszeitpläne**.

c. Wählen Sie **Aktion auswählen** > **Neu**.

2. Wählen Sie den *Erkennungstyp*, um das Formular mit den entsprechenden Optionen anzuzeigen (hier: *Externe Integration [KACE Cloud Mobile Device Manager, G Suite, Workspace ONE]*).
3. Geben Sie im Feld *Name* einen Namen für den Scan ein:

   Dieser Name wird auf der Seite *Erkennungszeitpläne* angezeigt.
4. Erweitern Sie *KACE Cloud Mobile Device Manager* und wählen Sie die Erkennungsoptionen aus.

Option	Beschreibung
Mandantenname	Der Name des Mandanten im KACE Cloud MDM, der mit den Geräten verknüpft ist, die Sie verwalten möchten.
Anmeldeinformationen	Die Details des Kontos, das für die Verbindung mit dem KACE Cloud MDM-Gerät verwendet wird. Wählen Sie vorhandene Anmeldeinformationen in der Dropdown-Liste aus oder wählen Sie **Neue Anmeldeinformationen hinzufügen** aus, um neue Anmeldeinformationen nach Bedarf hinzuzufügen. Weitere Informationen hierzu finden Sie unter Geheimschlüssel-Anmeldeinformationen hinzufügen und bearbeiten.
Automatische Provisionierung von Geräten	Bei Verwendung dieser Option werden alle beim nächsten Scan erkannten mobilen Geräte dem Inventar hinzugefügt. **HINWEIS:** Verwenden Sie diese Option mit Bedacht, um eine unerwartet umfangreiche Erweiterung Ihres Inventars zu vermeiden.

5. **Optional**: Geben Sie im Abschnitt *Benachrichtigen* eine E-Mail-Adresse ein, um sich bei Abschluss des Erkennungsscans benachrichtigen zu lassen. Die E-Mail enthält den Namen des Erkennungszeitplans.
6. Legen Sie den Scan-Zeitplan fest:

   TIPP: Zum Verwalten des Scan-Inventars ohne Überprüfen legen Sie den Zeitplan der Scan-Konfiguration auf **Keine**.

Option	Beschreibung
Kein(e)	Die Ausführung erfolgt im Zusammenhang mit einem Ereignis anstatt zu einem bestimmten Datum oder zu einem bestimmten Zeitpunkt.
jede Stunde	Der Vorgang wird im angegebenen Intervall durchgeführt.
Täglich/an einem bestimmten Tag um HH:MM	Die Erfassung wird täglich zu einem bestimmten Zeitpunkt oder an einem bestimmten Wochentag um eine bestimmte Uhrzeit ausgeführt.

Option	Beschreibung
Ausführen am n-ten jedes Monats/eines bestimmten Monats um HH:MM	Die Erfassung wird jeden Monat oder in einem bestimmten Monat an einem festgelegten Datum zu einer festgelegten Uhrzeit ausgeführt.
Ausführen am n-ten Wochentag **jedes Monats/ eines bestimmten Monats um HH:MM**	Die Erfassung wird jeden Monat oder in einem bestimmten Monat an einem festgelegten Wochentag zu einer festgelegten Uhrzeit ausgeführt.

Benutzerdefiniert	Führen Sie die Erfassung nach einem benutzerdefinierten Zeitplan aus.
	Verwenden Sie das Standard-5-Feld-Cron-Format (das erweiterte Cron-Format wird nicht unterstützt):
	`* * * * *`
	`| | | | +————————Wochentag (0-6) (Sonntag=0)`
	`| | | +————————Monat (1-12)`
	`| | +————————Monatstag (1-31)`
	`| +————————Stunde (0-23)`
	`+————————Minute (0-59)`
	Verwenden Sie bei der Angabe von Werten die folgenden Zeichen:
	• **Leerzeichen( )**: Die einzelnen Felder mit einem Leerzeichen trennen.
	• **Sternchen (*)**: Ein Sternchen repräsentiert den gesamten Wertebereich in einem Feld. Zum Beispiel repräsentiert ein Sternchen im Stundenfeld eine beliebige Stunde.
	• **Kommas (,)**: Mehrere Werte in einem Feld werden mit einem Komma getrennt. Zum Beispiel werden mit `0,6` im Feld „Wochentag“ Sonntag und Samstag angegeben.
	• **Bindestriche (-)**: Mit einem Bindestrich wird ein Wertebereich in einem Feld angegeben. Zum Beispiel entspricht `1-5` im Feld „Wochentag“ `1,2,3,4,5`, d. h. Montag bis Freitag.
	• **Schrägstriche (/)**: Die Angabe der Zeitabstände, mit denen eine Aktion wiederholt werden soll, erfolgt mit einem Schrägstrich. Zum Beispiel entspricht `*/3` im Feld Stunde `0,3,6,9,12,15,18,21`. Das Sternchen (`*`) gibt jede Stunde an, mit `/3` erfolgt aber eine Einschränkung auf durch drei teilbare Stunden.

Option	Beschreibung
	Beispiele: • `15 * * * *` Jeden Tag 15 Minuten nach jeder vollen Stunde ausführen • `0 22 * * *` Jeden Tag um 22:00 Uhr ausführen • `0 0 1 1,6 *` Am 1. Januar und 1. Juni um 00:00 Uhr ausführen • `30 8,12 * * 1-5` An Wochentagen um 08:30 Uhr und 12:30 Uhr ausführen • `0 2 */2 * *` Jeden zweiten Tag um 02:00 Uhr ausführen
Aufgabenplan anzeigen	Klicken Sie, um den Aufgabenplan anzuzeigen. Im Dialogfeld *Aufgabenplan* wird eine Liste der geplanten Aufgaben angezeigt. Klicken Sie auf eine Aufgabe, um die Aufgabendetails anzuzeigen. Weitere Informationen hierzu finden Sie unter Aufgabenpläne anzeigen.

7. Klicken Sie auf **Speichern**.

Verwandte Themen

Informationen zu Erkennungsergebnissen

Erkennungsergebnisse anzeigen und durchsuchen

Laufenden Erkennungsscan anhalten

Erkennungszeitpläne löschen

Erkennungszeitplan für ein G-Suite-Gerät hinzufügen

Mit einem externen Integrationszeitplan können Sie Ihr Netzwerk nach G-Suite-Geräten durchsuchen und Informationen zu diesen Geräten erfassen.

- Sie verfügen über eine Domain vom Typ "Google Apps for Business" oder "Google Apps for Education" mit Unterstützung der Chrome-Geräteverwaltung.
- Sie verfügen über ein Google-Administratorkonto, das der Geschäfts- oder Bildungsdomain angehört. Dem Konto muss die Superuser-Rolle zugewiesen sein.
- Sie verfügen über ein als Entwicklerkonto verwendetes Google-Konto und haben ein Projekt mit einer Client-ID und einem geheimen Client-Schlüssel erstellt. Siehe Client-ID und geheimen Client-Schlüssel für die Erkennung von Chrome-Geräten abrufen.

HINWEIS: G Suite-Geräte, die mithilfe dieser Methode ermittelt werden, werden nicht auf das Lizenzlimit der Appliance angerechnet.

1. Rufen Sie die Seite *Detail zum Erkennungszeitplan* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Inventar** und anschließend auf **Erkennungszeitpläne**.

c. Wählen Sie **Aktion auswählen > Neu**.

2. Wählen Sie den *Erkennungstyp*, um das Formular mit den entsprechenden Optionen anzuzeigen (hier: *Externe Integration [KACE Cloud Mobile Device Manager, G Suite, Workspace ONE]*).
3. Geben Sie im Feld *Name* einen Namen für den Scan ein:

   Dieser Name wird auf der Seite *Erkennungszeitpläne* angezeigt.
4. Erweitern Sie *G Suite* und wählen Sie die Erkennungsoptionen aus.

Option	Beschreibung
Chrome-Geräte ermitteln	Wenn aktiviert, werden Chrome-Geräte beim nächsten Scan ermittelt.
Mobile Geräte ermitteln	Wenn aktiviert, werden mobile Geräte der G Suite beim nächsten Scan ermittelt.
Anmeldeinformationen	Die Details des Kontos, das für die Verbindung mit dem Chrome-Gerät verwendet wird. Wählen Sie vorhandene Anmeldeinformationen in der Dropdown-Liste aus oder wählen Sie **Neue Anmeldeinformationen hinzufügen** aus, um nicht bereits aufgeführte Anmeldeinformationen hinzuzufügen. **WICHTIG: Das ausgewählte Anmeldeprofil muss über einen Genehmigungscode verfügen, der mit dem entsprechenden Gerätetyp verknüpft werden kann. Wenn Sie beispielsweise mobile Geräte der G Suite ermitteln möchten, können Sie kein Anmeldeprofil verwenden, dessen Genehmigungscode für Chrome-Geräte generiert wurde.** Weitere Informationen hierzu finden Sie unter Hinzufügen und Bearbeiten von Google OAuth-Anmeldeinformationen.
Automatische Provisionierung von Geräten	Bei Verwendung dieser Option werden alle beim nächsten Scan erkannten Geräte vom Typ "Chrome" dem Inventar hinzugefügt. **HINWEIS:** Verwenden Sie diese Option mit Bedacht, um eine unerwartet umfangreiche Erweiterung Ihres Inventars zu vermeiden.

5. **Optional**: Geben Sie im Abschnitt *Benachrichtigen* eine E-Mail-Adresse ein, um sich bei Abschluss des Erkennungsscans benachrichtigen zu lassen. Die E-Mail enthält den Namen des Erkennungszeitplans.
6. Legen Sie den Scan-Zeitplan fest:

   TIPP: Zum Verwalten des Scan-Inventars ohne Überprüfen legen Sie den Zeitplan der Scan-Konfiguration auf **Keine**.

Option	Beschreibung
Kein(e)	Die Ausführung erfolgt im Zusammenhang mit einem Ereignis anstatt zu einem bestimmten Datum oder zu einem bestimmten Zeitpunkt.

Option	Beschreibung
jede Stunde	Der Vorgang wird im angegebenen Intervall durchgeführt.
Täglich/an einem bestimmten Tag um HH:MM	Die Erfassung wird täglich zu einem bestimmten Zeitpunkt oder an einem bestimmten Wochentag um eine bestimmte Uhrzeit ausgeführt.
Ausführen am n-ten jedes Monats/eines bestimmten Monats um HH:MM	Die Erfassung wird jeden Monat oder in einem bestimmten Monat an einem festgelegten Datum zu einer festgelegten Uhrzeit ausgeführt.
Ausführen am n-ten Wochentag **jedes Monats/ eines bestimmten Monats um HH:MM**	Die Erfassung wird jeden Monat oder in einem bestimmten Monat an einem festgelegten Wochentag zu einer festgelegten Uhrzeit ausgeführt.

Benutzerdefiniert	Führen Sie die Erfassung nach einem benutzerdefinierten Zeitplan aus.
	Verwenden Sie das Standard-5-Feld-Cron-Format (das erweiterte Cron-Format wird nicht unterstützt):
	`* * * * *`
	`| | | | +————————Wochentag (0-6) (Sonntag=0)`
	`| | | +————————Monat (1-12)`
	`| | +————————Monatstag (1-31)`
	`| +————————Stunde (0-23)`
	`+————————Minute (0-59)`
	Verwenden Sie bei der Angabe von Werten die folgenden Zeichen:
	• **Leerzeichen( )**: Die einzelnen Felder mit einem Leerzeichen trennen.
	• **Sternchen (*)**: Ein Sternchen repräsentiert den gesamten Wertebereich in einem Feld. Zum Beispiel repräsentiert ein Sternchen im Stundenfeld eine beliebige Stunde.
	• **Kommas (,)**: Mehrere Werte in einem Feld werden mit einem Komma getrennt. Zum Beispiel werden mit `0,6` im Feld „Wochentag“ Sonntag und Samstag angegeben.
	• **Bindestriche (-)**: Mit einem Bindestrich wird ein Wertebereich in einem Feld angegeben. Zum Beispiel entspricht `1-5` im Feld „Wochentag“ `1,2,3,4,5`, d. h. Montag bis Freitag.
	• **Schrägstriche (/)**: Die Angabe der Zeitabstände, mit denen eine Aktion wiederholt werden soll, erfolgt mit einem Schrägstrich. Zum Beispiel entspricht `*/3` im Feld Stunde `0,3,6,9,12,15,18,21`. Das Sternchen (`*`) gibt jede Stunde an, mit `/3` erfolgt aber eine Einschränkung auf durch drei teilbare Stunden.

Option	Beschreibung
	Beispiele: • `15 * * * * Jeden Tag 15 Minuten nach jeder vollen Stunde ausführen` • `0 22 * * * Jeden Tag um 22:00 Uhr ausführen` • `0 0 1 1,6 * Am 1. Januar und 1. Juni um 00:00 Uhr ausführen` • `30 8,12 * * 1-5 An Wochentagen um 08:30 Uhr und 12:30 Uhr ausführen` • `0 2 */2 * * Jeden zweiten Tag um 02:00 Uhr ausführen`
Aufgabenplan anzeigen	Klicken Sie, um den Aufgabenplan anzuzeigen. Im Dialogfeld *Aufgabenplan* wird eine Liste der geplanten Aufgaben angezeigt. Klicken Sie auf eine Aufgabe, um die Aufgabendetails anzuzeigen. Weitere Informationen hierzu finden Sie unter Aufgabenpläne anzeigen.

7. Klicken Sie auf **Speichern**.

Verwandte Themen

Informationen zu Erkennungsergebnissen

Erkennungsergebnisse anzeigen und durchsuchen

Laufenden Erkennungsscan anhalten

Erkennungszeitpläne löschen

Erkennungszeitplan für ein Workspace ONE-Gerät hinzufügen

VMware® Workspace ONE® ist eine Mobilitätsverwaltungsplattform auf Unternehmensebene, die es Ihnen erlaubt, eine große Zahl unterschiedlicher Gerätetypen zu verwalten. Sie können mithilfe der Workspace ONE-Integration Erkennungsgeräte erfassen, die mit Workspace ONE und REST API-Aufrufen verwaltet werden.

HINWEIS: Workspace ONE-Geräte, die mithilfe dieser Methode erkannt werden, werden nicht auf das Lizenzlimit der Appliance angerechnet.

1. Rufen Sie die Seite *Detail zum Erkennungszeitplan* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Inventar** und anschließend auf **Erkennungszeitpläne**.
   c. Wählen Sie **Aktion auswählen** > **Neu**.
2. Wählen Sie den *Erkennungstyp*, um das Formular mit den entsprechenden Optionen anzuzeigen (hier: *Externe Integration [KACE Cloud Mobile Device Manager, G Suite, Workspace ONE]*).
3. Geben Sie im Feld *Name* einen Namen für den Scan ein:

Dieser Name wird auf der Seite *Erkennungszeitpläne* angezeigt.

4. Erweitern Sie *Workspace ONE* und wählen Sie die Erkennungsoptionen aus.

Option	Beschreibung
Host	Der Host-Name der Workspace ONE-Verwaltungskonsole.
REST API-Schlüssel	Der REST-API-Schlüssel der in der Workspace ONE-Verwaltungskonsole verfügbar ist. Der Schlüssel muss angegeben werden, damit die Integration von Workspace ONE über API-Aufrufe aktiviert wird.
Anmeldeinformationen	Die Details des Dienstkontos, die erforderlich sind, um eine Verbindung zum Gerät herzustellen und Befehle auszuführen Wählen Sie vorhandene Anmeldeinformationen in der Dropdown-Liste aus oder wählen Sie **Neue Anmeldeinformationen hinzufügen** aus, um nicht bereits aufgeführte Anmeldeinformationen hinzuzufügen. Siehe Hinzufügen und Bearbeiten von Benutzer-/Kennwort-Anmeldeinformationen.
Automatische Provisionierung von Geräten	Bei Verwendung dieser Option werden alle beim nächsten Scan erkannten Geräte vom Typ "Workspace ONE" dem Inventar hinzugefügt. **HINWEIS:** Verwenden Sie diese Option mit Bedacht, um eine unerwartet umfangreiche Erweiterung Ihres Inventars zu vermeiden.

5. **Optional**: Geben Sie im Abschnitt *Benachrichtigen* eine E-Mail-Adresse ein, um sich bei Abschluss des Erkennungsscans benachrichtigen zu lassen. Die E-Mail enthält den Namen des Erkennungszeitplans.
6. Legen Sie den Scan-Zeitplan fest:

TIPP: Zum Verwalten des Scan-Inventars ohne Überprüfen legen Sie den Zeitplan der Scan-Konfiguration auf **Keine**.

Option	Beschreibung
Kein(e)	Die Ausführung erfolgt im Zusammenhang mit einem Ereignis anstatt zu einem bestimmten Datum oder zu einem bestimmten Zeitpunkt.
jede Stunde	Der Vorgang wird im angegebenen Intervall durchgeführt.
Täglich/an einem bestimmten Tag um HH:MM	Die Erfassung wird täglich zu einem bestimmten Zeitpunkt oder an einem bestimmten Wochentag um eine bestimmte Uhrzeit ausgeführt.
Ausführen am n-ten jedes Monats/eines bestimmten Monats um HH:MM	Die Erfassung wird jeden Monat oder in einem bestimmten Monat an einem festgelegten Datum zu einer festgelegten Uhrzeit ausgeführt.

Option	Beschreibung
Ausführen am n-ten Wochentag **jedes Monats/ eines bestimmten Monats um HH:MM**	Die Erfassung wird jeden Monat oder in einem bestimmten Monat an einem festgelegten Wochentag zu einer festgelegten Uhrzeit ausgeführt.

Benutzerdefiniert	Führen Sie die Erfassung nach einem benutzerdefinierten Zeitplan aus.
	Verwenden Sie das Standard-5-Feld-Cron-Format (das erweiterte Cron-Format wird nicht unterstützt):
	`* * * * *`
	`| | | | +————Wochentag (0-6) (Sonntag=0)`
	`| | | +————Monat (1-12)`
	`| | +————Monatstag (1-31)`
	`| +————Stunde (0-23)`
	`+————Minute (0-59)`
	Verwenden Sie bei der Angabe von Werten die folgenden Zeichen:
	• **Leerzeichen( )**: Die einzelnen Felder mit einem Leerzeichen trennen.
	• **Sternchen (*)**: Ein Sternchen repräsentiert den gesamten Wertebereich in einem Feld. Zum Beispiel repräsentiert ein Sternchen im Stundenfeld eine beliebige Stunde.
	• **Kommas (,)**: Mehrere Werte in einem Feld werden mit einem Komma getrennt. Zum Beispiel werden mit `0,6` im Feld „Wochentag“ Sonntag und Samstag angegeben.
	• **Bindestriche (-)**: Mit einem Bindestrich wird ein Wertebereich in einem Feld angegeben. Zum Beispiel entspricht `1-5` im Feld „Wochentag“ `1,2,3,4,5`, d. h. Montag bis Freitag.
	• **Schrägstriche (/)**: Die Angabe der Zeitabstände, mit denen eine Aktion wiederholt werden soll, erfolgt mit einem Schrägstrich. Zum Beispiel entspricht `*/3` im Feld Stunde `0,3,6,9,12,15,18,21`. Das Sternchen (`*`) gibt jede Stunde an, mit `/3` erfolgt aber eine Einschränkung auf durch drei teilbare Stunden.

Option	Beschreibung
	Beispiele: • `15 * * * * Jeden Tag 15 Minuten nach jeder vollen Stunde ausführen` • `0 22 * * * Jeden Tag um 22:00 Uhr ausführen` • `0 0 1 1,6 * Am 1. Januar und 1. Juni um 00:00 Uhr ausführen` • `30 8,12 * * 1-5 An Wochentagen um 08:30 Uhr und 12:30 Uhr ausführen` • `0 2 */2 * * Jeden zweiten Tag um 02:00 Uhr ausführen`
Aufgabenplan anzeigen	Klicken Sie, um den Aufgabenplan anzuzeigen. Im Dialogfeld *Aufgabenplan* wird eine Liste der geplanten Aufgaben angezeigt. Klicken Sie auf eine Aufgabe, um die Aufgabendetails anzuzeigen. Weitere Informationen hierzu finden Sie unter Aufgabenpläne anzeigen.

7. Klicken Sie auf **Speichern**.

Verwandte Themen

Informationen zu Erkennungsergebnissen

Erkennungsergebnisse anzeigen und durchsuchen

Laufenden Erkennungsscan anhalten

Erkennungszeitpläne löschen

Hinzufügen eines Erkennungszeitplans für einen VMware ESXi-Host oder vCenter-Server

Wenn Ihr Unternehmen eine virtuelle VMware-basierte Umgebung nutzt, können Sie VMware ESXi-Hosts oder vCenter-Server mit Erkennungszeitplänen ermitteln. Fügen Sie einen authentifizierten Erkennungszeitplan hinzu, um das Netzwerk nach VMware ESXi-Hosts oder vCenter-Servern zu durchsuchen und Informationen zu diesen Geräten erfassen.

Ein bereitgestellter VMware ESXi-Host benötigt eine agentenbasierte Lizenz. Virtuelle Maschinen, die diesem Host zugeordnet sind, verbrauchen keine Lizenzen. Das vCenter, in dem der ESXi-Host ausgeführt wird, verbraucht keine Lizenz. Es fungiert als Brücke für die Verbindung zu bereitgestellten ESXi-Hosts.

1. Rufen Sie die Seite *Detail zum Erkennungszeitplan* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Inventar** und anschließend auf **Erkennungszeitpläne**.

c. Wählen Sie **Aktion auswählen > Neu**.

2. Wählen Sie den *Erkennungstyp* aus, um das Formular mit den entsprechenden Optionen anzuzeigen (hier: *Authentifiziert [WinRM, SNMP, SSH, VMware, Hyper-V]*).
3. Geben Sie im Feld *Name* einen Namen für den Scan ein:

   Dieser Name wird auf der Seite *Erkennungszeitpläne* angezeigt.
4. Erweitern Sie den Abschnitt *VMware* und konfigurieren Sie die Optionen für die Erkennung.

Option	Beschreibung
Timeout	Die Zeit, nach der der Scan endet, falls keine Reaktion erfolgt.
Anmeldeinformationen	Die Details des Dienstkontos, die erforderlich sind, um eine Verbindung zum Gerät herzustellen und Befehle auszuführen Wählen Sie vorhandene Anmeldeinformationen in der Dropdown-Liste aus oder wählen Sie **Neue Anmeldeinformationen hinzufügen** aus, um nicht bereits aufgeführte Anmeldeinformationen hinzuzufügen. Siehe Hinzufügen und Bearbeiten von Benutzer-/Kennwort-Anmeldeinformationen.

5. **Optional**: Geben Sie im Abschnitt *Benachrichtigen* eine E-Mail-Adresse ein, um sich bei Abschluss des Erkennungsscans benachrichtigen zu lassen. Die E-Mail enthält den Namen des Erkennungszeitplans.
6. Legen Sie den Scan-Zeitplan fest:

   TIPP: Zum Verwalten des Scan-Inventars ohne Überprüfen legen Sie den Zeitplan der Scan-Konfiguration auf **Keine**.

Option	Beschreibung
Kein(e)	Die Ausführung erfolgt im Zusammenhang mit einem Ereignis anstatt zu einem bestimmten Datum oder zu einem bestimmten Zeitpunkt.
jede Stunde	Der Vorgang wird im angegebenen Intervall durchgeführt.
Täglich/an einem bestimmten Tag um HH:MM	Die Erfassung wird täglich zu einem bestimmten Zeitpunkt oder an einem bestimmten Wochentag um eine bestimmte Uhrzeit ausgeführt.
Ausführen am n-ten jedes Monats/eines bestimmten Monats um HH:MM	Die Erfassung wird jeden Monat oder in einem bestimmten Monat an einem festgelegten Datum zu einer festgelegten Uhrzeit ausgeführt.
Ausführen am n-ten Wochentag **jedes Monats/eines bestimmten Monats um HH:MM**	Die Erfassung wird jeden Monat oder in einem bestimmten Monat an einem festgelegten Wochentag zu einer festgelegten Uhrzeit ausgeführt.

Benutzerdefiniert	Führen Sie die Erfassung nach einem benutzerdefinierten Zeitplan aus.
	Verwenden Sie das Standard-5-Feld-Cron-Format (das erweiterte Cron-Format wird nicht unterstützt):
	`* * * * *`
	`| | | | +————Wochentag (0-6) (Sonntag=0)`

Option	Beschreibung

	`| | | +————————Monat (1-12)`
	`| | +————————Monatstag (1-31)`
	`| +————————Stunde (0-23)`
	`+————————Minute (0-59)`
	
	Verwenden Sie bei der Angabe von Werten die folgenden Zeichen:
	
	• **Leerzeichen( )**: Die einzelnen Felder mit einem Leerzeichen trennen.
	• **Sternchen (*)**: Ein Sternchen repräsentiert den gesamten Wertebereich in einem Feld. Zum Beispiel repräsentiert ein Sternchen im Stundenfeld eine beliebige Stunde.
	• **Kommas (,)**: Mehrere Werte in einem Feld werden mit einem Komma getrennt. Zum Beispiel werden mit `0,6` im Feld „Wochentag“ Sonntag und Samstag angegeben.
	• **Bindestriche (-)**: Mit einem Bindestrich wird ein Wertebereich in einem Feld angegeben. Zum Beispiel entspricht `1-5` im Feld „Wochentag“ `1,2,3,4,5`, d. h. Montag bis Freitag.
	• **Schrägstriche (/)**: Die Angabe der Zeitabstände, mit denen eine Aktion wiederholt werden soll, erfolgt mit einem Schrägstrich. Zum Beispiel entspricht `*/3` im Feld Stunde `0,3,6,9,12,15,18,21`. Das Sternchen (`*`) gibt jede Stunde an, mit `/3` erfolgt aber eine Einschränkung auf durch drei teilbare Stunden.
	
	Beispiele:
	
	• `15 * * * * Jeden Tag 15 Minuten nach jeder vollen Stunde ausführen`
	• `0 22 * * * Jeden Tag um 22:00 Uhr ausführen`
	• `0 0 1 1,6 * Am 1. Januar und 1. Juni um 00:00 Uhr ausführen`
	• `30 8,12 * * 1-5 An Wochentagen um 08:30 Uhr und 12:30 Uhr ausführen`
	• `0 2 */2 * * Jeden zweiten Tag um 02:00 Uhr ausführen`

Aufgabenplan anzeigen	Klicken Sie, um den Aufgabenplan anzuzeigen. Im Dialogfeld *Aufgabenplan* wird eine Liste der geplanten Aufgaben angezeigt. Klicken Sie auf eine Aufgabe, um die Aufgabendetails anzuzeigen. Weitere Informationen hierzu finden Sie unter Aufgabenpläne anzeigen.

7. Klicken Sie auf **Speichern**.

Verwandte Themen

Informationen zu Erkennungsergebnissen

Erkennungsergebnisse anzeigen und durchsuchen

Laufenden Erkennungsscan anhalten

Erkennungszeitpläne löschen

Erkennungszeitplan für Microsoft Hyper-V oder System Center Virtual Machine Manager hinzufügen

Wenn Ihr Unternehmen eine virtuelle Hyper-V-basierte Umgebung verwendet, können Sie Microsoft Hyper-V- oder System Center Virtual Machine Manager(SCVMM)-Geräte mithilfe der Erkennungsplanung erkennen. Um Ihr Netzwerk nach Hyper-V- oder SCVMM-Geräten zu durchsuchen und Informationen über diese Geräte zu erfassen, fügen Sie einen authentifizierten Erkennungszeitplan hinzu.

Die mit dieser Methode in die Appliance importierten Geräte verbrauchen keine Lizenzen. Jedes SCVMM- und Hyper-V-Gerät verbraucht nur eine agentenlose Lizenz, die zur Bestandsaufnahme der zugrunde liegenden Windows-Systeme verwendet wird. SCVMM- und Hyper-V-Geräte, die ebenfalls mit dem KACE Agent bereitgestellt werden, verbrauchen jeweils zwei Lizenzen.

1. Rufen Sie die Seite *Detail zum Erkennungszeitplan* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Inventar** und anschließend auf **Erkennungszeitpläne**.
   c. Wählen Sie **Aktion auswählen** > **Neu**.
2. Wählen Sie den *Erkennungstyp* aus, um das Formular mit den entsprechenden Optionen anzuzeigen (hier: *Authentifiziert [WinRM, SNMP, SSH, VMware, Hyper-V]*).
3. Geben Sie im Feld *Name* einen Namen für den Scan ein:

   Dieser Name wird auf der Seite *Erkennungszeitpläne* angezeigt.
4. Erweitern Sie den Abschnitt *VMware, Hyper-V, VMM* und konfigurieren Sie die Optionen für die Erkennung.

Option	Beschreibung
Timeout	Die Zeit (maximal 60 Sekunden), nach der eine inaktive Verbindung getrennt wird.
Kerberos voraussetzen	Bei Verwendung dieser Option ist eine Kerberos-Authentifizierung erforderlich. Wenn Kerberos nicht verfügbar ist, wird NTLM nicht als Alternative verwendet. Für die Verwendung von Kerberos muss in der Erkennungskonfiguration auch DNS-Lookup aktiviert sein. Darüber hinaus muss in den lokalen Netzwerkeinstellungen der Appliance auch der DNS-Server angegeben werden.
Nach Hyper-V und Virtual Machine Manager suchen	Wählen Sie diese Option aus, damit die Appliance eine Microsoft Hyper-V- oder System Center Virtual Machine Manager-Infrastruktur mit agentenloser Verwaltung importieren kann. Weitere Informationen zu dieser Funktion finden Sie unter .

Option	Beschreibung
Port	Ohne Angabe in diesem Feld wird der Standardport 5985 verwendet.
Anmeldeinformationen	Die Details des Dienstkontos, die erforderlich sind, um eine Verbindung zum Gerät herzustellen und Befehle auszuführen Wählen Sie vorhandene Anmeldeinformationen in der Dropdown-Liste aus oder wählen Sie **Neue Anmeldeinformationen hinzufügen** aus, um neue Anmeldeinformationen nach Bedarf hinzuzufügen. Siehe Hinzufügen und Bearbeiten von Benutzer-/Kennwort-Anmeldeinformationen. **HINWEIS:** Die gleichen Anmeldeinformationen, die für ein SCVMM-Gerät angegeben werden, werden für die Verbindung mit jedem verwalteten Hyper-V-Gerät verwendet. Weitere Informationen hierzu finden Sie unter Zugangsdatenanforderungen für System Center Virtual Machine Manager.

5. **Optional**: Geben Sie im Abschnitt *Benachrichtigen* eine E-Mail-Adresse ein, um sich bei Abschluss des Erkennungsscans benachrichtigen zu lassen. Die E-Mail enthält den Namen des Erkennungszeitplans.
6. Legen Sie den Scan-Zeitplan fest:

TIPP: Zum Verwalten des Scan-Inventars ohne Überprüfen legen Sie den Zeitplan der Scan-Konfiguration auf **Keine**.

Option	Beschreibung
Kein(e)	Die Ausführung erfolgt im Zusammenhang mit einem Ereignis anstatt zu einem bestimmten Datum oder zu einem bestimmten Zeitpunkt.
jede Stunde	Der Vorgang wird im angegebenen Intervall durchgeführt.
Täglich/an einem bestimmten Tag um HH:MM	Die Erfassung wird täglich zu einem bestimmten Zeitpunkt oder an einem bestimmten Wochentag um eine bestimmte Uhrzeit ausgeführt.
Ausführen am n-ten jedes Monats/eines bestimmten Monats um HH:MM	Die Erfassung wird jeden Monat oder in einem bestimmten Monat an einem festgelegten Datum zu einer festgelegten Uhrzeit ausgeführt.
Ausführen am n-ten Wochentag **jedes Monats/eines bestimmten Monats um HH:MM**	Die Erfassung wird jeden Monat oder in einem bestimmten Monat an einem festgelegten Wochentag zu einer festgelegten Uhrzeit ausgeführt.
Benutzerdefiniert	Führen Sie die Erfassung nach einem benutzerdefinierten Zeitplan aus. Verwenden Sie das Standard-5-Feld-Cron-Format (das erweiterte Cron-Format wird nicht unterstützt): * * * * *

Option	Beschreibung

	`| | | | +————Wochentag (0-6) (Sonntag=0)`
	`| | | +————Monat (1-12)`
	`| | +————Monatstag (1-31)`
	`| +————Stunde (0-23)`
	`+————Minute (0-59)`
	
	Verwenden Sie bei der Angabe von Werten die folgenden Zeichen:
	• **Leerzeichen( )**: Die einzelnen Felder mit einem Leerzeichen trennen.
	• **Sternchen (*)**: Ein Sternchen repräsentiert den gesamten Wertebereich in einem Feld. Zum Beispiel repräsentiert ein Sternchen im Stundenfeld eine beliebige Stunde.
	• **Kommas (,)**: Mehrere Werte in einem Feld werden mit einem Komma getrennt. Zum Beispiel werden mit `0,6` im Feld „Wochentag“ Sonntag und Samstag angegeben.
	• **Bindestriche (-)**: Mit einem Bindestrich wird ein Wertebereich in einem Feld angegeben. Zum Beispiel entspricht `1-5` im Feld „Wochentag“ `1,2,3,4,5`, d. h. Montag bis Freitag.
	• **Schrägstriche (/)**: Die Angabe der Zeitabstände, mit denen eine Aktion wiederholt werden soll, erfolgt mit einem Schrägstrich. Zum Beispiel entspricht `*/3` im Feld Stunde `0,3,6,9,12,15,18,21`. Das Sternchen (`*`) gibt jede Stunde an, mit `/3` erfolgt aber eine Einschränkung auf durch drei teilbare Stunden.
	
	Beispiele:
	• `15 * * * *` Jeden Tag 15 Minuten nach jeder vollen Stunde ausführen
	• `0 22 * * *` Jeden Tag um 22:00 Uhr ausführen
	• `0 0 1 1,6 *` Am 1. Januar und 1. Juni um 00:00 Uhr ausführen
	• `30 8,12 * * 1-5` An Wochentagen um 08:30 Uhr und 12:30 Uhr ausführen
	• `0 2 */2 * *` Jeden zweiten Tag um 02:00 Uhr ausführen

Aufgabenplan anzeigen	Klicken Sie, um den Aufgabenplan anzuzeigen. Im Dialogfeld *Aufgabenplan* wird eine Liste der geplanten Aufgaben angezeigt. Klicken Sie auf eine Aufgabe, um die Aufgabendetails anzuzeigen. Weitere Informationen hierzu finden Sie unter Aufgabenpläne anzeigen.

7. Klicken Sie auf **Speichern**.

Verwandte Themen

Informationen zu Erkennungsergebnissen

Erkennungsergebnisse anzeigen und durchsuchen

Laufenden Erkennungsscan anhalten

Erkennungszeitpläne löschen

Zugangsdatenanforderungen für System Center Virtual Machine Manager

Für die Anmeldeinformationen, die für das Inventarisieren eines SCVMM-Geräts (System Center Virtual Machine Manager) mitsamt aller verwalteten Hyper-V-Geräte verwendet werden, gelten spezifische Anforderungen.

- Das Domänenkonto muss Mitglied des schreibgeschützten SCVMM-Profils **Administrator mit Leseberechtigung** oder eines Profils mit denselben/höheren Berechtigungen sein.
- Das Domänenkonto muss Mitglied der lokalen Gruppe **Hyper-V-Administratoren** auf jedem Hyper-V-Gerät sein.
- Das Domänenkonto muss über Berechtigungen zum Durchführen der agentenlosen Windows-Inventarisierung unter Verwendung von WinRM auf den SCVMM- und Hyper-V-Geräten verfügen.

Hinzufügen eines Erkennungszeitplans für SNMP-fähige computerfremde Geräte

Mit einem SNMP-Erkennungszeitplan mit dem Erkennungstyp „Authentifiziert“ können Sie Ihr Netzwerk nach computerfremden Geräten durchsuchen und Informationen zu diesen Geräten erfassen.

Zur Aktivierung von SNMP muss Port 161 auf der Appliance und dem Gerät geöffnet sein.

SNMP (Simple Network Management Protocol) ist ein Protokoll zum Überwachen von verwalteten Geräten in einem Netzwerk. SNMP v3 verwendet Authentifizierungs- und Verschlüsselungsalgorithmen zur Erhöhung der Sicherheit von SNMP-Datenübertragungen. Wenn Sie die SNMP v3-Optionen konfigurieren, führt die Appliance einen SNMP v3-Scan für ausgewählte Geräte durch. Ist der Scan nicht erfolgreich, führt die Appliance einen SNMP v2- oder einen SNMP v1-Scan mit der angegebenen öffentlichen Zeichenfolge durch.

Die Ergebnisse des SNMP-Scans enthalten alle SNMP-fähigen Geräte. Remote Shell-Erweiterungen versetzen die Appliance in die Lage, Verbindungen zu Geräten herzustellen, Befehle auszuführen und Erkennungsinformationen zu erfassen.

HINWEIS: Sobald ein Erkennungszeitplan gespeichert wurde, können Sie SNMP-Authentifizierung nicht mehr in SSH-Authentifizierung ändern.

1. Rufen Sie die Seite *Detail zum Erkennungszeitplan* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Inventar** und anschließend auf **Erkennungszeitpläne**.
   c. Wählen Sie **Aktion auswählen** > **Neu**.
2. Wählen Sie den *Erkennungstyp* aus, um das Formular mit den entsprechenden Optionen anzuzeigen (hier: *Authentifiziert [WinRM, SNMP, SSH, VMware, Hyper-V]*).

Vor dem Abschnitt *Benachrichtigen* werden die folgenden Optionen angezeigt:

- *DNS-Lookup*
- *Relay*
- *WinRM, Hyper-V, VMM*
- *SSH*
- *SNMP*

Für dieses Verfahren sind nur *DNS-Lookup* und *SNMP* relevant.

3. Geben Sie im Feld *Name* einen Namen für den Scan ein:

   Dieser Name wird auf der Seite *Erkennungszeitpläne* angezeigt.

4. Geben Sie im Feld *IP-Adressbereich* den zu scannenden IP-Adressbereich ein. Verwenden Sie Bindestriche, um einzelne Bereiche von IP-Adressklassen anzugeben. Geben Sie beispielsweise 192.168.2-5.1-200 ein, um nach allen IP-Adressen von 192.168.2-5.1 bis einschließlich 192.168.2-5.200 zu suchen.

   TIPP: Die Appliance unterstützt sowohl IPv6- (Internet Protocol Version 6) als auch IPv4-Adressen.

   VORSICHT: Ein Maximum von 25.000 IP-Adressen wird unterstützt. Wenn Sie einen IP-Bereich angeben, der mehr als 25.000 Adressen enthält, wird eine Warnmeldung angezeigt, wenn Sie versuchen, den Provisionierungszeitplan zu speichern.

5. Erweitern Sie *DNS-Lookup* und wählen Sie die Erkennungsoptionen aus.

   DNS-Lookup ermöglicht die Erkennung zur Ermittlung des Gerätenamens. Das DNS-Lookup ist wichtig, wenn Gerätenamen in den Erkennungsergebnissen und Inventarlisten angezeigt werden sollen.

Option	Beschreibung
DNS-Server für Lookup	Die IP-Adresse oder der Hostname des DNS-Servers **TIPP:** Die Appliance unterstützt sowohl IPv6- (Internet Protocol Version 6) als auch IPv4-Adressen.
Timeout	Die Zeit in Sekunden, nach der das Zeitlimit für DNS-Lookup abläuft. Wenn während dieser Zeit keine Adresse gefunden wird, tritt ein Timeout des Vorgangs auf.

6. Erweitern Sie *Relay* und wählen Sie die Erkennungsoptionen aus.

   Über die *Relay*-Optionen können Sie einen KACE Agent konfigurieren, um als Tunnel für den WinRM-, SSH- und SNMP-Datenverkehr zum Agent-Verbindungsprotokoll für WinRM-, SSH- und SNMP-Ermittlungspläne, agentenlose Bestandsaufnahme und Agentenbereitstellung zu agieren.

Option	Beschreibung
Relay-Gerät	Geben Sie das Gerät an, das als Relay für die agentenlose Geräteinventarisierung verwendet werden soll. Ein Relay-Gerät, das während der Ermittlung verwendet wird, wenn ein neues Gerät von den Ermittlungsergebnissen automatisch durch ein neues Gerät bereitgestellt wird.

Option	Beschreibung
	Ausgewählte Relay-Geräte sind auf den folgenden Seiten aufgeführt: • Auf der Seite *Details zur Geräteverbindung ohne Agent*, wenn ein neues Gerät automatisch aus Ermittlungsergebnissen bereitgestellt wird. Weitere Informationen zu dieser Seite finden Sie unter Verwaltung ohne Agent durch manuelle Eingabe von Geräteinformationen aktivieren. • Auf der Seite *Detail zum Provisionierungszeitplan*, wenn das Agent-Provisioning aus Ermittlungsergebnissen initiiert wird. Weitere Informationen hierzu finden Sie unter KACE Agent auf einem Gerät oder auf mehreren Geräten installieren. • Auf der Seite *Details zur Geräteverbindung ohne Agent*, wenn ein neues Gerät automatisch aus Ermittlungsergebnissen bereitgestellt wird. Weitere Informationen zu dieser Seite finden Sie unter Verwaltung ohne Agent durch manuelle Eingabe von Geräteinformationen aktivieren.

7. Erweitern Sie *SNMP* und wählen Sie die Erkennungsoptionen aus.

Option	Beschreibung
SNMP - vollständiger Durchlauf	Aktiviert auf Geräten einen vollständigen Durchlauf von Daten in der MIB (Management Information Base). Wenn diese Option deaktiviert ist, führt die Appliance einen „Bulk GET“-Vorgang durch, bei dem drei Haupt-OIDs (Objektbezeichner) durchsucht werden. Beachten Sie, dass ein vollständiger Durchlauf pro Gerät bis zu 20 Minuten dauern kann. „Bulk GET“ dauert standardmäßig etwa eine Sekunde und erfasst sämtliche Informationen, die zur Erkennung erforderlich sind. **HINWEIS:** Beim SNMP-Inventardurchlauf werden auf Windows-Geräten keine nicht-englischen Zeichen unterstützt. Werden nicht-englische Zeichen erkannt, meldet die SNMP-Inventarisierung einen Fehler und beendet das Laden von Inventarinformationen.
Timeout	Die Zeit (in Sekunden), nach der der Scan endet, falls keine Reaktion erfolgt.
Maximale Anzahl Versuche	Die Anzahl der Verbindungsversuche.
Anmeldeinformationen (SNMP v1/v2)	Die Details der SNMP v1/v2-Anmeldeinformationen, die erforderlich sind, um eine Verbindung zum Gerät herzustellen und Befehle auszuführen. Wählen Sie vorhandene Anmeldeinformationen

Option	Beschreibung
	in der Dropdown-Liste aus oder wählen Sie **Neue Anmeldeinformationen hinzufügen** aus, um nicht bereits aufgeführte Anmeldeinformationen hinzuzufügen. Siehe Hinzufügen und Bearbeiten von SNMP-Anmeldeinformationen.
Anmeldeinformationen (SNMP v3)	Die Details der SNMP v3-Anmeldeinformationen, die erforderlich sind, um eine Verbindung zum Gerät herzustellen und Befehle auszuführen. Wählen Sie vorhandene Anmeldeinformationen in der Dropdown-Liste aus oder wählen Sie **Neue Anmeldeinformationen hinzufügen** aus, um nicht bereits aufgeführte Anmeldeinformationen hinzuzufügen. Siehe Hinzufügen und Bearbeiten von SNMP-Anmeldeinformationen.

8. **Optional**: Geben Sie im Abschnitt *Benachrichtigen* eine E-Mail-Adresse ein, um sich bei Abschluss des Erkennungsscans benachrichtigen zu lassen. Die E-Mail enthält den Namen des Erkennungszeitplans.
9. Legen Sie den Scan-Zeitplan fest:

TIPP: Zum Verwalten des Scan-Inventars ohne Überprüfen legen Sie den Zeitplan der Scan-Konfiguration auf **Keine**.

Option	Beschreibung
Kein(e)	Die Ausführung erfolgt im Zusammenhang mit einem Ereignis anstatt zu einem bestimmten Datum oder zu einem bestimmten Zeitpunkt.
jede Stunde	Der Vorgang wird im angegebenen Intervall durchgeführt.
Täglich/an einem bestimmten Tag um HH:MM	Die Erfassung wird täglich zu einem bestimmten Zeitpunkt oder an einem bestimmten Wochentag um eine bestimmte Uhrzeit ausgeführt.
Ausführen am n-ten jedes Monats/eines bestimmten Monats um HH:MM	Die Erfassung wird jeden Monat oder in einem bestimmten Monat an einem festgelegten Datum zu einer festgelegten Uhrzeit ausgeführt.
Ausführen am n-ten Wochentag **jedes Monats/ eines bestimmten Monats um HH:MM**	Die Erfassung wird jeden Monat oder in einem bestimmten Monat an einem festgelegten Wochentag zu einer festgelegten Uhrzeit ausgeführt.

Benutzerdefiniert	Führen Sie die Erfassung nach einem benutzerdefinierten Zeitplan aus.
	Verwenden Sie das Standard-5-Feld-Cron-Format (das erweiterte Cron-Format wird nicht unterstützt):
	`* * * * *`
	`| | | | +————Wochentag (0-6) (Sonntag=0)`
	`| | | +————Monat (1-12)`
	`| | +————Monatstag (1-31)`
	`| +————Stunde (0-23)`

Option	Beschreibung
	`+————————Minute (0-59)` Verwenden Sie bei der Angabe von Werten die folgenden Zeichen: • **Leerzeichen( )**: Die einzelnen Felder mit einem Leerzeichen trennen. • **Sternchen (*)**: Ein Sternchen repräsentiert den gesamten Wertebereich in einem Feld. Zum Beispiel repräsentiert ein Sternchen im Stundenfeld eine beliebige Stunde. • **Kommas (,)**: Mehrere Werte in einem Feld werden mit einem Komma getrennt. Zum Beispiel werden mit `0,6` im Feld „Wochentag“ Sonntag und Samstag angegeben. • **Bindestriche (-)**: Mit einem Bindestrich wird ein Wertebereich in einem Feld angegeben. Zum Beispiel entspricht `1-5` im Feld „Wochentag“ `1,2,3,4,5`, d. h. Montag bis Freitag. • **Schrägstriche (/)**: Die Angabe der Zeitabstände, mit denen eine Aktion wiederholt werden soll, erfolgt mit einem Schrägstrich. Zum Beispiel entspricht `*/3` im Feld Stunde `0,3,6,9,12,15,18,21`. Das Sternchen (`*`) gibt jede Stunde an, mit `/3` erfolgt aber eine Einschränkung auf durch drei teilbare Stunden. Beispiele: • `15 * * * * Jeden Tag 15 Minuten nach jeder vollen Stunde ausführen` • `0 22 * * * Jeden Tag um 22:00 Uhr ausführen` • `0 0 1 1,6 * Am 1. Januar und 1. Juni um 00:00 Uhr ausführen` • `30 8,12 * * 1-5 An Wochentagen um 08:30 Uhr und 12:30 Uhr ausführen` • `0 2 */2 * * Jeden zweiten Tag um 02:00 Uhr ausführen`
Aufgabenplan anzeigen	Klicken Sie, um den Aufgabenplan anzuzeigen. Im Dialogfeld *Aufgabenplan* wird eine Liste der geplanten Aufgaben angezeigt. Klicken Sie auf eine Aufgabe, um die Aufgabendetails anzuzeigen. Weitere Informationen hierzu finden Sie unter Aufgabenpläne anzeigen.

10. Klicken Sie auf **Speichern**.

Verwandte Themen

Informationen zu Erkennungsergebnissen

Erkennungsergebnisse anzeigen und durchsuchen

Laufenden Erkennungsscan anhalten

Erkennungszeitpläne löschen

Informationen zu Erkennungsergebnissen

Die Erkennungsergebnisse enthalten die Informationen, die im Rahmen geplanter Erkennungsscans ermittelt wurden.

Entsprechen Geräte aus dem Inventar den Datensätzen in den Erkennungsergebnissen, wird der aktuelle Verbindungsstatus der Geräte angezeigt. Der Gerätename ist mit der Inventardetailseite für das entsprechende Gerät verknüpft und die Dropdown-Liste *Geräteaktionen* in der Spalte *DNS-Lookup* enthält die verfügbaren Geräteaktionen.

HINWEIS: Weitere Informationen zu den Browseranforderungen für Geräteaktionen finden Sie unter https://support.quest.com/kb/148787.

Erkennungsergebnisse bieten eine Übersicht über einen bestimmten Zeitpunkt. Der Status von neu für die Verwaltung festgelegten Geräten wird bei der nächsten Ausführung der Erkennung angezeigt.

Siehe Verwalten von Inventarinformationen.

Ergebnisse, die die IP-Adresse zum Zeitpunkt des Scans enthalten, geben möglicherweise nicht die aktuelle IP-Adresse eines bestimmten Geräts wieder, wenn sich die DHCP-zugewiesene IP-Adresse geändert hat.

Erkennungsergebnisse anzeigen und durchsuchen

Sie können Erkennungsergebnisse anzeigen und nach Geräteinformationen sowie nach den Eigenschaften der für die Geräteerkennung verwendeten Scans suchen.

1. Rufen Sie die Liste *Erkennungsergebnisse* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Inventar** und anschließend auf **Erkennungsergebnisse**.
2. Führen Sie einen der folgenden Schritte aus, um die Liste zu sortieren:
   - **Wählen Sie Aktion auswählen > Nicht erreichbare Elemente einschließen aus. Die Liste zeigt Geräte an, die eine Verbindung zur Appliance haben, sowie Geräte, die aktuell nicht erreicht werden können.**
   - **Wählen Sie in der Dropdown-Liste** *Anzeigen nach* **die Option Erkennungsname aus. Die Liste wird gruppenweise nach dem Namen des Erkennungszeitplans, unter dem sie erkannt wurden, sortiert.**
3. Klicken Sie zum Anzeigen der Gerätedetails auf den Link in der Spalte *Hostname* oder *IP-Adresse [Labels]*.
4. So suchen Sie nach Geräten:
   a. Klicken Sie oberhalb der Liste auf der rechten Seite auf die Registerkarte **Erweiterte Suche**, um den Bereich *Erweiterte Suche* anzuzeigen.
   b. Wählen Sie Suchkriterien aus:
      - Wählen Sie in der Dropdown-Liste ganz links ein Attribut aus. Beispiel: **Geräteinfo: Ping-Test**
      - Wählen Sie in der nächsten Dropdown-Liste eine Bedingung aus. Beispiel: **hat**.
      - Wählen Sie in der nächsten Dropdown-Liste das Statusattribut aus. Beispiel: **Fehler**.
   c. Klicken Sie auf **Suchen**.

Agent über die erkannte IP-Adresse oder den erkannten Hostnamen provisionieren

Sie können den Agenten über die IP-Adresse oder den Hostnamen auf der Seite *Erkennungsergebnisse* auf Geräten provisionieren.

Sobald Geräte in den Erkennungsergebnissen identifiziert wurden, können Sie den Agenten auf diesen Geräten mithilfe der Links auf der Seite *Erkennungsergebnisse* provisionieren oder installieren. Auf diese Weise werden die zu provisionierenden Geräte gleich zu Beginn identifiziert und müssen zur Identifizierung nicht während der Provisionierungsphase gescannt werden.

Das Provisionieren des Agenten ist besonders bei Windows-Geräten sinnvoll. Windows Geräte können zwar erkannt werden, doch es stehen für sie nur wenige Verwaltungsoptionen zur Verfügung, wenn der Agent nicht darauf installiert ist.

1. Rufen Sie die Liste *Erkennungsergebnisse* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Inventar** und anschließend auf **Erkennungsergebnisse**.
2. Aktivieren Sie das Kontrollkästchen neben einem oder mehreren Geräten.
3. Wählen Sie **Aktion auswählen** aus und führen Sie eine der folgenden Aktionen durch:
   - **Wählen Sie Provisionieren > Agent: IP-Adresse.**
   - **Wählen Sie Provisionieren > Agent: Hostname.**

   Die Seite *Detail zum Provisionierungszeitplan* wird angezeigt. Auf der Seite werden Informationen zu den ausgewählten Geräten angezeigt.
4. Bearbeiten Sie die Provisionierungsoptionen nach Bedarf.

   Siehe KACE Agent auf einem Gerät oder auf mehreren Geräten installieren.

Laufenden Erkennungsscan anhalten

Sie können einen laufenden Erkennungsscan jederzeit anhalten.

Sie können einen laufenden Erkennungsscan über die Liste *Erkennungszeitpläne* oder über die Seite *Detail zum Erkennungszeitplan* anhalten. Mit der Liste *Erkennungszeitpläne* lassen sich mehrere Scans gleichzeitig anhalten.

Wenn Sie einen Scan mit **Anhalten** unterbrechen, werden alle bis dahin gescannten Geräte in dem IP-Bereich unter *Erkennungsergebnisse* angezeigt.

1. Rufen Sie die Liste *Erkennungszeitpläne* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Inventar** und anschließend auf **Erkennungszeitpläne**.
2. Sie können einen laufenden Scan auf zwei Weisen anhalten:
   - **Öffnen Sie zum Anhalten eines oder mehrerer Scans das Menü Aktion auswählen.**
     1. Aktivieren Sie das Kontrollkästchen neben einem oder mehreren Zeitplänen.

2. Wählen Sie **Aktion auswählenAnhalten** aus und klicken Sie dann zum Bestätigen auf **Ja**.

   HINWEIS: Wird einer der ausgewählten Zeitpläne nicht ausgeführt, lässt sich durch Auswählen von **Anhalten** nicht verhindern, dass der Scan zum nächsten geplanten Zeitpunkt ausgeführt wird.

- **Beenden Sie einen laufenden Scan über die zugehörige Seite** *Detail zum Erkennungszeitplan***.**

1. Klicken Sie in der Spalte *Name* auf den gewünschten Erkennungszeitplan, um die zugehörige Seite *Detail zum Erkennungszeitplan* anzuzeigen.
2. Klicken Sie unten auf der Seite auf **Anhalten** und dann zur Bestätigung auf **Ja**.

   HINWEIS: Wird ein Scan ausgeführt, sehen Sie die Schaltfläche **Anhalten** statt **Jetzt ausführen**.

Das Scannen für den gekennzeichneten Erkennungszeitplan wurde angehalten. Die Spalte *Bearbeitungsstatus* in der Liste *Erkennungszeitpläne* zeigt *Anhalten*, bis der Scan vollständig beendet wurde. Sie erkennen das daran, dass als Status *Angehalten* angezeigt wird.

Erkennungszeitpläne löschen

Sie können Erkennungszeitpläne nach Bedarf löschen. Wenn Erkennungszeitpläne gelöscht werden, werden die Scan-Ergebnisse, die mit diesen Zeitplänen zusammenhängen, ebenfalls gelöscht. Die mithilfe dieser Zeitpläne erkannten (und dem Inventar hinzugefügten) Geräte verbleiben jedoch im Inventar.

1. Rufen Sie die Liste *Erkennungszeitpläne* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Inventar** und anschließend auf **Erkennungszeitpläne**.
2. Aktivieren Sie das Kontrollkästchen neben einem oder mehreren Zeitplänen.
3. Wählen Sie **Aktion auswählen > Löschen** und klicken Sie dann zum Bestätigen auf **Ja**.

Verwalten des Geräteinventars

Die Appliance ermöglicht die Verwaltung von Geräten. Mit der Appliance verwaltete Geräte werden als Geräteinventar bezeichnet.

Informationen zur Geräteverwaltung

Das Verwalten von Geräten mithilfe der Appliance umfasst das Sammeln und Pflegen von Informationen über die Geräte im Netzwerk und das Durchführen von Aufgaben, wie beispielsweise Gerätestatus überwachen, Berichte erstellen usw.

Sie haben folgende Möglichkeiten, um Geräte zum Appliance-Inventar hinzuzufügen:

- **KACE Agent auf Geräten installieren**. Geräte werden automatisch zum Inventar hinzugefügt, nachdem der Agent auf ihnen installiert wurde und der Agent Inventar an die Appliance meldet. Siehe Provisionierung des KACE Agent.
- **Verwaltung ohne Agent für Geräte aktivieren**. Die Verwaltung ohne Agent ist besonders bei Geräten nützlich, auf denen der KACE Agent nicht installiert werden kann, beispielsweise bei Geräten mit nicht unterstützten Betriebssystemen. Siehe Geräte ohne Agent verwalten.
- **Manuelles Hochladen von Inventarinformationen für Geräte**. Siehe Manuelles Hinzufügen von Geräten in der Administratorkonsole oder mithilfe der API.

HINWEIS: Die Produktlizenzvereinbarung berechtigt Sie zur Verwaltung einer bestimmten Anzahl von Geräten, die als verwaltete Computer, Assets und überwachte Server klassifiziert sind. Hierzu zählen auch Geräte, die als "Ausstehend" (MIA, Missing in Action) eingestuft sind oder nicht mehr verwendet werden. Geräte, die dem Inventar manuell oder über die API hinzugefügt wurden, werden bei den Lizenzlimits dagegen nicht berücksichtigt. Siehe Produktlizenzinformationen anzeigen.

Information zu den für Geräte verfügbaren Funktionen finden Sie unter Funktionen, die für jede einzelne Geräteverwaltungsmethode zur Verfügung stehen.

Funktionen, die für jede einzelne Geräteverwaltungsmethode zur Verfügung stehen

Die Funktionen zum Verwalten von Geräten variieren je nachdem, mithilfe welcher Methode das Gerät und das Betriebssystem des Geräts verwaltet werden.

Windows Geräte erhalten durch das Installieren des Agenten einen breiten Funktionsumfang. Für Linux®-Geräte und Geräte, auf denen der Agent nicht installiert werden kann (wie etwa Drucker oder Netzwerkgeräte), wird die Verwaltung ohne Agent empfohlen.

Die folgende Tabelle liefert ein hohes Maß an Ansichten von Komponenten und Funktionen, die für verwaltete Geräte zur Verfügung stehen.

HINWEIS: Zu den *Windows fremden* Betriebssystemen unter *Ohne Agent* zählen Mac OS X, CentOS™, Debian®, FreeBSD®, Oracle® Enterprise Linux, Red Hat Enterprise Linux, SUSE, Solaris® und Ubuntu.

Verfügbare Funktionen für verwaltete Geräte

Funktion oder Komponente	Agent	Ohne Agent							WSAPI Manuell
	Windows, Mac, Linux	Windows	Windows fremd	G Suite Geräte	KACE MDM	DMM	Workspace ONE	SNMP	
Startseite									
Dashboard Enthält ggf. Geräteinformationen. Siehe Informationen	X	X	X	X	X	X	X	X	

Funktion oder Komponente	Agent	Ohne Agent							WSAPI Manuell
	Windows, Mac, Linux	Windows	Windows fremd	G Suite Geräte	KACE MDM	DMM	Workspace ONE	SNMP	
zu Dashboards.									
Label-Verwaltung: Labels können Geräten zugeordnet werden. Siehe Informationen zu den Labels.	X	X	X	X	X	X	X	X	X
Suchen: In den Ergebnissen enthaltene Geräte. Siehe Suchen nach Informationen und Filtern von Listen.	X	X	X	X	X	X	X	X	X
Inventar									
Geräte: Liste enthält Geräte. Siehe Verwalten von Inventarinformationen.	X	X	X	X	X	X	X	X	X
Geräte > Inventar erzwingen. Siehe Erzwingen von Inventaraktualisierungen.	X	X	X	X	X	X	X	X	
Geräte > Einstellungen	X	X	X	X	X	X	X	X	

Funktion oder Komponente	Agent	Ohne Agent						WSAPI	Manuell
	Windows, Mac, Linux	Windows	Windows fremd	G Suite Geräte	KACE MDM	DMM	Workspace ONE	SNMP	
für "Ausstehend". Siehe Verwalten ausstehender Geräte.									
Geräte > SNMP-Konfigurationen anwenden. Siehe Erkennen bestimmter, dem Inventar hinzuzufügender SNMP-Objekte und Nicht-Computer-Geräte mithilfe von SNMP-Inventarkonfigurationen.								X	
Seite "Software": Liste enthält Software von Geräten. Siehe Informationen zur Seite "Software".	X	X	X	X	X	X	X		
Seite "Softwarekatalog": Liste enthält Software von Geräten. Siehe Anzeigen von Informationen	X nur Windows und Mac								

Funktion oder Komponente	Agent	Ohne Agent						WSAPI	
	Windows, Mac, Linux	Windows	Windows fremd	G Suite Geräte	KACE MDM	DMM	Workspace ONE	SNMP	Manuell
im Softwarekatalog.									
Erfassung der Nutzung: Die Erfassung der Nutzung kann für Geräte aktiviert werden. Siehe Verwenden der Erfassung der Softwarenutzung.	X nur Windows und Mac								
Blockieren von Software (Kennzeichnen als "Nicht zulässig"): Software kann daran gehindert werden, auf Geräten ausgeführt zu werden. Siehe Verwenden der Anwendungssteuerung.	X nur Windows und Mac								
Prozesse: Inventar verfügbar für Geräte. Siehe Verwalten	X	X	X						

Funktion oder Komponente	Agent	Ohne Agent							WSAPI Manuell
	Windows, Mac, Linux	Windows	Windows fremd	G Suite Geräte	KACE MDM	DMM	Workspace ONE	SNMP	
des Prozessinventars.									
Startprogramme: Inventar verfügbar für Geräte. Siehe Verwalten des Startprogramm-Inventars.	X	X	X						
Dienste: Inventar verfügbar für Geräte. Siehe Verwalten des Dienstinventars.	X	X							
Erkennungszeitpläne: Geräte können entdeckt werden. Siehe Informationen zu Geräteerkennung und -verwaltung.	X	X	X	X	X	X	X	X	X
Erkennungsergebnisse: Geräte können auf der Grundlage der Ergebnisliste provisioniert werden. Siehe Informationen zu Geräteerkennung	X	X	X	X	X	X	X	X	

Funktion oder Komponente	Agent	Ohne Agent							WSAPI Manuell
	Windows, Mac, Linux	Windows	Windows fremd	G Suite Geräte	KACE MDM	DMM	Workspace ONE	SNMP	
und -verwaltung.									
SNMP-Inventarkonfigurationen: Die Geräteliste kann erweitert werden. Siehe Erkennen bestimmter, dem Inventar hinzuzufügender SNMP-Objekte und Nicht-Computer-Geräte mithilfe von SNMP-Inventarkonfigurationen.								X	
Inventar: Regeln für benutzerdefinierte Inventarisierung Siehe Erstellen benutzerdefinierter Inventarregeln.	X								
Überwachung									
Warnungen: Empfangene Warnungen. Siehe Arbeiten mit Warnungen.	X	X	X						
Geräte: Die Liste enthält	X	X	X						

Funktion oder Komponente	Agent	Ohne Agent						WSAPI	Manuell
	Windows, Mac, Linux	Windows	Windows fremd	G Suite Geräte	KACE MDM	DMM	Workspace ONE	SNMP	
Geräte mit aktivierter Überwachung. Siehe Verwalten der Geräteüberwachung.									
Profile: Warnungen werden über Profile definiert. Siehe Verwenden von Überwachungsprofilen.	X	X	X						
Wartungsfenster: Sie können einen Zeitplan für die regelmäßige Aussetzung der Überwachung festlegen. Siehe Wartungsfenster planen, während dessen keine Alarme von einem Gerät erfasst werden.	X	X	X						
Log Enablement Packages Diese Pakete ermöglichen die	X	X	X						

Funktion oder Komponente	Agent	Ohne Agent							WSAPI Manuell
	Windows, Mac, Linux	Windows	Windows fremd	G Suite Geräte	KACE MDM	DMM	Workspace ONE	SNMP	
Überwachung von Leistungsschwellenwerten sowie von Anwendungen, wie z. B. Exchange, Internetinformationsdienste (Internet Information Services, IIS) usw. Siehe Konfigurieren der Anwendungs- und Schwellenwertüberwachung mit Log Enablement Packages (LEP).									
Assets									
Assets: Erstellung für Geräte möglich Siehe Informationen zum Verwalten von Assets.	X	X	X	X	X	X	X	X	X
Asset-Typen: Erstellung für Geräte möglich Siehe Hinzufügen und Anpassen von Asset-Typen	X	X	X	X	X	X	X	X	X

Funktion oder Komponente	Agent	Ohne Agent							WSAPI Manuell
	Windows, Mac, Linux	Windows	Windows fremd	G Suite Geräte	KACE MDM	DMM	Workspace ONE	SNMP	
und Verwalten von Asset-Informationen.									
Locations: Kann für Geräte, Benutzer und Assets definiert werden. Siehe Standorte verwalten.	X	X	X	X	X	X	X	X	X
Assets importieren: Import für Geräte möglich Siehe Importieren von Lizenzdaten in CSV-Dateien.	X								
Verteilung									
Verwaltete Installationen: Verwendung zum Installieren von Software auf Geräten möglich Siehe Verwenden verwalteter Installationen.	X								
Dateisynchronisierungen: Verwendung	X								

Funktion oder Komponente	Agent	Ohne Agent							WSAPI Manuell
	Windows, Mac, Linux	Windows	Windows fremd	G Suite Geräte	KACE MDM	DMM	Workspace ONE	SNMP	
zum Verwalten von Dateien auf Geräten möglich Siehe Dateisynchronisierungen erstellen und verwenden.									
Wake on LAN: Verfügbar für Geräte mit gültiger IP-Adresse und MAC-Adresse Siehe Verwenden von Wake on LAN.	X	X	X					X	
Replikation: Verwendung als Replikationsfreigaben möglich Siehe Verwenden von Replikationsfreigaben.	X								
Warnungen: Können gesendet und auf Geräten angezeigt werden (anders als bei Warnungen	X nur Windows und Mac								

Funktion oder Komponente	Agent	Ohne Agent						WSAPI	Manuell
	Windows, Mac, Linux	Windows	Windows fremd	G Suite Geräte	KACE MDM	DMM	Workspace ONE	SNMP	
der Serverüberwachung). Siehe Senden von Warnungen an verwaltete Geräte.									
Skripterstellung									
Jetzt ausführen: Verwendung zum Ausführen von Skripten auf Geräten möglich. Siehe Verwenden der Befehle "Ausführen" und "Jetzt ausführen".	X								
'Jetzt ausführen'-Status: Anzeige für Geräte möglich. Siehe Den Status von "Jetzt ausführen" überwachen und Skriptdetails anzeigen.	X								
Skriptprotokolle durchsuchen:	X								

Funktion oder Komponente	Agent	Ohne Agent						WSAPI	Manuell
	Windows, Mac, Linux	Windows	Windows fremd	G Suite Geräte	KACE MDM	DMM	Workspace ONE	SNMP	
In den Ergebnissen aufgeführte Geräte. Siehe Die Skriptprotokolle durchsuchen.									
Konfigurationsrichtlinien: Verwendung zum Konfigurieren von Geräten möglich. Siehe Informationen zu den Konfigurationsrichtlinienvorlagen.	X Nur Windows und Mac								
Mac Profile: Kann verwendet werden, um Richtlinien und Einstellungen auf Benutzer- und Systemebene auf Mac OS X Geräten zu konfigurieren. Siehe Verwalten von Mac Profilen.	X Nur Mac								
Sicherheit									
Patch-Verwaltung: Verwendung zum Aufspielen	X Nur Windows und Mac								

Funktion oder Komponente	Agent	Ohne Agent						WSAPI	Manuell
	Windows, Mac, Linux	Windows	Windows fremd	G Suite Geräte	KACE MDM	DMM	Workspace ONE	SNMP	
von Patches auf Geräte möglich. Siehe Informationen zur Patch-Verwaltung.									
OVAL-Scans: In den Tests enthaltene Geräte Siehe Informationen zu OVAL-Sicherheitsprüfungen.	X Nur Windows								
SCAP-Scans: In den Scans enthaltene Geräte. Siehe Informationen zu SCAP.	X Nur Windows								
Dell Aktualisierungen: Verwendung zum Aktualisieren von Geräten möglich. Siehe Verwalten von Dell Geräten und Aktualisierungen.	X Nur Windows								

Funktion oder Komponente	Agent	Ohne Agent							WSAPI Manuell
	Windows, Mac, Linux	Windows	Windows fremd	G Suite Geräte	KACE MDM	DMM	Workspace ONE	SNMP	
Service Desk									
Tickets: Erstellung und Zuordnung zu Geräten möglich. Siehe Erstellen von Tickets über die Administratorkonsole und Benutzerkonsole.	X	X	X	X	X	X	X	X	
Benutzerdownloads: Software kann aus der **Benutzerkonsole** auf die Geräte heruntergeladen werden. Siehe Verwalten von Benutzerdownloads.	X								
Knowledge Base. Siehe Verwalten von Knowledge Base-Artikeln.	X	X	X	X	X	X	X	X	
Ankündigungen: Kann Ankündigungen erstellen, die auf der Startseite der	X	X	X	X	X	X	X	X	

Funktion oder Komponente	Agent	Ohne Agent							WSAPI Manuell
	Windows, Mac, Linux	Windows	Windows fremd	G Suite Geräte	KACE MDM	DMM	Workspace ONE	SNMP	
Benutzerkonsole angezeigt werden. Siehe Benutzerkonsole-Ankündigungen hinzufügen, bearbeiten, ausblenden oder löschen.									
Konfiguration. Siehe Einrichten des Service Desks.	X	X	X	X	X	X	X	X	
Berichterstellung									
Berichte: Geräteinformationen verfügbar für Berichte. Siehe Erstellen von Berichten.	X	X	X	X	X	X	X	X	
Berichtszeitpläne: Zeigt erstellte Berichtszeitpläne an. Siehe Planen von Berichten.	X	X	X	X	X	X	X	X	
Benachrichtigungen: Geräte können in Benachrichtigungen eingefügt werden. Siehe Zeitplanung	X	X	X	X	X	X	X	X	

Funktion oder Komponente	Agent	Ohne Agent							WSAPI	Manuell
	Windows, Mac, Linux	Windows	Windows fremd	G Suite Geräte	KACE MDM	DMM	Workspace ONE	SNMP		
für Benachrichtigungen.										
Einstellungen: Systemsteuerung										
Geräteaktionen: Aktionen können auf Geräten ausgeführt werden. Siehe Aktionen auf Geräten ausführen.	X	X	X					X		
Warnstufen zur Lizenznutzung: Verfügbar für Anwendungen auf Geräten. Siehe Anwendungen Bedrohungsstufen zuweisen.	X	X	X	X	X	X	X	X		
Verlauf: Geräteinformationen können nachverfolgt werden. Siehe Asset-Verlauf verwalten.	X	X	X	X	X	X	X	X		
Protokolle: Geräteinformationen verfügbar. Siehe Appliance-Protokolle anzeigen.	X	X	X	X	X	X	X	X		

Funktion oder Komponente	Agent	Ohne Agent							WSAPI Manuell
	Windows, Mac, Linux	Windows	Windows fremd	G Suite Geräte	KACE MDM	DMM	Workspace ONE	SNMP	
Sicherung und Wiederherstellung: Geräteinformationen enthalten. Siehe Informationen zu Appliance-Sicherungen.	X	X	X	X	X	X	X	X	
Organisationen									
Filter: Organisationsfilter können Geräten zugeordnet werden. Siehe Verwalten von Organisationsfiltern.	X	X	X	X	X	X	X	X	
Geräte neu zuweisen: Geräte können Organisationen neu zugewiesen werden. Siehe Geräte umleiten.	X	X	X	X	X	X	X	X	X
Filtern von Geräten: Geräte können gefiltert und Organisationen neu zugewiesen werden. Siehe	X	X	X	X	X	X	X	X	

Funktion oder Komponente	Agent	Ohne Agent						WSAPI Manuell
	Windows, Mac, Linux	Windows	Windows fremd	G Suite Geräte	KACE MDM	DMM	Workspace ONE	SNMP
Geräte filtern.								
Organisationseinstellungen: Inventarintervalle konfigurierbar. Siehe Inventardatensammlung für verwaltete Geräte planen.	X	X	X	X	X	X	X	X

Informationen zu Inventarinformationen

Das Inventar enthält Informationen über die Geräte, Anwendungen, Prozesse, Startprogramme sowie Dienste auf verwalteten Geräten in Ihrem Netzwerk.

Das Inventar wird:

- Von einem auf verwalteten Geräten installierten KACE Agent erfasst
- Über die Inventar-API hochgeladen
- Über Verbindungen mit Geräten ohne Agent abgerufen

Sie können detaillierte Daten zu einzelnen verwalteten Geräten sowie zusammengefasste Daten, die über alle verwalteten Geräte hinweg gesammelt wurden, anzeigen. Außerdem können Sie die Inventarinformationen in Berichten sowie bei Entscheidungen bezüglich Upgrades, Fehlerbehebung, Einkäufen, Richtlinien usw. nutzen.

Dieser Abschnitt behandelt in erster Linie das Geräteinventar. Weitere Informationen zu Inventarelementen finden Sie unter:

- Verwalten von Anwendungen auf der Seite "Software"
- Verwalten des Softwarekataloginventars
- Verwalten des Prozess-, Startprogramm- und Dienstinventars

Erfassen von Änderungen an Inventareinstellungen

Wenn Verlaufsabonnements zur Aufbewahrung von Informationen konfiguriert wurden, können Sie Details zu den an Einstellungen, Assets und Objekten vorgenommenen Änderungen anzeigen.

Diese Informationen beinhalten auch das Datum der Änderung und den Benutzer, der diese vorgenommen hat. Dies kann bei der Fehlerbehebung nützlich sein. Siehe Informationen zu den Verlaufseinstellungen.

Informationen zum Inventaränderungsverlauf

Der Änderungsverlauf für das Geräteinventar beginnt, sobald Änderungen an den im ersten Bericht erfassten Informationen auftreten.

Bei der ersten Inventarmeldung eines verwalteten Geräts an die Appliance werden die Informationen als Grundlagenbericht betrachtet. Die Informationen werden daher nicht im Änderungsverlauf aufgezeichnet.

Verwalten von Inventarinformationen

Im Zuge der Verwaltung von Inventarinformationen können Sie benutzerdefinierte Datenfelder hinzufügen sowie im Inventar enthaltene Geräte und Gerätedetails anzeigen.

Benutzerdefinierte Datenfelder hinzufügen

Sie können benutzerdefinierte Datenfelder für Anwendungen hinzufügen, die manuell über die Liste *Software* hinzugefügt wurden.

Mithilfe hinzugefügter benutzerdefinierter Datenfelder können Sie Informationen aus der Registrierung oder aus anderen Gerätebereichen abrufen. Diese Informationen stehen auf der Gerätedetailseite und in Berichten zur Verfügung.

Mithilfe benutzerdefinierter Felder können Sie beispielsweise die *DAT-Dateiversionsnummer* aus der Registrierung, das *Dateierstellungsdatum*, den *Herausgeber der Datei* oder andere Daten für ein Gerät abrufen. Auf der Grundlage dieser Informationen können Sie dann Labels erstellen, um ähnliche Geräte zu gruppieren, oder Berichte mit diesen Informationen generieren.

1. Rufen Sie die Liste *Software* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Inventar** und anschließend auf **Software**.
2. Wählen Sie **Aktion auswählen > Neu**.
3. Geben Sie Werte in die Felder *Name*, *Version* und *Herausgeber* ein.

   Anhand dieser Informationen werden die benutzerdefinierten Datenfelder auf Detailseiten identifiziert.
4. Geben Sie in das Feld *Regel für benutzerdefinierte Inventarisierung* die entsprechende Syntax ein, um die gewünschten Informationen zu erhalten:
   - **Wenn ein Registrierungswert zurückgegeben werden soll, geben Sie Folgendes ein und ersetzen Sie valueType durch `TEXT`, `NUMMER` oder `DATUM`. `NUMMER` ist ein ganzzahliger Wert: `RegistryValueReturn(string absPathToKey, string valueName, string` valueType`)`**

     Beispiel: `RegistryValueReturn(HKEY_LOCAL_MACHINE\Software\McAfee.com\Virusscan Online,SourceDisk, TEXT)`
   - **Auf Windows, Mac und Linux Systemen können Sie die folgenden Attribute über die `stat()`-Funktion abrufen:**

     `access_time, creation_time, modification_time, block_size, blocks, size, device_id, group, inode, mode, number_links, owner, device_number`
   - **Auf Windows-Geräten können Sie die folgenden Attribute über die `VerQueryValue()`-Funktion abrufen:**

     `FileName, Comments, CompanyName, FileDescription, FileVersion, InternalName, LegalCopyright, LegalTrademarks, OriginalFilename,`

```
ProductName, ProductVersion, PrivateBuild, SpecialBuild, AccessedDate,
CreatedDate, ModifiedDate
```

5. Klicken Sie auf **Speichern**.

Siehe Erstellen benutzerdefinierter Inventarregeln.

Inventardatensammlung für verwaltete Geräte planen

Die Appliance erfasst Inventardaten zur Hardware und Software von Geräten mit und ohne Agentenverwaltung auf der Grundlage des festgelegten Datenerfassungszeitplans der Appliance.

Bei vom Agenten verwalteten Geräten stehen die Informationen zum Softwareinventar sowohl auf der Seite *Software* als auch auf der Seite *Softwarekatalog* zur Verfügung. Weitere Informationen zu diesen Seiten finden Sie unter Unterschiede zwischen den Seiten "Software" und "Softwarekatalog".

Bei Geräten ohne Agent werden die Softwareinformationen nur auf der Seite *Software* aufgeführt. Siehe Verwalten von Anwendungen auf der Seite "Software".

Wenn auf der Appliance die Organisationskomponente aktiviert wurde, können Sie die Inventardatenerfassung für jede Organisation individuell planen.

1. Führen Sie einen der folgenden Schritte aus:
   - **Wenn die Organisationskomponente für die Appliance aktiviert ist, melden Sie sich bei der Systemverwaltungskonsole der Appliance an: `https://appliance_hostname/system`. Oder wählen Sie in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen den Eintrag System aus. Klicken Sie anschließend auf Organisationen. Klicken Sie auf den Namen einer Organisation, um Informationen dazu anzuzeigen.**

     Die Seite *Detail zu Organisation* wird angezeigt. Suchen Sie hier nach dem Abschnitt *Kommunikations- und Agenten-Einstellungen*.
   - **Wenn die Organisationskomponente nicht für die Appliance aktiviert ist, melden Sie sich bei der Administratorkonsole der Appliance an: `https://appliance_hostname/admin`. Wählen Sie anschließend Einstellungen > Provisionierung und klicken Sie im Fensterbereich** *Provisionierung* **auf Kommunikationseinstellungen.**

     Die Seite *Kommunikationseinstellungen* wird angezeigt.
2. Geben Sie im Abschnitt *Agenten- und Kommunikationseinstellungen* folgende Einstellungen an:

   HINWEIS: Um die Auslastung der Appliance zu reduzieren, sollten Sie die Anzahl der Agenten-Verbindungen auf 500 pro Stunde begrenzen. Die Anzahl der Verbindungen, die neben den Inventarisierungs-, Skripterstellungs- und Erfassungsintervallen angezeigt wird, gilt nur für die aktuelle Organisation. Wenn die Organisationskomponente in Ihrer Appliance aktiviert ist, sollte die Gesamtzahl der Agenten-Verbindungen für alle Organisationen maximal 500 pro Stunde betragen.

Option	Empfohlene Einstellung	Anmerkungen
Agentenprotokollierung	Aktiviert	Gibt an, ob die Appliance Skriptergebnisse speichert, die von Agenten auf verwalteten Geräten übermittelt wurden. Agenten-Protokolle können in der Datenbank bis zu 1GB Speicherplatz benötigen. Wenn Speicherplatz keine Rolle spielt, aktivieren Sie die *Agentenprotokollierung*, um alle Protokollinformationen für vom Agenten verwaltete Geräte zu speichern. Diese Protokolle können bei der Fehlerbehebung nützlich sein. Um Speicherplatz

Option	Empfohlene Einstellung	Anmerkungen
		zu sparen und eine schnellere Kommunikation mit dem Agenten zu ermöglichen, deaktivieren Sie die *Agentenprotokollierung*.
Agenten-Inventar	12 Stunden	Die Häufigkeit, mit der Agenten auf verwalteten Geräten das Inventar melden. Diese Informationen werden im Abschnitt *Inventar* angezeigt.
Inventar ohne Agent	1 Tag	Die Häufigkeit, mit Geräte ohne Agent Inventar melden. Diese Informationen werden im Abschnitt *Inventar* angezeigt.
Kataloginventarisierung	24 Stunden	Die Häufigkeit, mit der verwaltete Geräte der Seite *Softwarekatalog* das Inventar melden sollen.
Erfassung der Nutzung	4 Stunden	Die Häufigkeit, mit der verwaltete Geräte der Appliance Erfassungsinformationen melden sollen. Damit dies möglich ist, muss die Erfassung auf Geräten und in Anwendungen aktiviert sein.
Skriptaktualisierung	4 Stunden	Die Häufigkeit, mit der Agenten auf den verwalteten Geräten aktualisierte Skriptkopien anfordern sollen, die auf verwalteten Geräten verfügbar sind. Dieses Intervall hat keine Auswirkungen darauf, wie häufig ein Skript ausgeführt wird.

3. Geben Sie im Abschnitt *Benachrichtigen* die Mitteilung für die Agenten-Kommunikation ein:

Option	Empfohlene Einstellung	Anmerkungen
Meldung auf der Begrüßungsseite des Agenten	Standardtext: **KACE Systemverwaltungs-Appliance** `überprüft die Aktualisierungen für die Konfigurations- und Verwaltungssoftware auf Ihrem PC. Bitte warten...`	Die Meldung, die Benutzern angezeigt wird, wenn Agenten Aufgaben ausführen, z.B. die Ausführung von Skripten auf ihren Geräten.

4. Legen Sie im Abschnitt *Ohne Agent* die Kommunikationseinstellungen für Geräte, die nicht vom Agenten verwaltet werden, fest:

Option	Beschreibung
SSH-Timeout	Die Zeit (in Sekunden oder Minuten), nach der eine inaktive Verbindung getrennt wird.

Option	Beschreibung
SNMP-Timeout	Die Zeit in Sekunden, nach der eine Verbindung geschlossen wird, wenn keine Aktivität stattfindet.
Maximale Anzahl Versuche	Die Anzahl der Verbindungsversuche.
WinRM-Timeout	Die Zeit (in Sekunden oder Minuten), nach der eine inaktive Verbindung getrennt wird.

5. Wenn die Organisationskomponente auf der Appliance nicht aktiviert ist, geben Sie die Einstellungen für den *Agenten* an.

   HINWEIS: Wenn die Organisationskomponente in Ihrer Appliance aktiviert ist, befinden sich die *Agent*-Einstellungen auf der Seite *Allgemeine Einstellungen* der Appliance.

Option	Beschreibung
Letzte Aktualisierung des Aufgabendurchsatzes	Dieser Wert gibt Datum und Uhrzeit der letzten Aktualisierung des Aufgabendurchsatzes der Appliance an.
Aktueller Lastdurchschnitt	Der Wert in diesem Feld steht für die Last einer Appliance zu einem bestimmten Zeitpunkt. Damit die Appliance normal läuft, muss der Feldwert zwischen 0,0 und 10,0 liegen.
Aufgabendurchsatz	Der Wert, der steuert, wie geplante Aufgaben, z.B. Inventarerfassung, Skripterstellung und Patch-Aktualisierungen, durch die Appliance ausbalanciert werden. **HINWEIS:** Dieser Wert kann nur erhöht werden, wenn der Wert im Feld Aktueller Lastdurchschnitt nicht über 10,0 liegt und die Zeit für die letzte Aktualisierung des Aufgabendurchsatzes mehr als 15 Minuten beträgt.

6. Klicken Sie auf **Speichern**.

   Die Änderungen werden wirksam, wenn sich Agenten bei der Appliance anmelden.
7. Wenn Sie mehrere Organisationen haben, wiederholen Sie die oben aufgeführten Schritte für jede Organisation.

Verwandte Themen

Appliance-Protokolle anzeigen

Allgemeine Appliance-Einstellungen bei aktivierter Organisationskomponente konfigurieren

Geräteinventar und Details anzeigen

Sie können die Liste der Geräte im Inventar auf der Seite *Geräte* und Informationen über jedes ausgewählte Gerät auf der Seite *Gerätedetail* anzeigen.

1. Rufen Sie die *Gerätedetailseite* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen*

aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.

b. Klicken Sie in der linken Navigationsleiste auf **Inventar** und anschließend auf **Geräte**.

c. Klicken Sie auf den Namen eines Geräts.

2. Klicken Sie über dem Abschnitt *Übersicht* auf **Alle erweitern**, um die Abschnitte auf der *Gerätedetailseite* zu erweitern.

   Welche Felder angezeigt werden ist abhängig von Gerätetyp und Betriebssystem. Handelt es sich bei dem Gerät beispielsweise um einen virtuellen Computer, wird das Feld *Monitor* nicht angezeigt, das Feld *Videocontroller* dagegen schon. Außerdem sind manche Felder für manche Betriebssysteme verfügbar und für andere nicht. So ist beispielsweise das Feld *Systembeschreibung* nur für Windows oder SNMP-Geräte verfügbar.

   Wie Sie Tabellen mit Inhaltsbeschreibungen der Gruppen und Abschnitte auf dieser Seite anzeigen, wird unter Elementegruppen und -abschnitte in Gerätedetails beschrieben.

3. **Optional**: Wenn die Änderungsnachverfolgung für Inventarinformationen aktiviert ist, klicken Sie oberhalb des Abschnitts *Übersicht* auf **Gesamten Verlauf anzeigen**, um den Verlauf der Inventaränderungen anzuzeigen.

Verwandte Themen

Konfigurieren der Verlaufseinstellungen

Kommunikation des Agenten verwalten

Inventardatensammlung für verwaltete Geräte planen

Informationen zu OVAL-Sicherheitsprüfungen

Informationen zu SCAP

Informationen zur Komponente Asset Management

Informationen zu Geräten anzeigen, die bei KACE Cloud MDM registriert sind

Die Appliance zeigt Informationen zu Mac OS X-Geräten an, die in einer integrierten KACE Cloud Mobile Device Manager-Instanz (MDM) registriert sind.

Die Art der für solche Geräte verfügbaren Informationen hängt davon ab, ob auf ihnen ein KACE Agent installiert ist. Es gibt drei mögliche Szenarien, die bestimmen, welche Art von Informationen von Mac OS X-Geräten erfasst werden, die bei KACE Cloud MDM registriert sind:

- „Hybrid-Appliance zuerst“-Gerätemanagement
- KACE Cloud MDM-Geräteverwaltung
- „Hybrid KACE Cloud MDM zuerst“-Gerätemanagement

„Hybrid-Appliance zuerst“-Gerätemanagement

1. Auf einem Mac OS X-Gerät ist ein KACE Agent installiert und für die Verbindung mit der Appliance konfiguriert.
2. Das Gerät ist bei KACE Cloud MDM registriert, das in die Appliance integriert ist.
3. Das Gerät erkennt das Gerät als standardmäßiges agentenbasiertes Gerät.

KACE Cloud MDM-Geräteverwaltung

1. Ein Mac OS X-Gerät ist bei KACE Cloud MDM registriert, das in die Appliance integriert ist.
2. KACE Cloud MDM erfasst Inventarinformationen vom Gerät.
3. Die Appliance erkennt das Gerät als standardmäßiges agentenloses KACE Cloud MDM-Gerät.

„Hybrid KACE Cloud MDM zuerst“-Gerätemanagement

1. Ein Mac OS X-Gerät ist bei KACE Cloud MDM registriert, das in die Appliance integriert ist.
2. KACE Cloud MDM erfasst Inventarinformationen vom Gerät.
3. Die Appliance erkennt das Gerät als standardmäßiges agentenloses KACE Cloud MDM-Gerät.
4. Ein KACE Agent ist auf dem Gerät installiert und für die Verbindung mit der Appliance konfiguriert.
5. Das Gerät erkennt das Gerät als standardmäßiges agentenbasiertes Gerät.

Weitere Informationen zu den Gerätfeldern auf der Seite *Gerätedetails* finden Sie unter Elementegruppen und -abschnitte in Gerätedetails.

Elementegruppen und -abschnitte in Gerätedetails

Die Seite *Gerätedetails* für ein Gerät enthält Inventarinformationen. Diese Informationen werden in verschiedenen Abschnitten dargestellt, die in Gruppen zusammengefasst sind. Der Umfang und Fokus von Informationen auf der Seite hängt von dem Gerät und jeglichen angegebenen Untertypen ab.

HINWEIS: Wenn Sie einen Asset-Untertyp zugeordnet haben, können Sie auswählen, ob die Details ausgeblendet werden sollen, die auf der Seite *Gerätedetail* für jedes Gerät angezeigt werden. Für den Untertyp *Drucker* können Informationen, die für Drucker nicht relevant sind, wie z. B. *Installierte Programme*, *Erkannte Software* und *Software mit erfasster Nutzung*, ausgeblendet werden. Es können auch ganze Gruppen versteckt werden. Siehe Asset-Untertypen hinzufügen und Voreinstellungen für die Seite "Gerätedetail" auswählen.

Benutzer mit eingeschränkten Zugriffsrechten können die Details aller Geräte anzeigen, sie können jedoch nur die Details der Geräte bearbeiten, die mit ihrer Rolle verknüpft sind. Weitere Informationen zu Benutzerrollen finden Sie unter Benutzerrollen hinzufügen oder bearbeiten.

Folgende Gruppen finden Sie auf der Seite *Gerätedetail*:

- Gruppe „Zusammenfassung“
- Gruppe „Inventarinformationen“
- Gruppe „Software“
- Gruppe „Aktivitäten“
- Gruppe „Sicherheit“
- Gruppe „Dell Command | Monitor“
- Gruppe „Dell Aktualisierungen“
- Gruppe für Protokolle und Diagnose
- Gruppe „Asset“

Gruppe „Zusammenfassung“

Grundlegende Informationen zum Identifizieren des Geräts. Die Elemente sind nicht wie andere Gruppen auf der Seite in Abschnitte unterteilt. Die Einträge, die auf der Seite *Gerätedetail* angezeigt werden, können je nach Gerät, Betriebssystem (sofern relevant), Verbindungstyp usw. abweichen.

Element	Beschreibung	Datenbankfeld
Systemname	Der Hostname oder die IP-Adresse des Geräts.	NAME
Asset-Untertyp	Der Asset-Untertyp für dieses Gerät, sofern einer zugewiesen wurde. Asset-Untertypen sind Unterkategorien von Assets,	

Element	Beschreibung	Datenbankfeld
	die Sie zu jedem Asset-Typ hinzufügen können, einschließlich benutzerdefinierter Asset-Typen. Dies ermöglicht es Ihnen, Untertypen von Assets zu erkennen und zu verwalten, wie z. B Geräte-Assets, bei denen es sich um Computer, Drucker oder Router handelt.	
Asset-Speicherort	Der Asset-Speicherort.	keine Angabe
Zugewiesen zu	Der Gerätebesitzer. Dieses Feld wird nur ausgefüllt, wenn der Geräte-Benutzerdatensatz auf der Appliance vorhanden ist. Wenn Sie mit dem KACE Cloud MDM integrieren und falls die Appliance mit dem KACE MDM Active Directory des Mandanten synchronisiert ist, wird der Name des KACE MDM Gerätebesitzers angezeigt. Für andere Arten von externen Geräten, und falls der Benutzerdatensatz des Gerätes nicht auf dem Gerät zu finden ist, wird das Feld auf *Nicht zugewiesen* gesetzt.	keine Angabe
Manuelle Eingabe	Dieses Feld gibt an, dass die Inventarinformationen manuell per WSAPI- oder XML-Upload hinzugefügt wurden. Klicken Sie auf **Bearbeiten**, um die Informationen zu ändern.	MANUAL_ENTRY
Geräteeintragstyp	Dieses Feld gibt Aufschluss über die Verwaltung des Geräts: *Gerät mit Agent*, *Gerät ohne Agent*, *Manuell eingegebener Datensatz* oder *Agent/ohne Agent* (Hybrid-KACE Cloud MDM-Bestand). Klicken Sie auf **Bearbeiten**, um Verbindungsprotokolle zu ändern.	keine Angabe
Systembeschreibung	Eine Beschreibung des Geräts, die im Rahmen der Inventarerfassung ohne Agent für Windows und SNMP-Geräte aufgefüllt wird.	Systembeschreibung
Systemmodell	Das Modell des Geräts	CS_MODEL
Gehäusetyp	Der Typ des Geräts, z.B. Desktop oder Notebook	CHASSIS_TYPE

Element	Beschreibung	Datenbankfeld
Besitz	**Nur KACE MDM-Geräte**. Gibt den Besitz des Geräts an: *Unternehmen Persönlich* oder *Unbekannt*.	OWNERSHIP
IP-Adresse	Die IP-Adresse des Geräts	IP
MAC-Adresse	Die Media Access Control (MAC)-Adressnummer des Geräts	MAC
RAM gesamt	Maximal verfügbarer RAM (Random Access Memory) des Geräts	RAM_TOTAL
Betriebssystemname	Das Betriebssystem des Geräts (beispielsweise Windows, Mac OS X® oder Linux).	OS_NAME
Service Pack	Die Versionsnummer des Service Packs (nur Windows oder SUSE Linux Enterprise Server).	SERVICE_PACK
Betriebszeit seit letztem Neustart	Die Zeit, die das Gerät seit dem letzten Neustart in Betrieb ist	UPTIME
Version des Agenten	Die Versionsnummer des auf dem Gerät installierten KACE Agent.	CLIENT_VERSION
Zeitzone des Geräts	Die Zeitzone, die der auf dem Gerät installierte KACE Agent verwendet.	TZ_AGENT
Quelle	Die Quelle der erfassten Gerätedetails. • **Vom Agenten verwaltete Geräte**: Dieses Feld ist auf `Agent` festgelegt. • **Geräte ohne Agent**: Dieses Feld gibt den Verbindungstyp an. Beispiel: `VMware`. • **Von Agenten verwaltete Geräte, die ebenfalls bei KACE Cloud MDM angemeldet sind**: Dieses Feld ist auf `Agent/KACE Cloud Mobile Device Manager` eingestellt. Klicken Sie auf den Link**KACE Cloud Mobile Device Manager**, um dieses Gerät im KACE	keine Angabe

Element	Beschreibung	Datenbankfeld
	MDM Cloud-Bestand anzuzeigen.	
Benutzername	Der Name des letzten Benutzers, der sich beim Gerät angemeldet hat Einige Geräte werden möglicherweise von mehreren Benutzern verwendet.	USER
Agentenverbindung	Die Zeit, die der Dienst Agenten-Messaging-Protokoll auf dem Gerät mit der Appliance und dem aktuellen Verbindungsstatus verbunden ist (ausschließlich verfügbar für über den Agent verwaltete Geräte). Die Informationen zum Verbindungsstatus umfassen: • : Ein über den Agent verwaltetes Gerät ist mit der Appliance verbunden. • : Ein von Agenten verwaltetes Gerät mit aktivierter Serverüberwachung ist mit der Appliance verbunden. • : Ein über den Agent verwaltetes Gerät ist nicht mit der Appliance verbunden. • : Die Aktivität des Agenten wird auf dem Gerät über die Taskleiste (Windows) oder die Menüleiste (Mac OS) bis zu der angegebenen Uhrzeit und dem angegebenen Datum unterbrochen. • : Ein manuell hinzugefügtes Gerät ist mit der Appliance verbunden. • : Auf einem von einem Agenten verwalteten Gerät wurde ein Problem festgestellt. Weitere Informationen zu Geräteproblemen finden Sie auf der Seite für Geräteprobleme. Weitere	KBSYS.SMMP_CONNECTION

Element	Beschreibung	Datenbankfeld
	Informationen hierzu finden Sie unter Identifizieren von Geräteproblemen.	
Verbindung ohne Agent	Die Zeit, die das Gerät ohne Agent auf dem Gerät mit der Appliance und dem aktuellen Verbindungsstatus verbunden ist (ausschließlich verfügbar für ohne Agent verwaltete Geräte). Die Informationen zum Verbindungsstatus umfassen: • : Die Verwaltung ohne Agent ist für das Gerät aktiviert. • : Für das Gerät sind die Verwaltung ohne Agent und die Serverüberwachung aktiviert. • : Für das Gerät ist die Verwaltung ohne Agent aktiviert, das Gerät ist jedoch derzeit nicht erreichbar.	keine Angabe
Methode für die Verbindung ohne Agent	Das Protokoll (z. B. SNMP), das zum Sammeln der Inventarinformationen vom Gerät verwendet wird	keine Angabe
Letztes Inventar	Der Zeitpunkt des letzten Inventarberichts	LAST_SYNC
Gerät erstellt	Datum und Uhrzeit der Erstellung des ersten Inventardatensatzes für das Gerät.	CREATED (Erstellt)
Gerät geändert	Datum und Uhrzeit der Änderung des Inventardatensatzes für das Gerät.	MODIFIED (Geändert)
Kontakt	**Nur Drucker**. Die Kontaktinformationen des ausgewählten Druckers, zum Beispiel die E-Mail-Adresse. Diese Informationen werden im verwalteten SNMP-Feld `sysContact` des Druckers gespeichert.	

Element	Beschreibung	Datenbankfeld
Standort	**Nur Drucker**. Der Standort des ausgewählten Druckers, zum Beispiel der Name des Unternehmens. Diese Informationen werden im verwalteten SNMP-Feld `sysLocation` des Druckers gespeichert.	
Volume **n**	Der Typ und die Größe des Dateisystems und die Größe des verwendeten Festplattenspeichers. Klicken Sie auf den Link **Nutzungsverlauf anzeigen** in diesem Feld, um die Änderungen in der Datenträgerauslastung anzuzeigen. Diese Information wird aktualisiert, wenn die Auslastung um 5 % oder mehr ansteigt oder abfällt. Für jedes Volume ist ein Eintrag vorhanden. Für VMware® ESXi® Host-Geräte wird jeder Datenspeicher im Zusammenhang mit dem ESXi-Host als Volume aufgeführt.	MACHINE_DISKS
Inventar erzwingen	Klicken Sie auf **Inventar erzwingen**, um die Inventarinformationen für das Gerät sofort zu aktualisieren und das Gerät mit der Appliance zu synchronisieren. Die Option **Inventar erzwingen** ist nur verfügbar, wenn die Verbindung über das Agenten-Messaging-Protokoll zu einem von einem Agenten verwalteten Gerät aktiv ist oder wenn bei Geräten ohne Agenten das Gerät erreichbar ist.	keine Angabe
Aktion auswählen	• Um Agent-Dateien hochzuladen, klicken Sie auf **Aktion auswählen > Agent-Dateien hochladen (Diagnose)**. Wenn Sie fertig sind, werden Links zu hochgeladenen Dateien in der Gruppe *Protokolle und Diagnose* auf dieser Seite angezeigt. • Um das Gerät zur Systemstart-Aktionen	keine Angabe

Element	Beschreibung	Datenbankfeld
	hinzuzufügen, die mit der KACE SDA (Systembereitstellungs-Appliance) erstellt werden, klicken Sie auf **Aktion auswählen** > **Zu SDA-Systemstart-Aktion hinzufügen**. KACE SDA-Systemstart-Aktionen werden verwendet, um Image-Bereitstellungen auf Zielgeräten zu automatisieren. Sie können Systemstart-Aktionen nur auf dem ausgewählten Gerät erstellen, wenn eine verknüpfte KACE SDA vorhanden ist und das Gerät über eine kabelgebundene Netzwerkverbindung verfügt. Dieser Befehl ist auch im Menü **Aktion auswählen** auf der Seite *Geräte* verfügbar. Wenn Sie auf diesen Befehl klicken, wird die Seite *Details zu automatisierter Bereitstellung* der KACE SDA angezeigt. Weitere Informationen zu dieser Seite finden Sie im *Administratorhandbuch* der KACE SDA. • Um das ausgewählte Gerät zu löschen, klicken Sie auf **Aktion auswählen** > **Löschen**.	
VMware UUID	Dieses Feld ist nur sichtbar, wenn Sie Sie ein VMware-Gerät wählen. Die UUID ist ein global eindeutiger Identifier für den vCenter-Server oder den ESXi-Host.	INSTANCE_UUID
Hyper-V UUID	Dieses Feld ist nur sichtbar, wenn Sie ein Hyper-V-Gerät wählen. Die UUID ist eine global eindeutige Kennung für den SCVMM oder den Hyper-V-Server.	INSTANCE_UUID
Virtual Machine Manager verwalten	Der Name des verwaltenden vCenter (VMware-Geräte) oder SCVMM (Hyper-V-Geräte).	keine Angabe

Element	Beschreibung	Datenbankfeld
	Wurde vom KACE Agent bereits ein vCenter oder SCVMM für die Verwaltung bereitgestellt, wird sein Name in der Spalte als Hyperlink angezeigt. Wenn Sie auf den Link klicken, wird die Seite aktualisiert, um Gerätedetails für den bereitgestellten Virtual Machine Manager anzuzeigen.	
Befehle des KACE Cloud Mobile Device Manager (MDM)	Wenn Sie den KACE Cloud MDM integrieren und ein KACE Cloud MDM-Gerät auswählen, stehen in diesem Abschnitt weitere Befehle zur Verfügung. • **Inventar erzwingen**: Anfragen aus dem KACE Cloud MDM zum Start einer neuen Inventarisierung für das Gerät. Nach Abschluss synchronisiert die Appliance die Inventarinformationen. • **Sperren**: Sperrt den Zugriff auf das ausgewählte Gerät. Wenn der Benutzer das nächste Mal mit dem Gerät interagiert, wird er zur Eingabe des Passcode des Geräts aufgefordert. • **Passcode festlegen**: Ermöglicht Ihnen, einen neuen Passcode für das ausgewählte Gerät festzulegen. **HINWEIS:** Dieser Befehl ist nur für Android-Geräte verfügbar. • **Passcode löschen**: Entsperrt das ausgewählte Gerät. Das Gerät bleibt entsperrt, bis ein neuer Passcode bereitgestellt wird. • **Einschränkungen aufheben**: **Nur Android- und iOS-Geräte.** Entfernt alle Einstellungen, die die Funktionalität des	keine Angabe

Element	Beschreibung	Datenbankfeld
	ausgewählten Geräts einschränken. • **Registrierung des Geräts aufheben**: Hebt die Registrierung des ausgewählten Geräts auf dem KACE Cloud MDM auf. • **Auf Werkseinstellungen zurücksetzen**: Stellt die Werkseinstellungen auf dem ausgewählten Gerät wieder her. • **Gerät neustarten**: **Nur Android- (verwaltet), iOS- (überwacht) und Mac OS-Geräte.** Startet das ausgewählte Gerät neu. • **Gerät herunterfahren**: **Nur iOS- (überwacht) und Mac OS-Geräte**. Schaltet das ausgewählte Gerät aus. • **Remotedesktop aktivieren**: **Nur Mac OS-Geräte.** Aktiviert Remotedesktopverbindungen zum ausgewählten Gerät. • **Remotedesktop deaktivieren**: **Nur Mac OS-Geräte.** Deaktiviert Remotedesktopverbindungen zum ausgewählten Gerät. • **Firmwarekennwort festlegen**: **Nur Mac OS-Geräte.** Ermöglicht Ihnen, ein Kennwort für die Firmware des ausgewählten Geräts festzulegen. • **Firmware-Kennwort löschen**: **Nur Mac OS-Geräte.** Löscht das Kennwort für die Firmware des ausgewählten Geräts.	

Element	Beschreibung	Datenbankfeld
	TIPP: Auf diese Befehle kann auch über die Seite *Geräteliste* vom Menü **Aktion wählen** aus zugegriffen werden, wenn Bulk-Aktionen für KACE Cloud Mobile Device Manager (MDM) aktiviert wurden. Diese Option ist standardmäßig deaktiviert. Um sie zu aktivieren, wählen Sie auf der Seite *Allgemeine Einstellungen* unter *Zulässige Bulk-Aktionen* das Kontrollkästchen **Bulk-Aktionen für KACE MDM aktivieren** aus. Weitere Informationen hierzu finden Sie unter Allgemeine Einstellungen auf Verwaltungs- oder organisationsspezifischer Ebene konfigurieren. Der Befehl **Inventar erzwingen** erscheint im Hauptmenü, während andere Befehle im Menü **KACE Cloud MDM** verfügbar sind.	
Befehle für virtuelle VMware-Maschinen	Wenn zu Ihrer verwalteten Umgebung eine oder mehrere bereitgestellte virtuelle VMware-Maschinen gehören, können Sie auf dieser Seite Aktionen für das Gerät einstellen, zum Beispiel das Ein- oder Ausschalten der virtuellen Maschinen. Diese Befehle stehen zur Verfügung, wenn folgende Voraussetzungen erfüllt werden: • Die bereitgestellten virtuellen Maschinen müssen auf einem bereitgestellten VMware ESXi-Server der Version 5.5 oder höher ausgeführt werden.	keine Angabe

Element	Beschreibung	Datenbankfeld
	HINWEIS: Mit Ihrer Produktlizenzvereinbarung kann der Administrator eine festgelegte Anzahl von Computern, Servern und Assets verwalten. Für jeden einzelnen bereitgestellten VMware ESXi-Server ist eine agentenlose Lizenz notwendig. Wenn Sie diese Funktion nutzen möchten, müssen Sie sicherstellen, dass Ihre Produktlizenzvereinbarung alle bereitgestellten ESXi-Hosts abdeckt. Weitere Informationen hierzu finden Sie unter http://quest.com/docs/Product_Guide.pdf. Wenn Sie Ihre Lizenzkapazität erhöhen möchten, besuchen Sie https://quest.com/buy. • VMware Tools müssen auf den virtuellen Zielmaschinen installiert sein, um die Befehle **Gastbetriebssystem schließen** und **Gastbetriebssystem neustarten** auszugeben. Alle anderen Befehle erfordern keine VMware Tools. • Das Benutzerkonto, welches im Inventar konfiguriert ist, muss über ausreichend Berechtigungen auf Administratorebene verfügen, um diese Aktionen durchzuführen. Die folgenden Befehle sind verfügbar, wenn Sie eine bereitgestellte virtuelle VMware-Maschine auswählen. • **Einschalten**: Fährt die ausgewählte virtuelle Maschine hoch. Wenn	

Element	Beschreibung	Datenbankfeld
	die virtuelle Maschine angehalten wird, schaltet diese Aktion die angehaltene virtuelle Maschine ein. • **Ausschalten**: Fährt die ausgewählte virtuelle Maschine runter. Wenn es sich bei der virtuellen Maschine um eine fehlertolerante primäre virtuelle Maschine handelt, werden auch eine oder mehrere sekundäre virtuelle Maschinen ausgeschaltet. • **Anhalten**: Hält die Ausführung der ausgewählten virtuellen Maschine an. • **Zurücksetzen**: Setzt das Einschalten der ausgewählten virtuellen Maschine zurück. Wenn die virtuelle Maschine derzeit eingeschaltet ist, wird diese durch diese Aktion zunächst ausgeschaltet und dann wieder eingeschaltet. • **Gastbetriebssystem herunterfahren**: Gibt einen Befehl an das Gastbetriebssystem auf der ausgewählten virtuellen Maschine aus, um ein sauberes Herunterfahren aller Dienste durchzuführen. • **Gastbetriebssystem neustarten**: Gibt einen Befehl an das Gastbetriebssystem auf der ausgewählten virtuellen Maschine aus, um einen Neustart durchzuführen.	

Element	Beschreibung	Datenbankfeld
	TIPP: Diese Befehle sind stets auf der Seite *Gerätedetails* verfügbar. Sie werden auch auf der Listenseite *Geräte* im Menü **Aktion auswählen** angezeigt, wenn Bulk-Aktionen für Geräte mit virtuellen Maschinen aktiviert sind. Diese Option ist standardmäßig deaktiviert. Um sie zu aktivieren, wählen Sie auf der Seite *Allgemeine Einstellungen* unter *Zulässige Bulk-Aktionen* das Kontrollkästchen **Bulk-Aktionen für virtuelle Maschinen aktivieren** aus. Weitere Informationen hierzu finden Sie unter Allgemeine Einstellungen auf Verwaltungs- oder organisationsspezifischer Ebene konfigurieren. Umfassende Informationen zu diesen Aktionen der virtuellen Maschinen finden Sie in der VMware ESXi-Dokumentation.	
Befehle für virtuelle Hyper-V-Maschinen	Wenn zu Ihrer verwalteten Umgebung eine oder mehrere bereitgestellte virtuelle Hyper-V-Maschinen gehören, können Sie auf dieser Seite eine Reihe von Aktionen für das Gerät einstellen, zum Beispiel das Ein- oder Ausschalten der virtuellen Maschinen. Die folgenden Befehle sind verfügbar, wenn Sie eine bereitgestellte virtuelle Hyper-V-Maschine auswählen. • **Einschalten**: Fährt die ausgewählte virtuelle Maschine hoch. Wenn die virtuelle Maschine angehalten wird, schaltet diese Aktion die angehaltene virtuelle Maschine ein. • **Ausschalten**: Fährt die ausgewählte virtuelle Maschine runter. Wenn es sich bei der virtuellen	keine Angabe

Element	Beschreibung	Datenbankfeld
	Maschine um eine fehlertolerante primäre virtuelle Maschine handelt, werden auch eine oder mehrere sekundäre virtuelle Maschinen ausgeschaltet. • **Anhalten**: Hält die Ausführung der ausgewählten virtuellen Maschine an. • **Fortsetzen**. Setzt die Ausführung einer angehaltenen virtuellen Maschine fort. • **Zurücksetzen**: Setzt das Einschalten der ausgewählten virtuellen Maschine zurück. Wenn die virtuelle Maschine derzeit eingeschaltet ist, wird diese durch diese Aktion zunächst ausgeschaltet und dann wieder eingeschaltet. • **Gastbetriebssystem herunterfahren**: Gibt einen Befehl an das Gastbetriebssystem auf der ausgewählten virtuellen Maschine aus, um ein sauberes Herunterfahren aller Dienste durchzuführen. • **Gastbetriebssystem neustarten**: Gibt einen Befehl an das Gastbetriebssystem auf der ausgewählten virtuellen Maschine aus, um einen Neustart durchzuführen.	

Element	Beschreibung	Datenbankfeld
	TIPP: Diese Befehle sind stets auf der Seite *Gerätedetails* verfügbar. Sie werden auch auf der Listenseite *Geräte* im Menü **Aktion auswählen** angezeigt, wenn Bulk-Aktionen für Geräte mit virtuellen Maschinen aktiviert sind. Diese Option ist standardmäßig deaktiviert. Um sie zu aktivieren, wählen Sie auf der Seite *Allgemeine Einstellungen* unter *Zulässige Bulk-Aktionen* das Kontrollkästchen **Bulk-Aktionen für virtuelle Maschinen aktivieren** aus. Weitere Informationen hierzu finden Sie unter Allgemeine Einstellungen auf Verwaltungs- oder organisationsspezifischer Ebene konfigurieren. Umfassende Informationen zu diesen Aktionen der virtuellen Maschinen finden Sie in der Hyper-V-Dokumentation.	
Befehle für Chrome-Geräte	Wenn Ihre verwaltete Umgebung bereitgestellte Chrome-Geräte enthält und Sie ein Chrom-Geräts auswählen, sind die folgenden Befehle verfügbar: • **Verschieben**: Verschiebt ein bereitgestelltes Gerät in eine andere Organisationseinheit. • **Deaktivieren**: Deaktiviert ein bereitgestelltes Gerät. Sie können diesen Befehl verwenden, wenn ein Gerät verloren gegangen ist oder gestohlen wurde. • **Reaktivieren**: Aktiviert ein zuvor deaktiviertes Gerät. • **Bereitstellung aufheben**: Entfernt alle Bereitstellungsrichtlinien vom Gerät. Normalerweise führen Sie diesen Schritt für Geräte aus, die nicht mehr in Ihrer Organisation	

Element	Beschreibung	Datenbankfeld
	verwendet und daher nicht mehr verwaltet werden müssen. **TIPP:** Diese Befehle sind stets auf der Seite *Gerätedetails* verfügbar. Sie werden auch auf der Listenseite *Geräte* im Menü **Aktion auswählen** angezeigt, wenn Bulk-Aktionen für Geräte mit virtuellen Maschinen aktiviert sind. Diese Option ist standardmäßig deaktiviert. Um sie zu aktivieren, wählen Sie auf der Seite *Allgemeine Einstellungen* unter *Zulässige Bulk-Aktionen* das Kontrollkästchen **Bulk-Aktionen für Chrome OS aktivieren** aus. Weitere Informationen hierzu finden Sie unter Allgemeine Einstellungen auf Verwaltungs- oder organisationsspezifischer Ebene konfigurieren. Umfassende Informationen zu diesen Aktionen für Chrome-Geräte finden Sie in der Google-Dokumentation.	

Gruppe „Inventarinformationen“

Weitere Details zu Elementen im Abschnitt *Übersicht*.

Abschnitt oder Element	Beschreibung	Datenbankfeld
Hardware	Informationen über die Hardware des Geräts. Wenn der Änderungsverlauf für diesen Abschnitt aktiviert ist und sich die Informationen in diesem Abschnitt geändert haben, wird der Link **Änderungen anzeigen** neben der Überschrift eingeblendet. Klicken Sie auf **Änderungen anzeigen**, um nur die geänderten Elemente anzuzeigen. Klicken Sie auf **Änderungen ausblenden**, um alle Elemente anzuzeigen.	

Abschnitt oder Element	Beschreibung	Datenbankfeld
RAM gesamt	Der insgesamt installierte Arbeitsspeicher (Random Access Memory, RAM) des Geräts.	RAM_TOTAL
Genutzter RAM	Die Größe des verwendeten RAM (Random Access Memory) auf dem Gerät	RAM_USED
Maximaler RAM	Die maximal vom Gerät unterstützte Menge an Arbeitsspeicher (Random Access Memory, RAM).	RAM_MAX
Systemhersteller	Der Hersteller des Geräts	CS_MANUFACTURER
Systemmodell	Das Modell des Geräts	CS_MODEL
CSP-ID	Die Seriennummer des Systems.	CSP_ID_NUMBER
Asset-Tag	**Nur Windows- Chrome- und KACE MDM-Geräte**. Das BIOS-Asset-Tag eines Systems. Administratoren können diesen Wert mithilfe eines BIOS-Dienstprogramms für das System festlegen.	ASSET_TAG
Domain	Die Windows Domäne, der das Gerät angehört.	CS_DOMAIN
Primärer Bus der Hauptplatine	Der Systembus	MOTHERBOARD_PRIMARY_BUS
Sekundärer Bus der Hauptplatine	Der Peripheriebus	MOTHERBOARD_SECONDARY_BUS
Prozessoren	Die Anzahl, der Typ und der Hersteller der CPUs	PROCESSORS
Architektur	Die Architektur des Gerätebetriebssystems (beispielsweise x86 oder x64).	SYS_ARCH
Virtuelles Gerät	Identifiziert virtuelle Geräte, z.B. Geräte auf VMware Plattformen. Wird nicht für physische Geräte wie Notebooks und Server angezeigt.	VIRTUELL
Trusted Platform Module (TPM)	Auf Geräten, auf denen der TPM dedizierte Mikroprozessor installiert ist, werden technische Daten sowie Informationen dazu angezeigt, ob TPM eingeschaltet und aktiviert ist.	MACHINE_TPM

Abschnitt oder Element	Beschreibung	Datenbankfeld
	Siehe Informationen zu Dell Data Protection | Encryption (DDP|E) und Verschlüsselungsinformationen in Gerätedetails.	
Intel AMT-Gerät	Auf Intel basierten Windows-Geräten mit vorhandener Intel AMT Technologie werden Informationen zur Konfiguration angezeigt. Siehe Informationen zu Intel AMT in Gerätedetails.	INTEL_AMT
CD/DVD-Laufwerke	Die Konfiguration der auf dem Gerät installierten CD-ROM- und DVD-ROM-Laufwerke	CDROM_DEVICES
Audiogeräte	Informationen über Audiogeräte auf dem Gerät	SOUND_DEVICES
Videocontroller	Informationen über Videocontroller auf dem Gerät	VIDEO_CONTROLLERS
Monitore	Typ und Hersteller des an das Gerät angeschlossenen Monitors Für virtuelle Geräte werden Überwachungsinformationen angezeigt, sofern sie vom Betriebssystem gemeldet werden.	MONITOR
Apple-Supportinformationen	Link zur Support-Seite von Apple	keine Angabe
SMC-Version	Die Version des System-Managementcontrollers der Geräte-CPU	BIOS_NAME
Seriennummer	Die Seriennummer des Geräts	BIOS_SERIAL_NUMBER
Start-ROM-Version	Die Start-ROM- oder Firmwareversion des Geräts	BIOS_VERSION
Dell Serviceinformationen	Informationen über Dell Hardware, einschließlich Service-Tag, Systemtyp, Versanddatum, Land und Serviceinformationen. Dieser Abschnitt beinhaltet auch die Spalte *Verbleibende Tage*, die die Anzahl der noch im Garantiezeitraum verbleibenden Tage angibt, sowie die Spalte *Zuletzt aktualisiert*, die angibt, wann die Serviceinformationen das letzte Mal aktualisiert wurden.	DELL_WARRANTY

Abschnitt oder Element	Beschreibung	Datenbankfeld
	Um die Dell Service Informationen zu aktualisieren, klicken Sie auf **Aktualisieren**.	
BIOS-Name	Der BIOS-Name	BIOS_NAME
BIOS-Version	Die BIOS-Version	BIOS_VERSION
BIOS-Herausgabedatum	Das Datum der Herausgabe der BIOS-Version	BIOS_DATUM
BIOS-Hersteller	Der BIOS-Hersteller	BIOS_MANUFACTURER
BIOS-Beschreibung	Die BIOS-Beschreibung	BIOS_Beschreibung
BIOS-Seriennummer	Die BIOS-Seriennummer	BIOS_SERIAL_NUMBER
Schwarzer Toner – Beschreibung	**Nur Drucker**. Hersteller und Modell des schwarzen Toners.	
Schwarzer Toner – Max. Füllstand	**Nur Drucker**. Max. Füllstand des schwarzen Toner-Pulvers.	
Schwarzer Toner – Aktueller Füllstand	**Nur Drucker**. Aktueller Füllstand des schwarzen Toner-Pulvers. Wenn der Toner nicht installiert ist, wird in diesem Feld eine Meldung angezeigt.	
Cyan-Toner – Beschreibung	**Nur Farbdrucker**. Hersteller und Modell des Cyan-Toners.	
Cyan-Toner – Max. Füllstand	**Nur Farbdrucker**. Max. Füllstand des Cyan-Toner-Pulvers.	
Cyan-Toner – Aktueller Füllstand	**Nur Farbdrucker**. Aktueller Füllstand des Cyan-Toner-Pulvers. Wenn der Toner nicht installiert ist, wird in diesem Feld eine Meldung angezeigt.	
Magenta-Toner – Beschreibung	**Nur Farbdrucker**. Hersteller und Modell des Magenta-Toners.	
Magenta-Toner – Max. Füllstand	**Nur Farbdrucker**. Max. Füllstand des Magenta-Toner-Pulvers.	
Magenta-Toner – Aktueller Füllstand	**Nur Farbdrucker**. Aktueller Füllstand des Magenta-Toner-Pulvers. Wenn der Toner nicht installiert ist, wird in diesem Feld eine Meldung angezeigt.	

Abschnitt oder Element	Beschreibung	Datenbankfeld
Gelber Toner – Beschreibung	**Nur Farbdrucker**. Hersteller und Modell des gelben Toners.	
Gelber Toner – Max. Füllstand	**Nur Farbdrucker**. Max. Füllstand des gelben Toner-Pulvers.	
Gelber Toner – Aktueller Füllstand	**Nur Farbdrucker**. Aktueller Füllstand des gelben Toner-Pulvers. Wenn der Toner nicht installiert ist, wird in diesem Feld eine Meldung angezeigt.	
Volume **n**	Der Typ und die Größe des Dateisystems und die Größe des verwendeten Festplattenspeichers. Klicken Sie auf den Link **Nutzungsverlauf anzeigen** in diesem Feld, um die Änderungen in der Datenträgerauslastung anzuzeigen. Diese Information wird aktualisiert, wenn die Auslastung um 5 % ansteigt oder abfällt. Für jedes Volume ist ein Eintrag vorhanden.	MACHINE_DISKS
Hewlett-Packard – Service-Informationen	**Nur Geräte von Hewlett-Packard**. Informationen über das ausgewählte Gerät von Hewlett-Packard (HP). Dieser Bereich wird angezeigt, wenn Sie die API-Schlüssel des Herstellers auf der Seite *Allgemeine Einstellungen* eingeben. Weitere Informationen hierzu finden Sie unter Allgemeine Appliance-Einstellungen bei aktivierter Organisationskomponente konfigurieren.	
	Seriennummer: Die Seriennummer des ausgewählten Geräts von HP	SERIAL
	Produktnummer: Die spezifische Nummer des ausgewählten Geräts von HP.	Teilenr.
	Produktname: Der Name des ausgewählten Geräts von HP.	PRODUCT
	Zuletzt aktualisiert: Der Zeitstempel der letzten	

Abschnitt oder Element	Beschreibung	Datenbankfeld
	Aktualisierung von Geräteinformationen.	
	Servicestatustyp: Der Servicetyp des ausgewählten Geräts: • W: Garantie • P: Festes Care Pack, vergleichbar mit erweitertem Service • C: Ein Vertrag, vergleichbar mit erweitertem Service	SERVICE_TYPE
	Typ: Die Beschreibung des Servicestatustyps. Zum Beispiel *Service* oder anderes.	TYP
	Startdatum: Startdatum des erweiterten Services.	START_DATE
	Enddatum Enddatum des Services.	END_DATE
	Servicelevel: Eine durch Kommas getrennte Liste der Service-Codes für das Gerät.	SERVICE_LEVEL
Lenovo Serviceinformationen	**Nur Geräte von Lenovo**. Informationen über das ausgewählte Gerät von Lenovo. Dieser Bereich wird angezeigt, wenn Sie die API-Schlüssel des Herstellers auf der Seite *Allgemeine Einstellungen* eingeben. Weitere Informationen hierzu finden Sie unter Allgemeine Appliance-Einstellungen bei aktivierter Organisationskomponente konfigurieren.	
	Produkt: der Name des ausgewählten Geräts von Lenovo.	PRODUCT
	Gekauft: Das Datum, an dem das ausgewählte Gerät von Lenovo gekauft wurde.	PURCHASED
	Versand: Das Datum, an dem das ausgewählte Gerät von Lenovo ausgeliefert wurde.	SHIPPED
	Garantie: Zeigt an, ob das ausgewählte Gerät von Lenovo	IN_WARRANTY

Abschnitt oder Element	Beschreibung	Datenbankfeld
	vom Service abgedeckt wird (*Ja* oder *Nein*).	
	Land: Das Land, in dem der ausgewählte Drucker von Lenovo gekauft wurde.	COUNTRY
	Upgrade-URL: Die URL, die die Aktualisierungsangaben enthält.	UPGRADE_URL
	Zuletzt aktualisiert: Der Zeitstempel der letzten Aktualisierung von Geräteinformationen.	
	ID: Service-ID.	ID
	Typ: Servicetyp: *UNBEKANNT*, *BASIS*, *UPGRADE*, *ERWEITERT* oder *SOFORT*.	TYP
	Startdatum: Startdatum des erweiterten Services.	START_DATE
	Enddatum Enddatum des Services.	END_DATE
	Name: Der Service-Name.	
	Beschreibung: Die Servicebeschreibung, sofern anwendbar.	DESCRIPTION (Beschreibung)
Drucker	Die Drucker, für deren Verwendung das Gerät konfiguriert ist.	PRINTERS (Drucker)
Netzwerkschnittstellen	Der Typ der Netzwerkschnittstelle, wie z. B. Ethernet-Karte oder Bluetooth-Adapter, und Details wie IP-Adresse und ob DHCP (Dynamic Host Configuration Protocol) für das zugehörige IPv4 (Internet Protocol Version 4) aktiviert oder deaktiviert ist.	MACHINE_NICS
SNMP-Daten	Die Ergebnisse eines SNMP Full Walk der Daten in der MIB (Management Information Base) eines Geräts, sofern Sie den Geräteerkennungstyp *Authentifiziert* so konfiguriert haben, dass ein Full Walk durchgeführt wird. Dieser	

Abschnitt oder Element	Beschreibung	Datenbankfeld
	Abschnitt wird nicht angezeigt, wenn die Erkennung mit einem „Bulk GET“-Vorgang durchgeführt wurde.	
MAC-Adresse	Die Drahtlos-MAC-Adresse des Geräts.	MAC_ADDRESS
DHCP	Ein Indikator, ob DHCP für die IPv4-Adresse aktiviert ist, die mit dieser Netzwerkschnittstelle verknüpft ist.	
IPv6-Hostkonfiguration	Eine Liste mit einer oder mehreren IPv6-Adressen (Internet Protocol Version 6), die in der Netzwerkschnittstelle zur Verfügung stehen. Für jedes aufgeführte Element wird in diesem Abschnitt die vollständige IPv6-Adresse und die Anzahl der Bits in der Länge des IPv6-Adressenpräfix angezeigt. Ein IPv6-Präfix besteht üblicherweise aus 64 Bits.	
DNS-Hostname	Der mit dieser Netzwerkschnittstelle verknüpfte Hostname.	
WLAN	**Nur KACE MDM-Geräte**. Die IP- oder MAC-Adresse des Geräts.	
Chrome-Betriebssystem	Chrome-bezogene Informationen. **HINWEIS:** Chrome-Werte befinden sich nicht in der Tabelle „MACHINE“, sondern in der Tabelle „MACHINE_CHROMEOS_DETAIL“.	keine Angabe
Verzeichnis-API-ID	Die eindeutige ID des Chrome-Geräts.	DEVICE_ID
Status	Der Status des Chrome-Geräts: ACTIVE, DEPROVISIONED, INACTIVE, RETURN_APPROVED, RETURN_REQUESTED, SHIPPED, UNKNOWN.	STATUS
Enddatum des Supports	Das Datum, an dem der Support für das Gerät endet. Gilt nur für direkt von Google erworbene Geräte.	SUPPORT_END_DATE

Abschnitt oder Element	Beschreibung	Datenbankfeld
Benutzerdefinierter Benutzer	Der Benutzer des Geräts gemäß Administratorangabe.	ANNOTATED_USER
Benutzerdefinierter Speicherort	Die Adresse oder der Ort des Geräts gemäß Administratorangabe.	ANNOTATED_LOCATION
Bestellnummer	Die Bestellnummer des Geräts. Nur direkt von Google erworbene Geräte besitzen eine Bestellnummer.	ORDER_NUMBER
Chrome-Version	Die Betriebssystemversion des Chrome-Geräts.	OS_VERSION
Plattformversion	Die Plattformversion des Chrome-Geräts.	PLATFORM_VERSION
Firmwareversion	Die Firmwareversion des Chrome-Geräts.	FIRMWARE_VERSION
Neustartmodus	Der Startmodus für das Gerät.	BOOT_MODE
Organisationseinheit	Der vollständige übergeordnete Pfad mit dem Namen der Google-Organisationseinheit, der dem Gerät zugeordnet ist.	ORG_UNIT_PATH
Ablauf der automatischen Aktualisierung	Das Datum und die Uhrzeit, bis zu dem das Gerät automatische Aktualisierungen erhält.	AUTO_UPDATE_EXPIRATION
Mobilinformationen	Informationen von Geräten, die über KACE Mobile Device Manager (KMDM) und Workspace ONE® verwaltet werden.	keine Angabe
UDID	Der eindeutige Bezeichner des Geräts. Nur für iOS Geräte.	UDID
Modem-Firmware	Die Firmwareversion des mobilen Geräts.	FIRMWARE_VERSION
Gerätetyp	**Nur DMM-Geräte**. Der Typ des mobilen Geräts. Beispiel: iPhone, iPad, iPod sowie Android Smartphone und Tablet.	DEVICE_TYPE
ICCID	**Nur KACE MDM- und DMM-Geräte**. Die eindeutige Seriennummer für die SIM-Karte des Geräts.	ICCID

Abschnitt oder Element	Beschreibung	Datenbankfeld
IMEI	**Nur KACE MDM- und DMM-Geräte**. Die internationale Kennung für mobile Geräte (International Mobile Equipment Identity, IMEI) des Geräts.	IMEI
Sprachroaming aktiviert	**Nur KACE MDM Android-Telefone**. Ein Hinweis darauf, ob beim ausgewählten KACE MDM Android-Telefon Sprachroaming aktiviert ist.	SPRACHROAMING AKTIVIERT
Datenroaming aktiviert	**Nur KACE MDM Android-Telefone**. Ein Hinweis darauf, ob beim ausgewählten KACE MDM Android-Telefon Datenroaming aktiviert ist.	DATA_ROAMING_ENABLED
MEID	**Nur KACE MDM-Geräte**. Die ID mobiler Geräte. Dies ist die eindeutige ID des ausgewählten mobilen Geräts.	MEID
Telefonnummer	**Nur DMM-Geräte**. Dem Gerät zugeordnete Telefonnummer.	PHONE_NUMBER
Mobilfunkanbieter	**Nur KACE MDM- und DMM-Geräte**. Der Mobilfunkanbieter.	CARRIER
Bluetooth MAC-Adresse	**Nur DMM-Geräte**. MAC-Adresse (Media Access Control, Medienzugriffssteuerung) für Bluetooth auf dem Gerät.	BLUETOOTH_MAC
Akkustand	**Nur KACE MDM- und DMM-Geräte**. Akkustand bei letzter Aktualisierung in Prozent.	BATTERY_LEVEL
Letzter Check-in	Der Zeitstempel der letzten Aktualisierung von Geräteinformationen.	LAST_CHECK_IN
Zeitpunkt der letzten Registrierung	Datum und Uhrzeit der letzten Registrierung des Geräts mit der Google-Administratorkonsole.	LAST_ENROLLMENT_TIME
Angemeldet	**Nur KACE MDM- und Workspace ONE-Geräte**. Datum und Uhrzeit der letzten Registrierung des Geräts bei KACE MDM oder der Workspace ONE-Konsole.	IS_ENROLLED

Abschnitt oder Element	Beschreibung	Datenbankfeld
Beaufsichtigt	**Nur KACE MDM iOS-Geräte**. Ein Hinweis darauf, ob das ausgewählte KACE MDM iOS-Gerät beaufsichtigt ist. Dies ist die höchste Kontrollstufe auf einem iOS-Gerät.	IS_SUPERVISED
Verloren-Modus	**Nur beaufsichtigte KACE MDM- und AirWatch-Geräte**. Ein Hinweis darauf, ob sich das ausgewählte KACE MDM iOS-Gerät im Verloren-Modus befindet. Der Verloren-Modus schützt ein Gerät davor, von einer dritten Person entsperrt zu werden.	IS_LOST
Verschlüsselt	**Nur KACE MDM-Geräte**. Ein Hinweis darauf, ob sich das ausgewählte KACE MDM iOS-Gerät im verschlüsselten Modus befindet.	IS_ENCRYPTED
Locator-Dienst aktiviert	**Nur KACE MDM iOS-Geräte**. Ein Hinweis darauf, ob beim ausgewählten KACE MDM iOS-Gerät der Locator-Dienst aktiviert ist. Dieser Service ruft die Gerätestandort-Informationen ab, sofern das Gerät reagiert.	LOCATOR_SERVICE_ENABLED
Aktivierungssperre aktiviert	**Nur KACE MDM iOS-Geräte**. Ein Hinweis darauf, ob die Aktivierungssperre auf dem ausgewählten KACE MDM iOS-Gerät aktiviert ist. Diese Funktion verhindert, dass ein verloren gegangenes oder gestohlenes iOS-Gerät von einer anderen Person benutzt wird.	ACTIVATION_LOCK_ENABLED
Gerootet	**Nur KACE MDM Android-Geräte**. Ein Hinweis darauf, ob das ausgewählte KACE MDM Android-Gerät entsperrt ist.	IS_ROOTED
Kompatibel	**Nur Workspace ONE-Geräte**. Gibt an, ob das Gerät die vorkonfigurierten Workspace ONE Compliance-Regeln erfüllt.	IS_COMPLIANT
Aktuelles Mobilnetzwerk	**Nur Workspace ONE-Geräte**. Der Name des mobilen Netzwerks, das mit dem	keine Angabe

Abschnitt oder Element	Beschreibung	Datenbankfeld
	Workspace ONE-Gerät verknüpft ist.	
Umgehungscode für Aktivierungssperre	**Nur DEP-verwaltete KACE MDM iOS-Geräte**. Der Umgehungscode, der als Gerätekennwort verwendet werden kann, wenn die Aktivierungssperre aktiviert ist.	ACTIVATION_LOCK_BYPASS_CODE
Überwachte Aktivierungssperre zulassen	**Nur DEP-verwaltete KACE MDM iOS-Geräte**. Zeigt an, ob die Aktivierungssperre für das Gerät aktiviert ist. Mit der Aktivierungssperre können Benutzer das Kennwort umgehen und sich mit dem Code zur Umgehung der Aktivierungssperre am Gerät anmelden.	ACTIVATION_LOCK_ALLOWED
DEP-verwaltet	**Nur KACE MDM iOS-Geräte**. Gibt an, ob das Gerät vom Apple Device Enrollment Program (DEP) verwaltet wird.	IS_DEP_MANAGED
DEP-Profil	**Nur DEP-verwaltete KACE MDM iOS-Geräte**. Der Namen des DEP-Profils, das dem Asset zugeordnet ist.	DEP_PROFIL
DEP-Profil zugewiesen von	**Nur DEP-verwaltete KACE MDM iOS-Geräte**. Der Name des Benutzerkontos, das dem Gerät das DEP-Profil zugewiesen hat.	DEP_ASSIGNED_BY
Zuweisungsdatum des DEP-Profils	**Nur DEP-verwaltete KACE MDM iOS-Geräte**. Das Datum, an dem das DEP-Profil dem Gerät zugewiesen wird.	DEP_ASSIGNED_DATE
DEP-Profilstatus	**Nur DEP-verwaltete KACE MDM iOS-Geräte**. Der Verwaltungsstatus des Geräts: • **Zugewiesen**: Apple DEP hat ein Profil erhalten	DEP_PROFILE_STATUS

Abschnitt oder Element	Beschreibung	Datenbankfeld
	und kann dem Gerät zugewiesen werden. • **Leer**: Das Profil ist dem Gerät nicht zugewiesen. • **Gedrückt**: Ein Profil wird an das aktivierte Gerät gesendet. • **Entfernt**: Dem Gerät wurde ein Profil zugewiesen, aber es wurde entfernt. Wenn das Gerät wieder aktiviert wird, verwaltet KACE MDM das Gerät nicht mehr.	
Gerät konfiguriert	**Nur DEP-verwaltete KACE MDM iOS-Geräte**.	IS_DEP_CONFIGURED
Nicht stören	Zeigt an, ob sich das Gerät im Modus „Nicht stören“ befindet.	DO_NOT_DISTURB_ENABLED
Exchange-Geräte-ID	Die dem Gerät zugewiesene Microsoft Exchange-ID.	EAS_DEVICE_ID
Erste Registrierung	Das Datum, an dem das Gerät bei KACE MDM registriert wurde.	ENROLLMENT_DATE
iCloud-fähig	**Nur KACE MDM iOS-Geräte**. Gibt an, ob die Cloud auf den Geräten aktiviert ist.	ICLOUD_ENABLED
Letztes iCloud-Backup	**Nur KACE MDM iOS-Geräte**. Das Datum, an dem Apple iCloud zuletzt auf dem Gerät gesichert wurde.	ICLOUD_LAST_BACKUP
Bei iTunes angemeldet	**Nur KACE MDM iOS-Geräte**. Gibt an, ob das Gerät bei iCloud angemeldet ist.	IS_ITUNES_ACCOUNT_ACTIVE
WLAN empfangen	**Nur KACE MDM Android-Geräte**. Die Anzahl der Bytes, die das Gerät über ein WLAN-Netzwerk empfangen hat.	WIFI_BYTES_RECV
WLAN gesendet	**Nur KACE MDM Android-Geräte**. Die Anzahl der Bytes, die das Gerät über ein WLAN-Netzwerk gesendet hat.	WIFI_BYTES_SENT
WWAN empfangen	**Nur KACE MDM Android-Geräte**. Die Anzahl der Bytes, die	WWAN_BYTES_RECV

Abschnitt oder Element	Beschreibung	Datenbankfeld
	das Gerät über ein Mobilfunknetz empfangen hat.	
WWAN gesendet	**Nur KACE MDM Android-Geräte**. Die Anzahl der Bytes, die das Gerät über ein Mobilfunknetz gesendet hat.	WWAN_BYTES_SENT
Agent	Agentenbezogene Informationen.	keine Angabe
Version des Agenten	Die Versionsnummer des auf dem Gerät installierten KACE Agent.	CLIENT_VERSION
Verbunden	Der Zeitpunkt, zu dem sich der AMP-Dienst (Agenten-Messaging-Protokoll) auf dem Gerät mit der Appliance verbunden hat.	CONNECT_TIME
Nicht verbunden	Bei getrennter Verbindung der Zeitpunkt, zu dem der AMP-Dienst (Agenten-Messaging-Protokoll) auf dem Gerät die Verbindung mit der Appliance getrennt hat.	DISCONNECT_TIME
KACE ID	Die Zeichenfolge, die zum Identifizieren des Geräts in der Datenbank der Appliance verwendet wird.	KUID
Datenbank-ID	Die eindeutige Nummer, die zum Identifizieren des Geräts in der Datenbank der Appliance verwendet wird.	ID
Manuelle Eingabe	Dieses Feld gibt an, ob die Inventarinformationen manuell über die WSAPI hinzugefügt oder manuell per XML hochgeladen wurden.	MANUAL_ENTRY
Geräteeintragstyp	Dieses Feld gibt Aufschluss über die Verwaltung des Geräts: *Gerät mit Agent*, *Gerät ohne Agent* oder *Manuell eingegebener Datensatz*. Klicken Sie auf **Bearbeiten**, um Verbindungsprotokolle zu ändern.	keine Angabe
Letztes Inventar	Der Zeitpunkt des letzten Inventarberichts	LAST_INVENTORY
Letzte Synchronisierung	Für über den Agenten verwaltete Geräte der Zeitpunkt, zu dem sich das Gerät zuletzt bei der Appliance angemeldet hat. Für	LAST_SYNC

Abschnitt oder Element	Beschreibung	Datenbankfeld
	Geräte ohne Agent der Zeitpunkt, zu dem die Appliance zuletzt mit dem Gerät und dem gesammelten Inventar verbunden war.	
Letzte Agenten-Aktualisierung	Der Zeitpunkt der letzten Aktualisierung des KACE Agent (sofern zutreffend).	LAST_CLIENT_UPDATE
Konductor-Aufgaben	Status von Aufgaben, die gerade auf vom Agenten verwalteten Geräten ausgeführt werden oder deren Ausführung auf diesen Geräten geplant ist. In diesem Abschnitt werden die folgenden Informationen zu den einzelnen Aufgaben angezeigt: • **Aufgabentyp**: Aufgabentyp. Abhängig von der Konfiguration der Appliance gibt es folgende Aufgabentypen: Benachrichtigungen, Inventar, kbot, Absturz-Upload und Skriptaktualisierungen. • **Startzeit**: Die Startzeit der Aufgabe. • **Abgeschlossen**: Die Abschlusszeit der Aufgabe. • **Nächste geplante Ausführung**: Die Zeit der nächsten geplanten Ausführung der Aufgabe. • **Timeout**: Die Frist zum Abschluss der Aufgabe. • **Priorität**: Die Wichtigkeit oder der Rang der Aufgabe. Diese Informationen werden auch auf der Listenseite *Agenten-Tasks* angezeigt. Weitere Informationen hierzu finden Sie unter Status von Agenten-Aufgaben anzeigen.	keine Angabe
Quarantäne	Informationen zur KACE Agent-Authentifizierung.	keine Angabe
Quarantine Record (Quarantäne-Datensatz)	Ein Link zu den Quarantänedetails für diesen Agenten. Weitere Informationen hierzu finden Sie unter Registrieren des KACE Agent bei der Appliance.	KUID

Abschnitt oder Element	Beschreibung	Datenbankfeld
Approved Time (Zeitpunkt der Genehmigung)	Datum und Uhrzeit der Authentifizierung des KACE Agent durch die Appliance.	APPROVED_TIME
Token Used (Verwendetes Token)	Wenn der KACE Agent zur Registrierung bei der Appliance ein Token verwendet hat, enthält dieses Feld den Token-Namen und einen Link zu den Token-Details.	TOKEN_ID
Genehmigt von	Wenn der KACE Agent nach der Zugriffsgewährung durch den Appliance-Administrator eine Verbindung zur Appliance hergestellt hat, enthält dieses Feld den Namen des Administrators, der die Verbindung des Agenten genehmigt hat.	APPROVED_BY
Benutzer	Informationen zum Benutzer des Geräts.	keine Angabe
Benutzer angemeldet	Der Benutzer, der derzeit bei dem Gerät angemeldet ist Dieser Eintrag umfasst den Namen des Benutzers sowie die Domäne, zu der der Benutzer gehört.	USER_LOGGED
Vollständiger Benutzername	Der vollständige Name des Benutzers, der das Gerät besitzt.	USER_FULLNAME
Benutzername	Der Name des aktuellen Benutzers	USER_NAME
Benutzerdomäne	Die Domäne, zu der der Benutzer gehört	USER_DOMAIN
Betriebssystem	Informationen zum Betriebssystem des Geräts.	keine Angabe
Name	Das Betriebssystem des Geräts, z.B. Windows, Mac OS X oder Linux	OS_NAME
Service Pack	Die Versionsnummer des Service Packs (nur Windows oder SUSE Linux Enterprise Server).	SERVICE_PACK
Betriebssystemversion	Die Versionsnummer des Betriebssystems	OS_VERSION

Abschnitt oder Element	Beschreibung	Datenbankfeld
Betriebssystem-Buildversion	Die Build-Nummer des Betriebssystems	OS_BUILD
Nummer	Die Nummer des Betriebssystems	OS_NUMBER
Betriebssystemarchitektur	Die Architektur des Gerätebetriebssystems (beispielsweise x86 oder x64).	OS_ARCH
Domain	Die Windows Domäne, der das Gerät angehört.	CS_DOMAIN
Datum der Betriebssysteminstallation	Das Datum der Installation des Betriebssystems	OS_INSTALLED_DATE
Letzter Start	Die Dauer der Ausführung des Betriebssystems	LAST_REBOOT
Betriebszeit seit letztem Neustart	Die Zeit, die das Gerät seit dem letzten Neustart in Betrieb ist	UPTIME
Systemverzeichnis	Der Speicherort des Systemverzeichnisses	SYSTEM_DIRECTORY
Registrierungsgröße	Die Größe der Registrierung	REGISTRY_SIZE
Maximale Registrierungsgröße	Die maximale Größe der Registrierung	REGISTRY_MAX_SIZE
Größe der Auslagerungsdatei	Die aktuelle Größe der Windows Auslagerungsdatei	PAGEFILE_SIZE
Max. Größe der Auslagerungsdatei	Die maximale Größe der Windows Auslagerungsdatei	PAGEFILE_MAX_SIZE
IE-Version	Die auf dem Gerät installierte Version des Internet Explorer	IE_VERSION
Edge-Version	Die auf dem Gerät installierte Version von Microsoft Edge.	EDGE_VERSION
WMI-Status	Der Status des Windows Verwaltungsinstrumentationsdienstes (WMI) (nur Windows Geräte).	WMI_STATUS
Datenträgerverschlüsselung	Informationen zur Verschlüsselung, sofern ein DDP|E Client sowie BitLocker oder FileVault 2 auf dem Gerät installiert wurde. Siehe Informationen zu Dell Data Protection |	

Abschnitt oder Element	Beschreibung	Datenbankfeld
	Encryption (DDP|E) und Verschlüsselungsinformationen in Gerätedetails.	
Zusammenfassung der Datenträgerverschlüsselung	Identifiziert die verwendete Verschlüsselungstechnologie und gibt an, ob die Verschlüsselung aktiviert ist.	keine Angabe
Dell Data Protection | Encryption (DDP|E)	Konfigurations- und Statusinformationen zu DDP|E.	keine Angabe
BitLocker	Konfigurations- und Statusinformationen zu Windows BitLocker.	keine Angabe
FileVault	Konfigurations- und Statusinformationen zu Mac OS X FileVault 2.	keine Angabe
Standort	Informationen von Geräten, die über Workspace ONE oder KACE MDM Cloud verwaltet werden.	
Adresse	Die Anschrift, an dem sich das Zielgerät befindet.	STREET_ADDRESS
Stadt	Die Stadt, in der sich das ausgewählte Gerät befindet.	LOCALITY
Bundesland/Provinz	Das Bundesland oder die Provinz, in dem sich das ausgewählte Gerät befindet.	REGION
Land	Das Land, in dem sich das Gerät befindet.	COUNTRY
Breitengrad	Der Breitengrad des Geräts der bei der letzten Aktualisierung erkannt wurde.	LATITUDE
Längengrad	Der Längengrad des Geräts des Geräts der bei der letzten Aktualisierung erkannt wurde.	LONGITUDE
Letzte Aktualisierung	Der Zeitstempel der letzten Aktualisierung von Geräteinformationen.	LAST_UPDATE
Anmerkungen	Geben Sie nach Bedarf beliebige weitere Informationen ein.	HINWEISE

Abschnitt oder Element	Beschreibung	Datenbankfeld
Virtuelle Maschinen	Wenn ein ESXi-Host oder ein Hyper-V-Server ausgewählt ist, listet diese Gruppe die virtuellen Maschinen auf, die dem ausgewählten Gerät zugeordnet sind. Einige Informationen in dieser Liste sind nur verfügbar, wenn VMware-Tools//Microsoft Integration-Services auf den virtuellen Maschinen installiert sind. Wenn einige Spalten nicht ausgefüllt sind, kann dies auf fehlende VMware-Tools oder Microsoft Integration-Services zurückzuführen sein.	
Name	Der Name des virtuellen Computers.	NAME
Hostname	Der Host-Name des virtuellen Computers. Wurde vom KACE Agent bereits ein virtueller Computer bereitgestellt, wird sein Name in der Spalte als Hyperlink angezeigt. Wenn Sie auf den Link klicken, wird die Seite aktualisiert, um Gerätedetails für den bereitgestellten virtuellen Computer anzuzeigen.	HOSTNAME
IP-Adresse	Die primäre IP-Adresse wurde dem virtuellen Computer zugewiesen.	IP

Abschnitt oder Element	Beschreibung	Datenbankfeld
Zustand	Gibt an, ob der virtuelle Computer ausgeführt wird. Mögliche Werte: • **0 - Running**: Virtueller Computer wird normal ausgeführt. • **1 - Shutting down**: Für virtuellen Computer steht shutdown-Befehl aus. • **2 – Resetting**: Für virtuellen Computer steht reset-Befehl aus. • **3 – Pending standby**: Für virtuellen Computer steht standby-Befehl aus. • **4 – Not running**: Virtueller Computer wird nicht ausgeführt. • **5 – Unknown**: Informationen für virtuellen Computer nicht verfügbar.	MACHINE_VIRTUAL_STATE
Status	Der Status des virtuellen Computer. Mögliche Werte: • **0 – OK**: Keine Probleme. • **1 – Warning**: Mögliches Problem. • **2 – Error: Definite problems**. • **3 – Unknown**: Status ist unbekannt.	MACHINE_VIRTUAL_STATUS
Hardwareversion	Die Hardwareversion einer virtuellen Maschine spiegelt die unterstützten virtuellen Hardwarefunktionen der virtuellen Maschine wider.	HARDWARE_VERSION
Hypervisors	Wenn eine vCenter- oder SCVMM-Umgebung ausgewählt ist, werden in dieser Gruppe die Hypervisoren aufgelistet, die von vCenter oder SCVMM verwaltet werden.	
Hostname	Der dem ESXi-Host oder Hyper-V-Server zugewiesene Hostname. Wenn ein ESXi- oder Hyper-V-Gerät bereits zum Inventar hinzugefügt wurde, wird sein Namen in dieser Spalte als	keine Angabe

Abschnitt oder Element	Beschreibung	Datenbankfeld
	Hyperlink angezeigt. Wenn Sie auf den Link klicken, wird die Seite aktualisiert und zeigt Gerätedetails für das ausgewählte Gerät an.	
Plattform	Die Plattform und Version des zugehörigen ESXi- oder Hyper-V-Hypervisors.	PLATFORM
IP-Adresse	Die dem ESXi-Host zugewiesene IP-Adresse.	keine Angabe
Virtuelle Maschinen	Die Anzahl der virtuellen Maschinen auf dem ESXi- oder Hyper-V Hypervisor.	keine Angabe
System-Seriennummer	Die Seriennummer des Geräts, das den ESXi- oder Hyper-V-Hypervisor hostet.	keine Angabe
Status	Der ESXi Host-Status an.	keine Angabe
SDA-Bereitstellungsinformationen	Wenn Sie ein von der KACE System Deployment Appliance (SDA) bereitgestelltes Gerät auswählen, zeigt diese Gruppe die Bereitstellungsdetails an.	
Bereitstellungszeit	Der Zeitpunkt, zu dem die Bereitstellung erfolgreich abgeschlossen wurde.	SDA_DEPLOYMENT_TIME
Bereitstellungstyp	Der Bereitstellungstyp, z. B. skriptbasierte Installation, System-Image oder benutzerdefinierte Bereitstellung.	SDA_DEPLOYMENT_TYPE
Bereitstellungsname	Der Name der Bereitstellung, wie in KACE SDA angegeben.	SDA_DEPLOYMENT_NAME
Bereitstellungs-URL	Die URL zur Bereitstellung auf dem zugehörigen KACE SDA.	SDA_DEPLOYMENT_URL
Bereitstellungs-ID	Die ID der Bereitstellung auf dem KACE SDA.	SDA_SCRIPTED_INSTALLATION_ID
SDA-Name	Der Hostname oder die IP-Adresse der KACE SDA.	SDA_NAME
SDA-URL	Die URL von KACE SDA.	SDA_URL

Abschnitt oder Element	Beschreibung	Datenbankfeld
Akkus	Diese Gruppe zeigt Akkuinformationen für agentenbasiert und agentlos verwalteten Windows-, Linux- und MacOS-Geräten an.	
Laden	Die aktuelle Akkukapazität in Prozenten.	CHARGE_PERCENT
Chemie	**Nur Windows- und Linux-Geräte**. Der Akkutyp, z. B. Lithium-Ionen usw.	CHEMISTRY
Stromleistung (mWh)	Die Akku-Stromleistung.	CURRENT_CAPACITY
Vorgesehene Kapazität (mWh)	Die vorgegebene maximale Kapazität des Akkus.	DESIGN_CAPACITY
Vollständige Ladekapazität (mWh)	Maximale Stromleistung des Akkus. Dieser Wert nimmt mit der Zeit ab.	FULL_CHARGE_CAPACITY
Zustand (%)	Der Prozentsatz der Akku-Stromleistung im Vergleich zur vorgegebenen maximalen Kapazität.	HEALTH_PERCENT
Hersteller	Der Akkuhersteller.	MANUFACTURER
Name	Der Name oder das Modell des Akkus.	NAME
Angeschlossen	Eine Anzeige dafür, ob der Akku derzeit an eine Stromquelle angeschlossen ist.	PLUGGED_IN
Anzahl der Aufladungen	**Nur MacOS-Geräte**. Die Anzahl der Ladevorgänge des Akkus.	RECHARGE_COUNT
Seriennummer	Die Seriennummer des Akkus.	SERIAL
Verbleibende Zeit (Minuten)	Die Anzahl der Minuten, nach deren Ablauf der Akku entladen ist. Wenn der Akku an eine Stromquelle angeschlossen ist, ist dieses Feld leer.	TIME_REMAINING

Gruppe „Software“

Details zu den auf dem Gerät installierten Anwendungen einschließlich Informationen zu Patches, laufenden Prozessen und Startprogrammen.

Abschnitt	Beschreibung	Datenbankfeld
Installierte Programme	Eine Liste mit der auf dem Gerät installierten Software. Wenn der Änderungsverlauf für diesen Abschnitt aktiviert ist und sich die Informationen in diesem Abschnitt geändert haben, wird der Link **Änderungen anzeigen** neben der Überschrift eingeblendet. Klicken Sie auf **Änderungen anzeigen**, um nur die geänderten Elemente anzuzeigen. Klicken Sie auf **Änderungen ausblenden**, um alle Elemente anzuzeigen.	keine Angabe
Erkannte Software	Erkannte Anwendungen sind ausführbare Dateien im Inventar der Appliance, die den Definitionen von Anwendungen im Softwarekatalog entsprechen. Sie können die Nutzungserfassung für erkannte Anwendungen und Suites aktivieren, diese Anwendungen als Nicht zulässig kennzeichnen und Lizenzinformationen für sie hinzufügen. Außerdem können Sie die Liste mit den erkannten Anwendungen im CSV-Format exportieren. Sie können die Liste mit erkannten Anwendungen, die Liste mit nicht katalogisierten Anwendungen und die Liste der lokal katalogisierten Anwendungen exportieren. Sie können nicht den gesamten Softwarekatalog exportieren.	keine Angabe
Software mit erfasster Nutzung	Anwendungen, für die Sie die Erfassung der Nutzung aktiviert haben	keine Angabe
Felder für benutzerdefinierte Inventarisierung	Eine Liste aller Felder für benutzerdefinierte Inventarisierung (einschließlich Feldname und -wert), die für dieses Gerät erstellt wurden.	keine Angabe
Hochgeladene Dateien	Die Dateien, die von diesem Gerät mit der Skriptaktion *Datei hochladen* in die Appliance hochgeladen wurden.	keine Angabe
In Softwareinventar als installiert gemeldete Patches	Auf diesem Gerät installierte Patches von Microsoft.	keine Angabe

Abschnitt	Beschreibung	Datenbankfeld
	Wenn der Änderungsverlauf für diesen Abschnitt aktiviert ist und sich die Informationen in diesem Abschnitt geändert haben, wird der Link **Änderungen anzeigen** neben der Überschrift eingeblendet. Klicken Sie auf **Änderungen anzeigen**, um nur die geänderten Elemente anzuzeigen. Klicken Sie auf **Änderungen ausblenden**, um alle Elemente anzuzeigen.	
Prozesse werden ausgeführt	Eine Liste der auf dem Gerät ausgeführten Prozesse. Wenn der Änderungsverlauf für diesen Abschnitt aktiviert ist und sich die Informationen in diesem Abschnitt geändert haben, wird der Link **Änderungen anzeigen** neben der Überschrift eingeblendet. Klicken Sie auf **Änderungen anzeigen**, um nur die geänderten Elemente anzuzeigen. Klicken Sie auf **Änderungen ausblenden**, um alle Elemente anzuzeigen.	keine Angabe
Startprogramme	Eine Liste der auf dem Gerät ausgeführten Startprogramme. Wenn der Änderungsverlauf für diesen Abschnitt aktiviert ist und sich die Informationen in diesem Abschnitt geändert haben, wird der Link **Änderungen anzeigen** neben der Überschrift eingeblendet. Klicken Sie auf **Änderungen anzeigen**, um nur die geänderten Elemente anzuzeigen. Klicken Sie auf **Änderungen ausblenden**, um alle Elemente anzuzeigen.	keine Angabe
Dienste	Eine Liste der auf dem Gerät ausgeführten Dienste. Wenn der Änderungsverlauf für diesen Abschnitt aktiviert ist und sich die Informationen in diesem Abschnitt geändert haben, wird der Link **Änderungen anzeigen** neben der Überschrift eingeblendet. Klicken Sie auf **Änderungen anzeigen**, um nur die geänderten Elemente anzuzeigen. Klicken Sie auf	keine Angabe

Abschnitt	Beschreibung	Datenbankfeld
	Änderungen ausblenden, um alle Elemente anzuzeigen.	

Gruppe „Aktivitäten“

Informationen zu Aktionen, die auf dem Gerät ausgeführt werden sollen.

Abschnitt	Beschreibung	Datenbankfeld
Überwachung	Informationen zur Serverüberwachung (sofern aktiviert) und Informationen dazu, ob das Betriebssystem des Geräts unterstützt wird. Wird das Betriebssystem nicht unterstützt, wird eine Meldung mit einem entsprechenden Hinweis angezeigt. Wenn das Gerät überwacht werden kann, aber die Überwachung nicht aktiviert ist, wird die Schaltfläche **Überwachung aktivieren** angezeigt.	keine Angabe
Aktiv/Angehalten	Gibt an, ob die Überwachung für das Gerät aktiviert ist.	keine Angabe
Profile	Dem Gerät zugewiesene Warnkriterienprofile.	keine Angabe
Wartungsfenster	Dem Gerät zugewiesene Wartungsfenster.	keine Angabe
Stufe/Warnung	Aktive Warnungen für das Gerät mit Symbolen für die jeweilige Warnstufe.	keine Angabe
Labels	Die dem Gerät zugewiesenen Labels. Labels dienen zum Organisieren und Kategorisieren von Inventar und Assets.	keine Angabe
Fehler bei verwalteten Installationen	Eine Liste mit verwalteten, nicht erfolgreichen Installationen. Klicken Sie auf den Link **Detail zu verwalteter Installation**, um auf nähere Informationen zu den verwalteten Installationen zuzugreifen.	keine Angabe
Liste der verwalteten Installationen	Eine Liste mit verwalteten Installationen, die planmäßig bei der nächsten Verbindung	keine Angabe

Abschnitt	Beschreibung	Datenbankfeld
	des Geräts mit der Appliance an diesen gesendet werden.	
Service-Desk-Tickets	Eine Liste der mit diesem Gerät verknüpften Tickets. Hierbei kann es sich entweder um Tickets handeln, die dem Gerätebesitzer zugewiesen wurden, oder um Tickets, die vom Gerätebesitzer gesendet wurden. Klicken Sie auf die Ticket-ID (beispielsweise TICK:0032), um Details zum Ticket anzuzeigen.	keine Angabe
SNMP-Inventarkonfigurationen	Eine Liste der diesem Gerät zugeordneten SNMP-Inventarkonfigurationen. Um Zugriff auf die Details der Konfigurationen zu erhalten oder Konfigurationen hinzuzufügen, klicken Sie auf **Zugewiesene SNMP-Konfigurationen verwalten**.	keine Angabe

Gruppe „Sicherheit“

Informationen zu Patches und Sicherheitslücken für Geräte.

Abschnitt	Beschreibung	Datenbankfeld
Status von Patch-Erkennung/-Bereitstellung	Eine Liste der auf dem Gerät ermittelten und bereitgestellten Patches. Wenn Patch-Versuche unternommen wurden, die fehlgeschlagen sind, können Sie auf **Versuche zurücksetzen** klicken, um die Anzahl der Patch-Versuche auf die maximal zulässige Anzahl zurückzusetzen.	keine Angabe
Bedrohungsstufe 5 Liste	Bedrohungen, die für Anwendungen, Prozesse, Systemstartelemente oder Dienste auf dem Gerät schädlich sind.	keine Angabe
Status der Windows-Funktionsaktualisierung	Eine Liste der auf dem Gerät ermittelten und bereitgestellten Windows-Funktionsaktualisierungsaufgaben. Wenn Aktualisierungsversuche unternommen wurden, die fehlgeschlagen sind, können Sie auf **Versuche zurücksetzen** klicken, um die Anzahl der	

Abschnitt	Beschreibung	Datenbankfeld
	Patch-Versuche auf die maximal zulässige Anzahl zurückzusetzen.	
OVAL-Sicherheitslücken	Die Ergebnisse der OVAL-Tests (Open Vulnerability Assessment Language, Offener Mitre-Standard für Sicherheitslücken), die auf diesem Gerät ausgeführt wurden. Nur auf diesem Gerät fehlgeschlagene Tests werden mit ihrer OVAL-ID und der Kennzeichnung *Angreifbar* aufgeführt. Erfolgreiche Tests werden gemeinsam als *Sicher* markiert.	keine Angabe
Überprüfung der SCAP-Konfiguration	Die Ergebnisse der Überprüfung der FDCC-/SCAP-Konfigurationsscans, die auf diesem Gerät durchgeführt wurden.	keine Angabe
Linux Package Repository Information (Informationen zum Linux-Paket-Repository)	Eine Liste der URLs zu den Geräten zugeordneten Linux-Paket-Repositorys.	keine Angabe
Linux Package Upgrades Status (Status der Linux-Paketaktualisierungen)	Eine Liste der auf dem Gerät ermittelten und bereitgestellten Patches. Wenn Patch-Versuche unternommen wurden, die fehlgeschlagen sind, können Sie auf **Versuche zurücksetzen** klicken, um die Anzahl der Patch-Versuche auf die maximal zulässige Anzahl zurückzusetzen.	keine Angabe

Gruppe „Dell Command | Monitor“

Zusätzliche Inventarinformationen zu ausgewählten Dell Clientsystemen über Dell Command | Monitor.

Abschnitt	Beschreibung	Datenbankfeld
Warnungen	DCM Protokolleinträge. Diese können von der Firmware erkannte Hardwarefehler angeben.	keine Angabe
Hardware	Die erfassten Informationen, die ausführliche Akkuinformationen und Nutzungsdaten, Vorhandensein und Konfiguration des Dienstprozessors, Arbeitsspeicherinventar und	keine Angabe

Abschnitt	Beschreibung	Datenbankfeld
	angeschlossene Dell Monitore umfassen.	

Informationen zur den Klassen und Eigenschaften, die von der Appliance mithilfe von Dell Command | Monitor abgefragt werden, finden Sie unter Informationen zu Dell Command | Monitor.

Gruppe „Dell Aktualisierungen“

Informationen zu Aktualisierungen und Inventar (nur für Geräte von Dell).

Abschnitt	Beschreibung	Datenbankfeld
Dell Updates Detect/Deploy Status (Erkennungs-/ Bereitstellungsstatus von Dell Aktualisierung)	Eine Liste der erkannten und auf dem Gerät bereitgestellten Dell Aktualisierungen sowie aller zugehörigen Zeitpläne. Wenn Aktualisierungsversuche unternommen wurden, die fehlgeschlagen sind, können Sie auf **Versuche zurücksetzen** klicken, um die Anzahl der Aktualisierungsversuche auf die maximal zulässige Anzahl zurückzusetzen.	keine Angabe

Gruppe für Protokolle und Diagnose

Informationen zu Appliance-Datensätzen.

- **Verwaltungsdienst-Protokolle**: Die Hauptaufgabe des Verwaltungsdiensts der Appliance besteht in der Ausführung der Offline-KScripts. Die Verwaltungsdienstprotokolle zeigen die Schritte an, die von der Verwaltung vorgenommen wurden.
- Dienst zum Ausführen der Offline-KScripts. Hierzu gehören das Herunterladen von Abhängigkeiten und die Überprüfung der KBOTS-Datei. Fehler bei der Ausführung von Offline-KScripts werden in den Verwaltungsdienst-Protokollen protokolliert.
- **Bootstrap-Protokolle**: Die Appliance sendet eine Bootstrap-Anforderung, um Inventarinformationen für Geräte abzurufen, die sich erstmals angemeldet haben. Die auf diese Anforderung bezogenen Protokolle werden in den Bootstrap-Protokollen angezeigt.
- **Client-Protokolle**: Die Appliance sendet eine Anforderung an den Agenten, um regelmäßig Inventarinformationen abzurufen. Auf dem Gerät wird ein Skript ausgeführt. Daraufhin werden die Inventarinformationen an die Appliance gesendet und das Inventar in die Appliance hochgeladen. Diese Aktionen werden in den Agenten-Protokollen angezeigt.
- **Scripting-Updater**: Von dem Gerät wird regelmäßig eine Anforderung gesendet, um die neuesten Informationen in Bezug auf die Änderungen in Offline-KScripts abzurufen. Diese Informationen werden in Scripting-Updater-Protokollen angezeigt.
- **Statusmeldungen des Inventars ohne Agent**: Das Protokoll zeigt Meldungen bezüglich der Erfassung und Einsendung von Inventardaten von Geräten, die ohne Agenten verwaltet werden.

Abschnitt	Beschreibung	Datenbankfeld
Agentenprotokolle	Die Protokolle des KACE Agent.	keine Angabe
Agent-Diagnosedateien	Sie können diese Dateien über **Aktion auswählen > Agent-**	keine Angabe

Abschnitt	Beschreibung	Datenbankfeld
	Dateien hochladen auf dieser Seite hochladen.	
Installationsprotokolle der Benutzerkonsole	Details zu Paketen der **Benutzerkonsole**, die auf diesem Gerät installiert sind.	keine Angabe
Skriptprotokoll	Skripte, z. B. die auf diesem Gerät ausgeführten Konfigurationsrichtlinienskripte sowie der verfügbare Status aller laufenden Skripte.	keine Angabe
Serverseitige Geräteprotokolldaten	Protokolleinträge für das ausgewählte Gerät. In diesem Abschnitt werden die letzten fünf Einträge jedes zugehörigen Protokolls angezeigt, anhand derer Sie vorhandene Probleme beheben können.	keine Angabe
Geräteaktivität	**Nur Chrome-Geräte**. Zeigt das Datum, an dem das Gerät zuletzt aktiv war, die Dauer der Aktivität und den Aktivitätsverlauf an. Jeder Eintrag im Aktivitätsverlauf zeigt das Datum und die Länge der einzelnen Benutzersitzungen an.	keine Angabe

Gruppe „Asset“

In diesem Abschnitt werden die Details zu dem Asset angezeigt, mit dem dieses Gerät verknüpft ist. Klicken Sie auf den Link **Dieses Asset bearbeiten**, um die Asset-Informationen zu bearbeiten.

Abschnitt	Beschreibung	Datenbankfeld
Asset-Informationen	Details wie Datum und Uhrzeit der Erstellung und letzten Änderung des Datensatzes, der Asset-Typ (z. B. Gerät) sowie der Name des Assets.	keine Angabe
Barcodes	Barcodes die mit diesem Asset verknüpft sind, sofern vorhanden.	keine Angabe
Zugehörige Assets	Mit diesem Asset verwandte Assets, wie z. B. über- und untergeordnete Assets.	keine Angabe
Aufgabenverlauf	Eine Liste der auf dem Gerät ausgeführten Aufgaben.	keine Angabe

Informationen zu Dell Data Protection | Encryption (DDP|E) und Verschlüsselungsinformationen in Gerätedetails

Wenn auf Geräten im Netzwerk der DDP|E Client installiert ist, kann die Appliance Status- und Konfigurationsinformationen erfassen und auf der Seite *Gerätedetail* anzeigen.

Festlegen des Registrierungsschlüssels in Windows DDP|E Client erforderlich

Damit die Appliance detaillierte Inventardaten von Windows DDP|E Clients erfassen kann, müssen Sie im Client den Schlüssel `DumpXmlInventory` festlegen.

```
Schlüssel: HKLM\SYSTEM\CurrentControlSet\services\DellMgmtAgent\Parameters
DWORD-Wert: DumpXmlInventory
Daten: 0x1
```

Dieser Registrierungswert verursacht, dass der DDP|E eine Datei `inventory.xml` auf das Zielgerät schreibt, die daraufhin vom Inventar analysiert wird. Siehe Dump Inventory-Registrierungsschlüssel zur Inventarerfassung von Windows DDP|E-Client-Geräten hinzufügen.

Diese Anforderung gilt nur für Windows.

Dell Data Protection | Encryption (DDP|E)

DDP|E besteht aus Anwendungen, die dem Benutzer Folgendes ermöglichen:

- Erkennen von Risiken für die Datensicherheit auf Desktops, Notebooks und externen Medien
- Schützen von Daten auf diesen Geräten durch Durchsetzung von Zugriffskontrollrichtlinien, Authentifizierung und Verschlüsselung sensibler Daten
- Zentrales Verwalten von Daten mit Richtlinien unter Verwendung kollaborativer Tools, die sich in vorhandene Benutzerverzeichnisse integrieren
- Unterstützen von Schlüssel- und Datenwiederherstellung, automatischen Aktualisierungen und Verfolgen geschützter Geräte

Unterstützte Betriebssysteme für DDP|E

Betriebssystem	Versionen
Windows	7, 8, 8,1
Mac OS X	10.7.5, 10.8.3–10.8.5, 10.9.2–10.9.3

Auf der Seite „Gerätedetail“ angezeigte DDP|E Informationen

Element	Beschreibung	MACHINE_DDPE Datenbankfeld
Eindeutige ID	Eine Identifikation des DDP|E Clients, die vom DDP|E Server verwendet wird.	MCID
Version des Agenten	Installierte Version des DDP|E Clients.	AGENT_VERSION
Hostname des Servers	Hostname des DDP|E Servers, der diesen DDP|E Client verwaltet.	SERVER_HOSTNAME

Element	Beschreibung	MACHINE_DDPE Datenbankfeld
Schutzstatus	Beispielwerte lauten *Geschützt* und *Ungeschützt*. Werte wie *Gesperrt* oder *Unbekannt* können auf ein Problem hindeuten.	PROTECTION_STATUS
Letztes generiertes Inventar	Zeitstempel der letzten Inventarisierung des DDP|E Clients. Nicht zu verwechseln mit dem K1 Inventar.	PROTECTION_STATUS_UPDATED

Auf der Seite „Gerätedetail“ angezeigte DDP|E Volume-Informationen

Element	Beschreibung	MACHINE_DDPE_VOLUME Datenbankfeld
Gerät	Name des Geräts/Volume, das vom Betriebssystem gemeldet wird.	DEVICE_ID
Schutzstatus	Angabe der aktuellen Ebene/des Status des DDP|E Schutzes auf dem DDP|E Client.	PROTECTION_STATUS
Schutzgrund	Art des auf dem DDP|E Client verwendeten Schutzes. Die Option lautet für gewöhnlich *Anbietergeschützt*, was für DDP|E oder BitLocker steht.	PROTECTION_REASON

BitLocker

BitLocker ist eine in Windows enthaltene Funktion zur vollständigen Datenträgerverschlüsselung.

Unterstützte Betriebssysteme für BitLocker

Betriebssystem	Versionen
Windows	Vista, 7 (Enterprise und Ultimate)
Windows	8, 8.1 (Pro und Enterprise)
Windows Server	2008, 2008 R2, 2012, 2012 R2

Auf der Seite „Gerätedetail“ angezeigte BitLocker Informationen

Element	Beschreibung	MACHINE_BITLOCKER_VOLUME Datenbankfeld
Geräte-ID	Eindeutiger Bezeichner für das Volume auf dem System.	DEVICE_ID
Persistente Volume-ID	Ein persistenter Bezeichner für das Volume auf dem System.	PERSISTENT_VOLUME_ID

Element	Beschreibung	MACHINE_BITLOCKER_VOLUME Datenbankfeld
Schutzstatus	Gibt an, ob BitLocker das Volume schützt. • Schutz aus • Schutz ein • Schutz unbekannt	PROTECTION_STATUS
Metadatenversion	Mögliche Werte: • 0 • 1 • 2	VERSION
Verschlüsselungsmethode	Verwendeter Verschlüsselungstyp. Beispiel: *AES-128*. Mögliche Werte: • Kein(e) • AES-128 mit Diffusor • AES-256 mit Diffusor • AES-128 • AES-256 • Verschlüsselt • Unbekannt	SELF_ENCRYPTION_DRIVE _ENCRYPTION_METHOD (nur selbstverschlüsselnde Laufwerke) ENCRYPTION_METHOD (Nur softwarebasierte Verschlüsselung)
Hardware-Verschlüsselungsstatus	**HINWEIS:** Die Eigenschaft „Hardware-Verschlüsselungsstatus“ wird von Systemen mit Windows 8 (oder höher) unterstützt. Mögliche Werte: • Unbekannt • Nicht unterstützt • Kein Schutz • Verwendet Software • Verwendet Hardware	HARDWARE_ENCRYPTION_STATUS
Sperrstatus	Mögliche Werte: • Unbekannt • Entsperrt • Gesperrt	LOCK_STATUS

Element	Beschreibung	MACHINE_BITLOCKER_VOLUME Datenbankfeld
Konvertierungsstatus	Status der Konvertierung. Mögliche Werte: • Unbekannt • Vollständig entschlüsselt • Vollständig verschlüsselt • Verschlüsselung läuft • Entschlüsselung läuft • Verschlüsselung angehalten • Entschlüsselung angehalten	CONVERSION_STATUS
Verschlüsselungsfortschritt (%)	Der Fortschritt der Konvertierung in Prozent.	ENCRYPTION_PERCENTAGE
Bereinigungsstatus	Status der Speicherplatzbereinigung. Mögliche Werte: • Unbekannt • Freier Speicherplatz nicht bereinigt • Freier Speicherplatz bereinigt • Speicherplatzbereinigung läuft • Speicherplatzbereinigung angehalten	WIPING_STATUS
Bereinigungsfortschritt (%)	Der Fortschritt der Speicherplatzbereinigung in Prozent.	WIPING_PERCENTAGE

Element	Beschreibung	MACHINE_BITLOCKER_VOLUME Datenbankfeld
Schlüsselschutzvorrichtungen	Aktive Schlüsselschutzvorrichtungen. Mögliche Werte: • Unbekannt • Trusted Platform Module (TPM) • Externer Schlüssel • Numerisches Kennwort • TPM und PIN • TPM und Systemstartschlüssel • TPM und PIN und Systemstartschlüssel • Öffentlicher Schlüssel • Passphrase • TPM-Zertifikat • CNG-Schutzvorrichtung (CryptoAPI Next Generation)	KEY_PROTECTORS

FileVault 2

FileVault 2 ist eine in Mac OS X enthaltene Funktion zur vollständigen Datenträgerverschlüsselung.

Unterstützte Betriebssysteme für FileVault 2

Betriebssystem	Versionen
Mac OS X	10,8, 10,9, 10,10

Auf der Seite „Gerätedetail“ angezeigte FileVault 2 Informationen

Element	Beschreibung	MACHINE_FILEVAULT_VOLUME Datenbankfeld
Aktiviert	Gibt an, ob FileVault aktiviert ist.	IS_ENABLED
Persönlicher Wiederherstellungsschlüssel	Gibt das Vorhandensein eines persönlichen Wiederherstellungsschlüssels an.	HAS_PERSONAL_RECOVERY_KEY
Institutioneller Wiederherstellungsschlüssel	Gibt das Vorhandensein eines vom Unternehmen bereitgestellten X.509-basierten asymmetrischen Schlüsselpaars an.	HAS_INSTITUTIONAL_RECOVERY_KEY

Element	Beschreibung	MACHINE_FILEVAULT_VOLUME Datenbankfeld
Autorisierte Benutzer	Eine Liste der Konten, die das Laufwerk in EFI entsperren können.	AUTHORIZED_USERS
Konvertierungsstatus	Der Status des Verschlüsselungsvorgangs. Beispiele umfassen *Konvertierung ausstehend*, *Konvertierung läuft*, *Konvertierung angehalten* und *Abgeschlossen*.	CONVERSION_STATUS
Konvertierungsfortschritt (%)	Der Fortschritt der Konvertierung in Prozent.	CONVERSION_PERCENTAGE
Verschlüsselungsstatus	Status der Verschlüsselung. Beispiel: *Gesperrt* oder *Entsperrt*.	ENCRYPTION_STATUS
Verschlüsselungstyp	Verwendeter Verschlüsselungstyp. Beispiel: *AES-XTS*.	ENCRYPTION_TYPE
Gerät	Eindeutiger Bezeichner für das Volume auf dem System.	DEVICE_ID
Version		VERSION

Trusted Platform Module (TPM)

TPM ist ein dedizierter Mikroprozessor, der Hardware schützt, indem er Kryptografieschlüssel in Geräte integriert.

Unterstützte Betriebssysteme für TPM

Betriebssystem	Versionen
Windows	Vista, 7, 8, 8.1
Windows Server	2008, 2008 R2, 2012, 2012 R2

Auf der Seite „Gerätedetail“ angezeigte TPM Informationen

Element	Beschreibung	MACHINE_TPM Datenbankfeld
Hersteller	Hersteller des TPM-Chips.	MANUFACTURER_ID_TEXT
Herstellerversion	Version des TPM-Chips.	MANUFACTURER_VERSION
Herstellerversionsinformationen	Weitere Informationen zur für den Hersteller spezifischen Version.	MANUFACTURER_VERSION_INFO

Element	Beschreibung	MACHINE_TPM Datenbankfeld
Spezifikationsversion	Die Version der TCG-Spezifikation (Trusted Computing Group), die das TPM unterstützt.	SPECIFICATION_VERSION
Version der physischen Anwesenheit	Die Version der physischen Anwesenheitsschnittstelle, die das Gerät unterstützt. Die physische Anwesenheitsschnittstelle ist ein Kommunikationsmechanismus, der Gerätevorgänge ausführt, bei denen eine physische Anwesenheit erforderlich ist.	PHYSICAL_PRESENCE_VERSION _INFO
TPM aktiviert	Schritt 1 der TPM-Initialisierung.	IS_TPM_ENABLED
TPM aktiviert	Schritt 2 der TPM-Initialisierung.	IS_TPM_ACTIVATED
TPM in Besitz	Schritt 3 der TPM-Initialisierung.	IS_TPM_OWNED

Dump Inventory-Registrierungsschlüssel zur Inventarerfassung von Windows DDP|E-Client-Geräten hinzufügen

Wenn auf einem Windows DDP|E-Client der Registrierungsschlüssel `DumpXmlInventory` nicht vorhanden ist, kann die Appliance nicht auf die XML-Inventardatei zugreifen, um die entsprechenden Feldinformationen zu erfassen.

Dell Data Protection | Encryption ist auf dem Windows Gerät installiert. Weitere Informationen finden Sie unter http://www.dell.com/support/home/us/en/19/product-support/product/dell-data-protection-encryption/drivers.

Das Verfahren zum Hinzufügen des Schlüssels ist für vom Agenten verwaltete Geräte und ohne Agent verwaltete Geräte unterschiedlich.

- Registrierungsschlüssel DumpXmlInventory zu einem Windows Gerät mit Agentenverwaltung hinzufügen
- Registrierungsschlüssel DumpXmlInventory zu einem ohne Agent verwalteten Windows Gerät hinzufügen

Registrierungsschlüssel DumpXmlInventory zu einem Windows Gerät mit Agentenverwaltung hinzufügen

Damit die Appliance Feldinformationen aus der XML-Inventardatei eines Clients extrahieren kann, muss diesem Windows DDP|E-Client der Registrierungsschlüssel `DumpXmlInventory` hinzugefügt werden.

Für Windows-Geräte mit Agentenverwaltung kann zum Hinzufügen des Registrierungsschlüssels "dump inventory" ein Standard-Offline-KScript der Appliance-Skriptfunktion verwendet werden. Dieser Schlüssel ist erforderlich, damit der DDP|E-Agent die detaillierten XML-Inventardaten in das Appliance-Dateisystem schreiben kann.

HINWEIS: Nachdem der Registrierungsschlüssel hinzugefügt worden ist, erfordert der DDP|E-Service einen vollständigen Richtlinien-Aktualisierungszeitplan, bevor die Appliance Inventarinformationen erfassen kann.

1. Rufen Sie die Seite *Skriptdetail* auf, um das Skript *K1000 Enable Detailed DDPE Inventory (Windows)* zu bearbeiten.

a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.

b. Klicken Sie in der linken Navigationsleiste auf **Skripterstellung** und anschließend auf **Skripte**.

c. Wählen Sie aus der Liste **K1000 Enable Detailed DDPE Inventory (Windows)** aus.

2. Legen Sie im Abschnitt *Konfiguration* die Skripteinstellungen fest:

Option	Beschreibung
Name	*K1000 Enable Detailed DDPE Inventory (Windows)*, der Name dieses Standardskripts.
Aktiviert	Aktivieren Sie dieses Kontrollkästchen, um das Skript auf den Zielgeräten auszuführen. Aktivieren Sie ein Skript erst, nachdem Sie es getestet haben und es zur Ausführung bereit ist. Aktivieren Sie das Skript für ein Testlabel, bevor Sie es auf allen Geräten aktivieren.
Typ	Der Skripttyp ist **Offline-KScripts**.
Status	Gibt an, dass das Skript für die Implementierung im Netzwerk bereit ist. Stellen Sie den Status auf **Produktion** ein.
Beschreibung	Enthält eine kurze Beschreibung der Aktionen, die vom Standardskript ausgeführt werden.
Anmerkungen	Geben Sie nach Bedarf beliebige weitere Informationen ein.

3. Geben Sie im Abschnitt *Bereitstellung* die Bereitstellungsoptionen an:

Option	Beschreibung
Alle Geräte	Stellen Sie die Funktion auf allen Geräten bereit. Deaktivieren Sie das Kontrollkästchen, um die Bereitstellung auf bestimmte Labels oder Geräte zu beschränken.
Labels	Beschränken Sie die Bereitstellung auf Geräte, die zu angegebenen Labels gehören. Klicken Sie zum Auswählen von Labels auf **Bearbeiten**, ziehen Sie die Labels ins Fenster *Bereitstellung beschränken auf* und klicken Sie dann auf **Speichern**. Wenn Sie ein Label auswählen, das über eine Replikationsfreigabe oder eine alternative Download-Quelle verfügt, werden digitale Assets aus dieser Replikationsfreigabe oder aus dieser alternativen Download-Quelle kopiert und nicht direkt von der Appliance heruntergeladen. **HINWEIS:** Die Appliance nutzt eine Replikationsfreigabe, bevor sie den Alternativen KACE Speicherort verwendet.

Option	Beschreibung
Geräte	Mit dieser Option begrenzen Sie die Bereitstellung auf ein Gerät oder mehrere Geräte. Um nach Geräten zu suchen, beginnen Sie mit Ihrer Eingabe in das Feld.
Betriebssysteme	Das Betriebssystem, auf dem die Anwendung ausgeführt wird. Die Bereitstellung der Anwendungen erfolgt nur auf Geräten mit den ausgewählten Betriebssystemen. a. Klicken Sie auf **Betriebssysteme verwalten**. b. Wählen Sie im daraufhin angezeigten Dialogfeld **Betriebssysteme** die Betriebssystemversionen in der Navigationsstruktur aus. Sie haben die Möglichkeit, Betriebssystemversionen nach Familie, Produkt, Architektur, Versions-ID oder Build-Version auszuwählen. Je nach Bedarf können Sie eine bestimmte Build-Version oder einen übergeordneten Knoten auswählen. Wenn Sie einen übergeordneten Knoten im Baum auswählen, werden die zugehörigen untergeordneten Knoten automatisch mit ausgewählt. Aufgrund dieses Verhaltens können Sie beliebige zukünftige Betriebssystemversionen auswählen, da Geräte in Ihrer verwalteten Umgebung hinzugefügt oder aktualisiert werden. Wenn Sie beispielsweise alle aktuellen und zukünftigen Versionen auswählen möchten, die mit der Windows 10 x64-Architektur verbunden sind, wählen Sie unter **Alle** > **Windows** > **Windows 10** die Option **x64** aus.

4. Geben Sie im Abschnitt *Planen* die Ausführungsoptionen an:

Option	Beschreibung
Kein(e)	Die Ausführung erfolgt im Zusammenhang mit einem Ereignis anstatt zu einem bestimmten Datum oder zu einem bestimmten Zeitpunkt.
jede Stunde	Der Vorgang wird im angegebenen Intervall durchgeführt.
Täglich/an einem bestimmten Tag um HH:MM	Die Erfassung wird täglich zu einem bestimmten Zeitpunkt oder an einem bestimmten Wochentag um eine bestimmte Uhrzeit ausgeführt.
Ausführen am n-ten jedes Monats/eines bestimmten Monats um HH:MM	Die Erfassung wird jeden Monat oder in einem bestimmten Monat an einem festgelegten Datum zu einer festgelegten Uhrzeit ausgeführt.

Option	Beschreibung
Ausführen am n-ten Wochentag **jedes Monats/ eines bestimmten Monats um HH:MM**	Die Erfassung wird jeden Monat oder in einem bestimmten Monat an einem festgelegten Wochentag zu einer festgelegten Uhrzeit ausgeführt.

Benutzerdefiniert	Führen Sie die Erfassung nach einem benutzerdefinierten Zeitplan aus.
	Verwenden Sie das Standard-5-Feld-Cron-Format (das erweiterte Cron-Format wird nicht unterstützt):
	`* * * * *`
	`| | | | +————————Wochentag (0-6) (Sonntag=0)`
	`| | | +————————Monat (1-12)`
	`| | +————————Monatstag (1-31)`
	`| +————————Stunde (0-23)`
	`+————————Minute (0-59)`
	Verwenden Sie bei der Angabe von Werten die folgenden Zeichen:
	• **Leerzeichen( )**: Die einzelnen Felder mit einem Leerzeichen trennen.
	• **Sternchen (*)**: Ein Sternchen repräsentiert den gesamten Wertebereich in einem Feld. Zum Beispiel repräsentiert ein Sternchen im Stundenfeld eine beliebige Stunde.
	• **Kommas (,)**: Mehrere Werte in einem Feld werden mit einem Komma getrennt. Zum Beispiel werden mit `0,6` im Feld „Wochentag“ Sonntag und Samstag angegeben.
	• **Bindestriche (-)**: Mit einem Bindestrich wird ein Wertebereich in einem Feld angegeben. Zum Beispiel entspricht `1-5` im Feld „Wochentag“ `1,2,3,4,5`, d. h. Montag bis Freitag.
	• **Schrägstriche (/)**: Die Angabe der Zeitabstände, mit denen eine Aktion wiederholt werden soll, erfolgt mit einem Schrägstrich. Zum Beispiel entspricht `*/3` im Feld Stunde `0,3,6,9,12,15,18,21`. Das Sternchen (`*`) gibt jede Stunde an, mit `/3` erfolgt aber eine Einschränkung auf durch drei teilbare Stunden.

Option	Beschreibung
	Beispiele: • `15 * * * * Jeden Tag 15 Minuten nach jeder vollen Stunde ausführen` • `0 22 * * * Jeden Tag um 22:00 Uhr ausführen` • `0 0 1 1,6 * Am 1. Januar und 1. Juni um 00:00 Uhr ausführen` • `30 8,12 * * 1-5 An Wochentagen um 08:30 Uhr und 12:30 Uhr ausführen` • `0 2 */2 * * Jeden zweiten Tag um 02:00 Uhr ausführen`
Aufgabenplan anzeigen	Klicken Sie, um den Aufgabenplan anzuzeigen. Im Dialogfeld *Aufgabenplan* wird eine Liste der geplanten Aufgaben angezeigt. Klicken Sie auf eine Aufgabe, um die Aufgabendetails anzuzeigen. Weitere Informationen hierzu finden Sie unter Aufgabenpläne anzeigen.

5. Überspringen Sie die Abschnitte *Abhängigkeiten* und *Aufgaben*.
6. Führen Sie einen der folgenden Schritte aus:
   - **Klicken Sie auf Jetzt ausführen, um das Skript sofort mittels Push an alle Geräte zu übertragen.**

     Verwenden Sie diese Option mit Vorsicht. Siehe Verwenden der Befehle "Ausführen" und "Jetzt ausführen".
   - **Klicken Sie auf Speichern.**

Registrierungsschlüssel DumpXmlInventory zu einem ohne Agent verwalteten Windows Gerät hinzufügen

Damit die Appliance Feldinformationen aus der XML-Inventardatei eines Clients extrahieren kann, muss diesem Windows DDP|E-Client der Registrierungsschlüssel `DumpXmlInventory` hinzugefügt werden.

Für ohne Agent verwaltete Windows Geräte müssen Sie ein neues Gruppenrichtlinienobjekt auf einem Gerät unter Windows Server 2008 oder 2012 erstellen, damit die Registrierungseinstellungen auf mehreren Geräten in der Domäne bereitgestellt werden können.

1. Öffnen Sie auf einem Gerät unter Windows Server 2008 oder 2012 die *Gruppenrichtlinien-Verwaltungskonsole*.
2. Klicken Sie mit der rechten Maustaste auf **Gruppenrichtlinienobjekte** und auf **Neu**.
3. Geben Sie einen beschreibenden Namen für das neue Gruppenrichtlinienobjekt an (z. B. Dell Data Protection | Encryption: Inventarregistrierungseinstellung) und klicken Sie auf **OK**.
4. Klicken Sie mit der rechten Maustaste auf das neue Gruppenrichtlinienobjekt und anschließend auf **Bearbeiten**.
5. Navigieren Sie zu **Computerkonfiguration** > **Voreinstellungen** > **Windows Einstellungen** > **Registrierung**.
6. Klicken Sie mit der rechten Maustaste auf **Registrierung** und wählen Sie **Neu** > **Registrierungselement** aus.
7. Wählen Sie auf der Registerkarte *Allgemein* die Option **Aktualisieren** im Dropdown-Menü *Aktion* aus.
8. Wählen Sie **HKEY_LOCAL_MACHINE** in der Dropdown-Liste *Struktur* aus.
9. Geben Sie einen *Schlüsselpfad* für `SYSTEM\CurrentControlSet\services\DellMgmtAgent\Parameters` an.
10. Geben Sie einen *Wert* von DumpXmlInventory an.
11. Wählen Sie **REG_DWORD** in der Dropdown-Liste *Werttyp* aus.
12. Geben Sie 1 im Datenfeld *Wert* an.
13. Wählen Sie die Option *Hexadezimal* in der Gruppe *Basis* aus und klicken Sie auf **OK**.
14. Schließen Sie den *Gruppenrichtlinienverwaltungs-Editor*.

Sie können jetzt das neue Gruppenrichtlinienobjekt mit einer bestimmten Domäne, Organisationseinheit usw. verknüpfen.

WICHTIG: Sie sollten das Gruppenrichtlinienobjekt auf einem bestimmten Computer oder auf mehreren Computern testen, bevor es auf allen Systemen bereitgestellt wird.

Informationen zu Intel AMT in Gerätedetails

Auf Intel basierten Windows-Geräten mit vorhandener Intel AMT Technologie kann die Appliance Informationen zur AMT Konfiguration anzeigen.

Intel AMT ist eine hardwarebasierte Technologie für die Remote-Verwaltung von Intel basierten Computern. Intel AMT ist eine Funktion der Intel® Core™ Prozessoren mit Intel® vPro™ Technologie.

HINWEIS: Die hier erwähnte Datenerfassung erfolgt separat von den vPro und AMT Daten, die die Appliance mithilfe von Dell Command | Monitor erfasst. Siehe Informationen zu Dell Command | Monitor.

Intel AMT Ressourcen und Appliance-Anforderungen

Informationen vom Dell Tech Center erhalten Sie unter http://en.community.dell.com/techcenter/enterprise-client/w/wiki/7537.dell-command-intel-vpro-out-of-band. Informationen sowie einen Downloadlink für die Intel Setup- und Konfigurationssoftware (Setup and Configuration Software, SCS) mit den für die Konfiguration von Intel AMT erforderlichen Komponenten finden Sie unter http://www.intel.com/content/www/us/en/software/setup-configuration-software.html.

Damit die Appliance Zugriff auf die vollständigen Inventarinformationen auf einem AMT Gerät erhält, muss auf dem Gerät die Intel Management Engine installiert sein. Treiberdownloads von Intel stehen Ihnen unter https://downloadcenter.intel.com/search?keyword=intel+management+engine zur Verfügung.

Intel AMT Informationen

Auf der Seite „Gerätedetail“ angezeigte Intel AMT Informationen

Element	Beschreibung	MACHINE_INTEL_AMT Datenbankfeld
SKU	Die Lagermengeneinheit des Geräts. Folgende Werte sind möglich: • Vollständige AMT Verwaltungsfunktionen • Standardmäßige Verwaltungsfunktionen	SKU
Status	Gibt an, ob AMT auf dem Gerät aktiviert ist.	STATE IS_AMT_CONFIGURED
Konfigurationsmodus	Der aktuelle Konfigurationsmodus des AMT Geräts. Folgende Werte sind möglich: • SMB-Modus • Unternehmensmodus • Kein(e)	CONFIGURATION_MODE
Steuerungsmodus	Der aktuelle Steuerungsmodus des AMT Geräts. Folgende Werte sind möglich: • Clientsteuerungsmodus • Administratorsteuerungsmodus • Kein(e)	CONTROL_MODE
Firmwareversion	Die Version der Firmware auf dem AMT Gerät.	FW_VERSION
MEI Treiber	Zeigt an, ob der MEI Treiber installiert ist und funktioniert, und gibt ggf. die Treiberversion an.	IS_MEI_ENABLED MEI_VERSION

Suchen und Verwalten von Geräten

Verwenden Sie für die Suche nach Geräten im Inventar sowie für deren Verwaltung die erweiterte Suche sowie Label und Warnungen.

Suche nach Geräten im Inventar

Mit der erweiterten Suche können Sie für jedes Feld im Inventardatensatz einen Wert angeben und das gesamte Inventar nach diesen Werten durchsuchen.

Diese Art der Suche ist hilfreich, wenn Sie nach Geräten mit bestimmten Eigenschaften wie etwa einer bestimmten BIOS-Version, MAC-Adresse oder einem bestimmten Betriebssystem suchen. Siehe Auf Seitenebene mit erweiterten Optionen suchen.

Sie können auch eine einfache Suche ausführen, um schnell ein bestimmtes Gerät zu finden. Sie können beispielsweise nach einem Gerät suchen, dessen Barcode bestimmte Zeichen enthält.

Verwenden von Benachrichtigungen für die Suche nach Geräten

Sie können Benachrichtigungen so konfigurieren, dass automatisch E-Mail-Nachrichten an Administratoren gesendet werden, wenn Geräte die von Ihnen ausgewählten Kriterien erfüllen. Sie können zum Beispiel E-Mail-Benachrichtigungen basierend auf der Datenträgernutzung einrichten, wenn Sie Administratoren benachrichtigen möchten, sobald ein bestimmtes Speicherlimit auf einem Datenträger erreicht ist. Siehe Benachrichtigungszeitpläne über den Bereich "Berichterstellung" hinzufügen.

Filtern von Geräten nach Organisationseinheit

Mithilfe von LDAP-Labels können Sie Geräte nach einer auf einem LDAP- oder Active Directory-Server vorhandenen Organisationseinheit filtern. Siehe Informationen zu LDAP-Labels.

Geräte mithilfe von Labels gruppieren

Sie können manuelle Labels und Smart Labels verwenden, um Geräte zu gruppieren. Dadurch können Sie Aktionen wie das Aktualisieren von Software für eine Gruppe von Geräten ausführen.

Um die Erfassung von Anwendungen im Softwarekatalog zu ermöglichen, müssen Sie den Geräten, auf denen die Anwendungen installiert sind, ein für die Erfassung aktiviertes Label zuweisen. Weitere Informationen zur Erfassung finden Sie unter Verwenden der Erfassung der Softwarenutzung.

Manuelle Gerätelabels hinzufügen, zuweisen und entfernen

Sie können manuelle Labels hinzufügen und diese auf Geräte anwenden oder von diesen entfernen. Manuelle Labels bleiben so lange mit Geräten verknüpft, bis sie manuell von den Geräten entfernt werden.

1. Rufen Sie die Liste *Geräte* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Inventar** und anschließend auf **Geräte**.
2. Aktivieren Sie die Kontrollkästchen neben einem oder mehreren Geräten.
3. Wählen Sie **Aktion auswählen** > **Label hinzufügen**.
4. Geben Sie im Textfeld *Label hinzufügen* einen Namen für das Label ein.

   TIPP: Vermeiden Sie in Labelnamen die Verwendung des umgekehrten Schrägstrichs (\). Wenn Sie einen umgekehrten Schrägstrich in einem Labelnamen verwenden müssen, fügen Sie einen zweiten umgekehrten Schrägstrich hinzu (\\), damit er nicht als Befehl interpretiert wird.
5. Klicken Sie auf **Label hinzufügen**.
6. So weisen Sie ein vorhandenes Label zu:
   a. Aktivieren Sie das Kontrollkästchen neben einem oder mehreren Geräten.
   b. Wählen Sie **Aktion auswählen** > **Labels zuweisen**.
   c. Ziehen Sie Labels in das Feld *Diese Labels übernehmen* und klicken Sie anschließend auf **Labels zuweisen**.

      Das Label wird neben dem Gerätenamen in der Liste *Geräte* angezeigt.
7. So können Sie ein manuelles Label entfernen:
   a. Aktivieren Sie das Kontrollkästchen neben einem oder mehreren Geräten.

b. Wählen Sie **Aktion auswählen** > **Label entfernen** > **Label_Name** aus.

Das Label wird von den Geräten entfernt.

Smart Labels für Geräte verwenden

Verwenden Sie Smart Labels, um Geräte automatisch auf der Grundlage bestimmter Kriterien zu suchen und mit einem Label zu versehen.

Wenn Sie zum Beispiel Notebooks in einer bestimmten Niederlassung nachverfolgen möchten, können Sie ein Label mit der Bezeichnung "Niederlassung in San Francisco" und dann ein Smart Label auf Basis des IP-Adressbereichs oder des Subnetzes für Geräte erstellen, die sich in der Niederlassung in San Francisco befinden. Bei jeder Inventarisierung eines Geräts aus dem IP-Adressbereich wird automatisch das Smart Label "Büro San Francisco" zugewiesen. Wenn das Gerät den IP-Adressbereich verlässt und danach erneut inventarisiert wird, wird das Label automatisch entfernt.

Smart Labels werden auf verwaltete Geräte angewendet bzw. entfernt, wenn die Geräte eine Verbindung mit der Appliance herstellen. Wenn Sie also ein Smart Label erstellen, das die Erfassung der Nutzung auf Geräten ermöglicht, kann es einige Zeit dauern, bis das Smart Label auf die Geräte angewendet wird und die Geräte mit der Meldung von Erfassungsinformationen beginnen. Die Erfassung der Nutzung wird für Geräte, die den Smart Label-Kriterien entsprechen, erst nach der Inventarisierung der Geräte und der Anwendung des Smart Labels aktiviert.

Weitere Informationen hierzu finden Sie unter Verwalten von Smart Labels.

In der folgenden Tabelle sind einige Beispiele für nützliche Smart Labels aufgeführt, die einem Gerät auf Basis seiner Inventarattribute zugewiesen werden können:

Beispiel-Labelname	Beispielkriterien
Win7 wenig Speicherplatz	Windows 7-Geräte mit weniger als 1 GB freiem Speicherplatz
WS2012 ohne 2916993	Windows Server 2012-Geräte ohne Hotfix 2916993
Gebäude 3	Geräte mit einem IP-Adressbereich mit Ursprung in Gebäude 3
CN Sales	Geräte, deren Name das Wort **Sales** enthält

Aktionen auf Geräten ausführen

Mit Geräteaktionen können Sie Aktionen auf Geräten per Remotezugriff ausführen (vorausgesetzt, auf den Remotegeräten sind die entsprechenden Programme installiert).

Sie haben auswählbare Geräteaktionen erstellt. Informationen zum Hinzufügen oder Bearbeiten von Geräteaktionen finden Sie unter Allgemeine Appliance-Einstellungen ohne aktivierte Organisationskomponente konfigurieren.

HINWEIS: Diese Funktion wird nur auf Windows-Geräten unterstützt. Auf dem Windows-Gerät, auf dem die Geräteaktion ausgeführt wird, muss der KACE Agent ab Version 9.0 installiert und verbunden sein.

HINWEIS: Wenn Sie das Gerät über den Agenten initiieren, muss die ausführbare Datei für die Aktion hier platziert werden: `%PATH%`. Der Agent ist 32-Bit, also verwenden Sie auf 64-Bit-Windows-Geräten `%windir%/System32` als Alias für das Verzeichnis `%windir%/Wow64`. Wenn Sie ein Programm ausführen müssen, das sich im Verzeichnis `%windir%/System32` auf einem 64-Bit-Windows-System befindet, müssen Sie das virtuelle Verzeichnis `%windir%/SysNative` verwenden. Sie können entweder `%windir%/SysNative` zu Ihrer Umgebungsvariable `%PATH%` hinzufügen oder einen vollqualifizierten Pfad angeben, indem Sie bei der Definition Ihrer Geräteaktion `%windir%/SysNative` Ihrer ausführbaren Datei voranstellen.

1. Rufen Sie die Seite *Gerätedetail* für ein Gerät auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Inventar** und anschließend auf **Geräte**.
   c. In der Liste *Geräte* wählen Sie in der Zeile, die das erforderliche Gerät enthält das Kontrollkästchen.
2. Wählen Sie in der Dropdown-Liste *Aktionen* eine Aktion aus.

   HINWEIS: Wurden keine Geräteaktionen erstellt, wird die Dropdown-Liste *Aktionen* nicht angezeigt.

   TIPP: Durch das Zuweisen eines Geräts zu einem Benutzer (**Aktion Wählen > Zuweisen zu**) werden alle zugewiesenen Geräte für den gewählten Benutzer auf der Seite *Meine Geräte* in der **Benutzerkonsole** angezeigt. Wenn der Benutzer versucht, Software herunterzuladen und zu installieren, kann er ein Zielgerät aussuchen wie erforderlich.

Manuell hinzugefügte Geräte anzeigen

Geräte, die manuell hinzugefügt wurden, werden auf der Liste *Geräte* zusammen mit anderen verwalteten Geräten angezeigt. Mit der erweiterten Suche können Sie die Liste *Geräte* filtern, sodass nur noch manuell hinzugefügte Geräte angezeigt werden.

1. Rufen Sie die Liste *Geräte* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Inventar** und anschließend auf **Geräte**.
2. So filtern Sie die Liste so, dass nur noch manuell hinzugefügte Geräte angezeigt werden:
   a. Klicken Sie oberhalb der Liste auf der rechten Seite auf die Registerkarte **Erweiterte Suche**, um den Bereich *Erweiterte Suche* anzuzeigen.
   b. Legen Sie die erforderlichen Kriterien fest, um Geräte zu finden, die manuell hinzugefügt wurden:

Option	Kriterien
Feldname	Identitätsinformationen des Geräts: Inventartyp
Operator	ist

Option	Kriterien
Wert	Wählen Sie eine der folgenden Möglichkeiten: • **WSAPI-Agent**: Inventar, das über die API hochgeladen wurde • **XML-Import**: Inventar, das auf der Seite *Softwaredetails* hochgeladen wurde.

c. Klicken Sie auf **Suchen**.

Manuell hinzugefügte Geräte werden angezeigt.

Geräte aus dem Inventar löschen

Nicht verwendete oder veraltete Geräte können manuell aus dem Inventar gelöscht werden. Dadurch verhindern Sie, dass die Geräte auf die Anzahl der Geräte angerechnet werden, die Sie gemäß Ihrer Quest KACE Lizenz verwalten dürfen.

1. Rufen Sie die Liste *Geräte* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Inventar** und anschließend auf **Geräte**.
2. Aktivieren Sie das Kontrollkästchen neben einem oder mehreren Geräten.
3. Wählen Sie **Aktion auswählen** > **Löschen** und klicken Sie dann zum Bestätigen auf **Ja**.

Registrieren des KACE Agent bei der Appliance

Die Appliance verwendet einen Registrierungsprozess, um den unbefugten Zugriff auf ihre Ressourcen zu verhindern. Nur authentifizierte KACE Agenten können eine erfolgreiche Verbindung herstellen.

Alle Agenten, die versuchen, eine Verbindung zur Appliance herzustellen, werden in eine Quarantäneliste gesetzt. Wenn ein Agent über ein gültiges Token verfügt, authentifiziert die Appliance den Agent und gewährt automatisch Zugriff auf die Appliance. Agenten, die kein Token haben, bleiben in Quarantäne, bis ein Systemadministrator ihre Verbindungsanforderung genehmigt.

Sie können Agent-Token erstellen und verwalten sowie Anforderungen von Agenten in Quarantäne verwalten, um eine Verbindung zur Appliance herzustellen.

Verwalten von KACE Agent-Token

KACE Agent-Token ermöglichen der Appliance die Authentifizierung und Registrierung von Agenten, sodass sie auf die Appliance-Ressourcen zugreifen können.

Jedes Token kann einem oder mehreren Agenten zugeordnet werden. Verwenden Sie die Seite *Agent Token Detail (Details zu Agent-Token)*, um Agent-Token zu erstellen oder zu ändern. Auf dieser Seite werden auch alle Geräte identifiziert, die ein bestimmtes Token für die Verbindung mit der Appliance verwendet haben. Zudem können Sie die Agent-Installationsprogramme herunterladen, die das ausgewählte Token enthalten.

Alle Agenten, die über kein gültiges Token verfügen, müssen vom Appliance-Administrator genehmigt werden, damit eine erfolgreiche Verbindung hergestellt werden kann. Weitere Informationen hierzu finden Sie unter In Quarantäne befindliche KACE Agenten überprüfen.

1. Führen Sie einen der folgenden Schritte aus:
   - **Melden Sie sich bei der Administratorkonsole der Appliance an: `https://appliance_hostname/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option** *Organisationsmenü in Verwaltungskopfzeile anzeigen* **aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.**
   - **Melden Sie sich bei der Systemadministratorkonsole der Appliance an: `https://appliance_hostname/system`. Oder wählen Sie in der Dropdown-Liste rechts oben auf der Seite den Eintrag System aus.**

   Die Seite *Dashboard* oder *System-Dashboard* wird angezeigt.
2. Rufen Sie die Seite *Agent Token Detail (Details zum Agent-Token)* auf:
   a. Klicken Sie in der linken Navigationsleiste auf **Einstellungen** und anschließend auf **Agent-Token**.

   Die Seite *Agent Tokens (Agent-Token)* wird angezeigt und enthält eine Liste aller Agent-Token. Für jedes Token werden ein Token-Status, der Name des Benutzers, der es erstellt hat, das Ablaufdatum (falls zutreffend), wie oft das Token zum Registrieren eines Agent-Geräts bei der Appliance verwendet wird, und das Nutzungslimit (falls zutreffend) angezeigt.
3. Führen Sie auf der Seite mit den *Agent-Token* einen der folgenden Schritte aus:
   - **Klicken Sie zum Erstellen eines neuen Agent-Tokens auf Aktion auswählen > Neu.**

     TIPP: Um Token zu löschen oder zu widerrufen, wählen Sie sie in der Liste aus, und verwenden Sie die entsprechenden Befehle aus dem Menü **Aktion auswählen**. Sie können diese Aktion auch auf der Seite *Agent Token Detail (Details zum Agent-Token)* ausführen.
   - **Um ein vorhandenes Agent-Token zu bearbeiten, klicken Sie in der Liste auf den Token-Namen.**
4. Geben Sie auf der Seite *Agent Token Detail (Details zum Agent-Token)*, die unter *Konfigurieren* angezeigt wird, die folgenden Informationen ein:

Option	Beschreibung
Name	Der Name des Agent-Tokens. Wählen Sie einen Namen aus, den Sie leicht erkennen und einem bestimmten Agenten, einer Plattform oder einem bestimmten Zweck zuordnen können.
Gültig bis	Wenn dieses Token für eine begrenzte Zeit gültig sein soll, wählen Sie **Enable Expiration (Ablauf aktivieren)** aus, und geben Sie das Ablaufdatum und die Uhrzeit nach Bedarf an. Um das angegebene Datum und die angegebene Uhrzeit zu ändern, klicken Sie auf **Löschen**, und geben Sie das neue Ablaufdatum ein.
Organisation	Der Name der Organisation, die dieses Token verwendet. Sie können eine bestimmte Organisation oder alle Organisationen auswählen, indem Sie die Option *All Orgs (Alle Organisationen)* aktivieren.

Option	Beschreibung
	HINWEIS: Dieses Feld wird nur angezeigt, wenn Sie die **Systemverwaltungskonsole** verwenden.

5. Wenn Sie angeben möchten, wie oft das Token verwendet werden kann, um einen oder mehrere Agenten bei der Appliance zu registrieren, wählen Sie unter *Use Limit (Verwendungslimit)* die Option **Enable Use Limit (Verwendungslimit aktivieren)** aus, und geben Sie im angezeigten Feld die maximale Verwendungsanzahl an.

   Sofern die Historie eines Agenten nicht aus der Appliance gelöscht wird, registriert sich der Agent nur einmal bei der Appliance, sodass diese Zahl die Gesamtzahl der Anmeldungen eines oder mehrerer Agenten bei der Appliance darstellt.

6. Klicken Sie auf **Speichern**.

   Wenn Sie ein neues Agent-Token erstellt haben, werden auf der Seite zusätzliche Abschnitte angezeigt: *Informationen*, *Agent Token Bundle Installers (Installationsprogramme für Agent-Token)*, *Token Usage by Machines (Token-Nutzung nach Maschinen)* und *Token Usage by Provisioning Schedules (Token-Nutzung nach Provisionierungszeitplänen)*.

7. **Optional**. Schauen Sie sich den Inhalt der folgenden Abschnitte an:

Abschnitt	Beschreibung
Information	Allgemeine Informationen zum Agent-Token, z. B. zum Zeitpunkt der Erstellung, zur letzten Änderung, zum Namen des Benutzers, der es erstellt hat, zum Status und zur Token-Zeichenfolge. Um die Token-Zeichenfolge in die Zwischenablage zu kopieren, klicken Sie im Feld *Token* auf das Symbol. Sie können die Token-Zeichenfolge angeben, während Sie den KACE Agent auf einem Zielgerät installieren. Weitere Informationen zur Agenten-Installation finden Sie unter Manuelle Bereitstellung des KACE Agent.
Agent Token Bundle Installers (Installationsprogramme für Agent-Token)	Links zu Installationsprogrammen des KACE Agent für jedes unterstützte Betriebssystem. Jedes Installationspaket enthält dieses Agent-Token.
Token Usage by Machines (Token-Nutzung nach Maschinen)	Eine Liste der Geräte im Appliance-Inventar, die dieses Agent-Token verwenden, und das Datum und die Uhrzeit, zu der der Geräteadministrator den Zugriff für jedes Gerät genehmigt hat.
Token Usage by Provisioning Schedules (Token-Nutzung nach Provisionierungszeitplänen)	Eine Liste von Provisionierungszeitplänen für dieses Agent-Token. Für jeden Eintrag in der Liste wird der IP-Adressbereich aufgeführt und angegeben, ob der Zeitplan aktiviert ist.

In Quarantäne befindliche KACE Agenten überprüfen

Die Appliance verfolgt alle Agenten, die eine Verbindung zur Appliance anfordern.

In der Standardansicht werden auf der Seite *Quarantäne* nur die Agenten angezeigt, die auf die Registrierung warten. Sie können damit die entsprechenden Agenten überprüfen und registrieren. Um bereits verbundene Agenten anzuzeigen, ändern Sie einfach den Listenfilter.

HINWEIS: Auf der Listenseite *Quarantäne* wird in der Spalte *Zone* jeder Agent als *Intern* oder *Extern* angezeigt. Wenn Sie Ihre Firewall so konfigurieren, dass Port 443 dem Port 52230 der Appliance extern zugeordnet wird, werden Agenten, die über die Firewall eine Verbindung zu Port 443 herstellen, auf dieser Seite als "Extern" angezeigt. Agenten, die sich direkt mit dem Port 443 der Appliance verbinden, werden als "Intern" angezeigt. Diese Funktion ist optional, Sie können sie jedoch verwenden, wenn die Appliance z. B. in einem Umkreisnetzwerk gehostet wird. Weitere Informationen finden Sie unter https://go.kace.com/to/k1000-external-agent-port.

Agenten, die ein gültiges Token enthalten, werden automatisch verbunden. Weitere Informationen zu diesen Token finden Sie unter Verwalten von KACE Agent-Token.

1. Führen Sie eine der folgenden Aktionen aus, um die Liste *Quarantäne* aufzurufen:

   - **Wenn für Ihre Appliance die Organisationskomponente aktiviert ist, können Sie folgendermaßen auf eine Quarantäneliste auf Systemebene zugreifen:**

     Melden Sie sich bei der Systemadministratorkonsole der Appliance an: `https://`**appliance_hostname**`/system`. Oder wählen Sie in der Dropdown-Liste rechts oben auf der Seite den Eintrag **System** aus. Wählen Sie anschließend **Organisationen** > **Quarantäne**. Eine Quarantäneliste auf Systemebene enthält die Agenten, die allen von der Appliance verwalteten Organisationen zugeordnet sind.

   - **Wenn die Organisationskomponente nicht für die Appliance aktiviert ist oder Sie auf eine Quarantäneliste auf Organisationsebene zugreifen möchten, melden Sie sich bei der Administratorkonsole der Appliance an: `https://appliance_hostname/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option** *Organisationsmenü in Verwaltungskopfzeile anzeigen* **aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus. Wählen Sie anschließend Inventar > Quarantäne.**

     Eine Quarantäneliste auf Organisationsebene enthält nur die Agenten, die der ausgewählten Organisation zugeordnet sind.

   Die Seite mit der *Quarantäneliste* wird angezeigt. Standardmäßig verwendet die Liste den Filter *Aktion ausstehend*, der nur die Agenten anzeigt, die genehmigt werden müssen. Sie können verschiedene Filter anwenden, um *Alle Elemente* und *Genehmigte* oder *Gesperrte Agenten* anzuzeigen. Wenn Sie die Spalte *Genehmigungsstatus* anzeigen, können Sie sehen, welche Agenten den Status *Genehmigt*, *Blockiert* und *Awaiting Action (Aktion ausstehend)* aufweisen.

2. Überprüfen Sie die Elemente in der Liste, und genehmigen Sie alle Agenten wie erforderlich.

   Um einen oder mehrere Agenten zu genehmigen, wählen Sie sie in der Liste aus, und klicken Sie auf **Aktion wählen** > **Genehmigen**. Sie können Agenten nach Bedarf auch sperren oder löschen. Durch das Sperren eines Agenten in Quarantäne wird dieser nur aus der Ansicht *Awaiting Action (Aktion ausstehend)* auf der Seite *Quarantäne* entfernt. Sie können einen Agenten, den Sie nicht zulassen möchten, generell sperren. Wenn Sie einen gesperrten Agenten aus allen Ansichten entfernen möchten, können Sie ihn löschen. Ein gesperrter Agent wird erneut in der Ansicht *Awaiting Action (Aktion ausstehend)* angezeigt, wenn er den Verbindungsversuch wiederholt. Wenn Sie zum Beispiel einen verdächtigen Hostnamen von einem externen Agenten sehen, können Sie diesen Agenten entweder sperren oder löschen. Der Status "Gesperrt" ist als permanente Liste blockierter Geräte gedacht, die aus der Ansicht "Awaiting Action" (Aktion ausstehend) ausgeblendet bleiben und die zu keinem Zeitpunkt genehmigt werden sollen.

3. Um mehr über einen unter Quarantäne stehenden Agenten zu erfahren:

   a. Klicken Sie in der Liste auf den Namen des Agenten.

   b. Prüfen Sie auf der Seite *Quarantine Detail (Quarantänedetails)* die Agenten-Details:

   Auf dieser Seite werden die Details zum ausgewählten KACE Agent angezeigt, z. B. der Name des Geräts, auf dem der Agent installiert ist, die MAC-Adresse des Geräts usw. Wenn der Agent ein Token verwendet hat, um eine Verbindung mit der Appliance herzustellen, wird der Token-Name auf der Seite angezeigt. Auf dieser Seite können Sie auch Agenten genehmigen, blockieren oder löschen.

c. Klicken Sie abschließend auf **Abbrechen**.

4. **System-level Agents only (Nur Agenten auf Systemebene)**. Wenn Sie einen Agenten auf Systemebene mit einer bestimmten Organisation verknüpfen möchten, wählen Sie ihn in der Liste aus, und klicken Sie auf **Aktion auswählen** > **Assign to Organization (Organisation zuweisen)** > **<***Organisationsname***>**

   Der ausgewählte Agent-Datensatz wird jetzt auf der *Quarantäneliste* der Organisation angezeigt, sodass der Administrator des Unternehmens diesen Agent ggf. überprüfen und registrieren kann. Wenn ein Agent genehmigt wird, ohne einer Organisation zugewiesen zu werden, kann der Agent nach der ersten Inventarisierung einer Organisation mithilfe von Organisationsfiltern zugewiesen werden.

Provisionierung des KACE Agent

Bei der Agenten-Provisionierung wird der KACE Agent auf Geräten installiert, die Sie mithilfe des Agenten dem Appliance-Inventar hinzufügen möchten.

Informationen zum KACE Agent

Der KACE Agent ist eine Anwendung, die auf Geräten installiert werden kann, um Inventarberichte und andere Geräteverwaltungsfunktionen nutzen zu können.

Auf verwalteten Geräten installierte Agenten kommunizieren über das Agenten-Messaging-Protokoll mit der Appliance. Agenten führen geplante Aufgaben durch, beispielsweise das Erfassen von Inventarinformationen auf verwalteten Geräten und das Verteilen von Software an verwaltete Geräte. Die Kommunikation zwischen einem Agenten und der Appliance erfolgt über einen proprietären KACE Tunnel, der mithilfe des TLS 1.3-Protokolls verschlüsselt wird. Der Agent sendet und empfängt unverschlüsselte Daten über den TLS 1.3-verschlüsselten KACE Tunnel.

Die Verwaltung ohne Agent ist für Geräte verfügbar, auf denen die Agentensoftware nicht installiert werden kann (wie etwa Drucker oder Geräte mit nicht unterstütztem Betriebssystem). Siehe Verwenden der Verwaltung ohne Agent.

Nachverfolgen von Änderungen der Agenteneinstellungen

Wenn Verlaufsabonnements zur Aufbewahrung von Informationen konfiguriert wurden, können Sie Details zu den an Einstellungen, Assets und Objekten vorgenommenen Änderungen anzeigen.

Diese Informationen beinhalten auch das Datum der Änderung und den Benutzer, der diese vorgenommen hat. Dies kann bei der Fehlerbehebung nützlich sein. Siehe Informationen zu den Verlaufseinstellungen.

Provisionierungsmethoden für den KACE Agent

Sie können den KACE Agent auf unterschiedliche Weise auf den zu verwaltenden Geräten bereitstellen.

- **Provisionieren mithilfe des Assistenten für die Agenten-Provisionierung**: Mit dem Assistenten für die Agenten-Provisionierung können Sie den Agenten auf Geräten unter Windows, Mac OS X und Linux provisionieren. Im Assistenten können Sie wählen, ob Sie den Agenten mithilfe des Tools für die Gruppenrichtlinienobjekt-Provisionierung auf Windows-Geräten bereitstellen oder ob Sie die integrierte Provisionierung verwenden möchten, um den Agenten auf Geräten unter Windows, Mac OS X oder Linux bereitzustellen.

  Bei Windows-Geräten empfiehlt sich die Verwendung des Tools für die Gruppenrichtlinienobjekt-Agenten-Provisionierung, da sich dadurch der Aufwand für die vorbereitende Konfiguration des Zielgeräts verringert. Das Tool benötigt eine Active Directory-Umgebung. Bei der integrierten Provisionierung müssen Sie die zu verwaltenden Geräte vor der Provisionierung clientseitig konfigurieren.

- **Provisionieren mithilfe der manuellen Bereitstellung**: Die manuelle Bereitstellung ist hilfreich, wenn die automatisierte Agenten-Provisionierung nicht praktikabel ist oder Sie den KACE Agent per E-Mail oder mithilfe von Anmeldeskripten bereitstellen möchten.

Verwandte Themen

KACE Agent mithilfe des Tools für die Gruppenrichtlinienobjekt-Agenten-Provisionierung für Windows Geräte bereitstellen

KACE Agent mithilfe der integrierten Provisionierung bereitstellen

Manuelle Bereitstellung des KACE Agent

Dateifreigabe aktivieren

Zur Provisionierung von Agentensoftware müssen Sie die Dateifreigabe aktivieren.

Wenn die Organisationskomponente auf Ihrer Appliance aktiviert ist, finden Sie weitere Informationen unter Dateifreigabe auf Systemebene aktivieren. Andernfalls finden Sie weitere Informationen unter Dateifreigabe ohne aktivierte Organisationskomponente aktivieren.

Dateifreigabe auf Systemebene aktivieren

Wenn auf Ihrer Appliance die Organisationskomponente aktiviert ist, müssen Sie zur Bereitstellung des Agenten die Dateifreigabe auf Systemebene aktivieren.

HINWEIS: Wenn die Organisationskomponente auf Ihrer Appliance nicht aktiviert ist, befolgen Sie die Anweisungen in Dateifreigabe ohne aktivierte Organisationskomponente aktivieren.

1. Rufen Sie die Seite *Sicherheitseinstellungen* auf:
   a. Melden Sie sich bei der Systemadministratorkonsole der Appliance an: `http://`**appliance_hostname**`/system`. Oder wählen Sie in der Dropdown-Liste rechts oben auf der Seite den Eintrag **System** aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Einstellungen** und anschließend auf **Systemsteuerung**.
   c. Klicken Sie in der *Systemsteuerung* auf **Sicherheitseinstellungen**.
2. Geben Sie im Abschnitt *Samba* folgende Einstellungen an:

Option	Beschreibung
Für Appliances mit aktivierter Organisationskomponente: **Dateifreigaben in Organisation aktivieren**	Verwenden Sie die Client-Freigabe der Appliance, um Dateien zu speichern (beispielsweise zur Anwendungsinstallation auf verwalteten Geräten). Bei der Client-Freigabe der Appliance handelt es sich um einen integrierten Windows Dateiserver, den der Provisionierungsdienst verwenden kann, um die Verteilung des Samba Clients in Ihrem Netzwerk zu unterstützen. Quest empfiehlt, diesen Dateiserver nur zu aktivieren, wenn Sie Anwendungsinstallationen auf verwalteten Geräten ausführen.
NTLMv2-Authentifizierung für Dateifreigaben der Appliance erforderlich	Aktivieren Sie die NTLMv2-Authentifizierung für die Appliance-Dateifreigaben. Wenn diese Einstellung aktiviert ist, müssen verwaltete Geräte, die eine Verbindung mit den Appliance-Dateifreigaben herstellen, NTLMv2 unterstützen und sich bei der Appliance mithilfe von NTLMv2 authentifizieren. Obwohl NTLMv2 sicherer ist als NTLM und LANMAN, sind Konfigurationen ohne NTLMv2 häufiger und diese Option ist in der Regel deaktiviert. Wenn Sie diese Option aktivieren, werden **lanman auth** und **ntlm auth** auf dem Samba Server deaktiviert. NTLMv2 Level 1 – 4 werden unterstützt. Falls Sie NTLM v2 Level 5 benötigen, sollten Sie in Erwägung ziehen, den

Option	Beschreibung
	KACE Agenten manuell bereitzustellen. Siehe Manuelle Bereitstellung des KACE Agent.
NTLMv2 für Offboard-Dateifreigaben erforderlich	Erzwingt, dass einige Funktionen der Appliance, die durch den Samba-Client unterstützt werden (z. B. die Agenten-Provisionierung), mithilfe von NTLMv2 bei den Offboard-Netzwerkdateifreigaben authentifiziert werden müssen. Obwohl NTLMv2 sicherer ist als NTLM und LANMAN, sind Konfigurationen ohne NTLMv2 häufiger und diese Option ist in der Regel deaktiviert. Wenn Sie diese Option aktivieren, wird die Option **client ntlmv2 auth** für Samba Client-Funktionen aktiviert.

3. Klicken Sie auf **Speichern**.
4. Starten Sie die Appliance neu, wenn Sie dazu aufgefordert werden.

Aktivieren Sie beim Neustart der Appliance die Dateifreigabe auf Organisationsebene. Siehe Dateifreigabe auf Organisationsebene mit aktivierter Organisationskomponente aktivieren.

Dateifreigabe auf Organisationsebene mit aktivierter Organisationskomponente aktivieren

Wenn auf Ihrer Appliance die Organisationskomponente aktiviert ist, müssen Sie zur Bereitstellung des Agenten die Dateifreigabe auf Organisationsebene aktivieren.

Überprüfen Sie, ob Organisations-Dateifreigaben aktiviert sind. Anleitungen dazu finden Sie unter Dateifreigabe auf Systemebene aktivieren.

1. Rufen Sie die Seite *Allgemeine Einstellungen* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Einstellungen** und anschließend auf **Systemsteuerung**.
   c. Klicken Sie in der *Systemsteuerung* auf **Allgemeine Einstellungen**.
2. Wählen Sie im Abschnitt *Samba Freigabeeinstellungen* die Option **Dateifreigabe aktivieren** aus.

   Ist die Dateifreigabe deaktiviert, müssen Sie sie auf Systemebene aktivieren. Siehe Sicherheitseinstellungen für die Appliance konfigurieren.
3. **Optional**: Geben Sie ein Kennwort für die Dateifreigabe durch Benutzer ein.
4. Klicken Sie auf **Samba Einstellungen speichern**.
5. Starten Sie die Appliance neu, wenn Sie dazu aufgefordert werden.
6. Wenn Sie mehrere Organisationen haben, wiederholen Sie die oben aufgeführten Schritte für jede Organisation.

Dateifreigabe ohne aktivierte Organisationskomponente aktivieren

Wenn die Organisationskomponente auf Ihrer Appliance nicht aktiviert ist, müssen Sie zur Bereitstellung des Agenten die Dateifreigabe in den Sicherheitseinstellungen der Appliance aktivieren.

1. Rufen Sie die Seite *Sicherheitseinstellungen* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen*

aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.

b. Klicken Sie in der linken Navigationsleiste auf **Einstellungen** und anschließend auf **Systemsteuerung**.

c. Klicken Sie in der *Systemsteuerung* auf **Sicherheitseinstellungen**.

2. Aktivieren Sie im Bereich *Samba* das Kontrollkästchen **Dateifreigabe aktivieren**.
3. **Optional**: Wählen Sie Authentifizierungsoptionen aus:

Option	Beschreibung
NTLMv2 zur Authentifizierung von Dateifreigaben der Appliance erforderlich	Aktivieren Sie die NTLMv2-Authentifizierung für die Appliance-Dateifreigaben. Wenn diese Einstellung aktiviert ist, müssen verwaltete Geräte, die eine Verbindung mit den Appliance-Dateifreigaben herstellen, NTLMv2 unterstützen und sich bei der Appliance mithilfe von NTLMv2 authentifizieren. Obwohl NTLMv2 sicherer ist als NTLM und LANMAN, sind Konfigurationen ohne NTLMv2 häufiger und diese Option ist in der Regel deaktiviert. Wenn Sie diese Option aktivieren, werden **lanman auth** und **ntlm auth** auf dem Samba Server deaktiviert. NTLMv2 Level 1 – 4 werden unterstützt. Falls Sie NTLM v2 Level 5 benötigen, sollten Sie in Erwägung ziehen, den KACE Agenten manuell bereitzustellen. Siehe Manuelle Bereitstellung des KACE Agent.
NTLMv2-Authentifizierung für Offboard-Dateifreigaben erforderlich	Erzwingt, dass einige Funktionen der Appliance, die durch den Samba-Client unterstützt werden (z. B. die Agenten-Provisionierung), mithilfe von NTLMv2 bei den Offboard-Netzwerkdateifreigaben authentifiziert werden müssen. Obwohl NTLMv2 sicherer ist als NTLM und LANMAN, sind Konfigurationen ohne NTLMv2 häufiger und diese Option ist in der Regel deaktiviert. Wenn Sie diese Option aktivieren, wird die Option **client ntlmv2 auth** für Samba Client-Funktionen aktiviert.

4. Klicken Sie auf **Speichern**.
5. Starten Sie die Appliance neu, wenn Sie dazu aufgefordert werden.

KACE Agent mithilfe des Tools für die Gruppenrichtlinienobjekt-Agenten-Provisionierung für Windows Geräte bereitstellen

Bei Windows-Geräten empfiehlt Quest die Verwendung des Tools für die Gruppenrichtlinienobjekt-Agenten-Provisionierung, da sich dadurch der Aufwand für die vorbereitende Konfiguration der Zielgeräte verringert.

Das Gruppenrichtlinienobjekt-Provisionierungstool nutzt Active Directory® und Gruppenrichtlinien, um die Installationseinstellungen zu verteilen und die Agenteninstallation auszuführen. Das Tool erstellt ein Gruppenrichtlinienobjekt oder ändert ein bereits vorhandenes, um den KACE Agent zu installieren, wenn sich ein Gerät über Active Directory authentifiziert.

Wenn ein Zielgerät die Gruppenrichtlinie nach Abschluss des Erstellungs- oder Änderungsprozesses erstmals aktualisiert, wird auf den Geräten, von denen dieses Gruppenrichtlinienobjekt angewendet wird, eine neue clientseitige Gruppenrichtlinienerweiterungs-DLL registriert. Bei der nächsten Aktualisierung der Gruppenrichtlinie

durch das Gerät löst Windows dann die neu registrierte clientseitige Erweiterung aus, um den KACE Windows Agent zu installieren.

Den Artikel der Quest Knowledge Base mit dem Link zum Herunterladen des Tools für die Gruppenrichtlinienobjekt-Provisionierung finden Sie unter https://support.quest.com/kb/133776.

Agentenbereitstellung mithilfe des Tools für die Gruppenrichtlinienobjekt-Agenten-Provisionierung vorbereiten

Damit Sie Agenten mithilfe des Tools für die Gruppenrichtlinienobjekt-Agenten-Provisionierung auf Windows-Geräten bereitstellen können, müssen Sie zunächst sicherstellen, dass das System ordnungsgemäß konfiguriert ist.

Die Verwendung des Tools für die Gruppenrichtlinienobjekt-Agenten-Provisionierung setzt die Erfüllung folgender Systemanforderungen voraus:

- **Ab Windows Vista**: Mit den **Remoteserver-Verwaltungstools** (Remote Server Administration Tools, RSAT) können IT-Administratoren Rollen und Features von Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 oder Windows Server 2012 R2 remote über einen Computer unter Windows 8.1, Windows 8, Windows 7 oder Windows Vista verwalten.

  Weitere Informationen finden Sie unter http://social.technet.microsoft.com/wiki/contents/articles/2202.remote-server-administration-tools-rsat-for-windows-client-and-windows-server-dsforum2wiki.aspx.

- **.NET Framework 3.5**.
- **Windows Server 2012 oder höher Active Directory-Funktionsebene**.
- **Distributionsfreigabe**. Verwenden Sie eine Freigabe, auf die alle Zugriff haben. Legen Sie die `.msi`-Datei beispielsweise nicht auf der NETLOGON-Freigabe ab, da nicht jeder Benutzer auf diese Freigabe zugreifen kann, was schließlich dazu führt, dass die Aktualisierung nicht erfolgreich ist. Als Speicherort muss eine dauerhaft zugängliche Freigabe gewählt werden. Das Installationsprogramm ist eine MSI-Datei (Microsoft Installer). Zum Deinstallieren oder Aktualisieren der Software benötigt MSI Zugriff auf die `.msi`-Datei. Andernfalls kann `msiexec` nicht deinstalliert werden.

KACE Agent mithilfe des GPO Tools für die Gruppenrichtlinienobjekt-Provisionierung bereitstellen

Sie können den KACE Agent mithilfe des GPO Tools für die Gruppenrichtlinienobjekt-Provisionierung auf mehreren Geräten installieren. Dabei beginnen Sie mit dem Assistenten für die Agenten-Provisionierung. Mit dieser Methode sind Provisionierungen für Windows Geräte möglich.

- Sie verfügen über eine Active Directory-Umgebung.
- Sie besitzen die erforderlichen Zugriffsberechtigungen zum Einrichten von Softwareinstallationen.
- Die unter Agentenbereitstellung mithilfe des Tools für die Gruppenrichtlinienobjekt-Agenten-Provisionierung vorbereiten aufgeführten Systemanforderungen werden erfüllt.

Bei dieser Aufgabe arbeiten Sie zunächst in der Windows Gruppenrichtlinien-Verwaltungskonsole oder in der Windows Verwaltung (mit dem GPO Tool für die Gruppenrichtlinienobjekt-Provisionierung) und wenden sich dann wieder der Appliance zu.

1. Rufen Sie den Assistenten für die Agenten-Provisionierung auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie auf der linken Navigationsleiste auf **Einstellungen** und anschließend auf **Provisionierung**.
   c. Klicken Sie im Bereich *Provisionierung* auf **Assistent für die Agenten-Provisionierung**.

Die Seite *Assistent für die Agenten-Provisionierung: Schritt 1 von 3* wird angezeigt.

2. Aktivieren Sie das Kontrollkästchen für *Provisionierung mithilfe der Windows Gruppenrichtlinie (empfohlen)* und klicken Sie anschließend auf **Weiter**, um die Seite *Assistent für die Agenten-Provisionierung: Schritt 2 von 3* anzuzeigen.
3. Klicken Sie auf den Link zum Knowledge Base-Artikel über die Agentenbereitstellung mithilfe des Appliance-GPO-Tools für die Gruppenrichtlinienobjekt-Agenten-Provisionierung unter https://support.quest.com/kb/133776.

   Der Knowledge Base-Artikel enthält einen Download-Link für die MSI-Datei des Tools für die Gruppenrichtlinienobjekt-Agenten-Provisionierung.

   Zum Installieren und Starten des Tools müssen Sie die Oberfläche der Appliance verlassen.
4. Laden Sie die MSI-Datei herunter und führen Sie sie aus, um das Tool zu installieren.
5. Starten Sie das installierte Tool über das Startmenü.

   Der Bereitstellungs-Assistent führt Sie durch die Schritte zum Konfigurieren und Anwenden eines Gruppenrichtlinienobjekts für die Softwarebereitstellung. Der Assistent verwendet nach Möglichkeit Standardwerte, um den Konfigurationsaufwand gering zu halten.

   HINWEIS: Im Tool werden nur Gruppenrichtlinienobjekte angezeigt, zu deren **Bearbeitung** Sie berechtigt sind.
6. Kehren Sie zur Seite *Agenten-Provisionierung: Schritt 2 von 3* der Appliance zurück, wenn Sie alle Arbeiten mit dem Tool erledigt haben, und klicken Sie auf **Weiter**.
7. Klicken Sie auf **Fertig stellen** auf der Seite *Agenten-Provisionierung: Schritt 3 von 3* anzuzeigen.

Agenten werden auf den Clientgeräten installiert, wenn die Gruppenrichtlinie auf diesen Geräten aktualisiert wurde. Abhängig von der Umgebung findet die Installation entweder beim Neustart des Geräts oder nach einem 90-minütigen Aktualisierungszyklus für die Gruppenrichtlinie statt.

Rufen Sie die Seite *Geräte* auf, um den Fortschritt der Geräte zu überwachen, auf denen der Agent installiert und eingecheckt wird.

KACE Agent mithilfe der integrierten Provisionierung bereitstellen

Sie können den KACE Agent auf mehreren Geräten installieren, indem Sie einen IP-Adressbereich als Ziel für die Bereitstellung konfigurieren (integrierte Provisionierung). Als Ziel für die integrierte Provisionierung können Geräte unter Windows, Mac OS X oder Linux verwendet werden.

Nach der Vorbereitung der einzelnen Clientzielgeräte verwenden Sie den Assistenten für die Agenten-Provisionierung der Appliance, um die Geräte zu ermitteln und einen Provisionierungszeitplan einzurichten.

Installation des KACE Agent vorbereiten

Damit Sie den KACE Agent mithilfe der integrierten Provisionierung auf Geräten installieren können, müssen Sie zunächst die Systemanforderungen überprüfen, die Dateifreigabe aktivieren und die Geräte vorbereiten.

Informationen zur Dateifreigabe finden Sie unter Dateifreigabe aktivieren.

Systemanforderungen für die Installation des KACE Agent überprüfen

Vergewissern Sie sich, dass der Zugriff auf die erforderlichen Ports möglich ist und das Gerät die Systemanforderungen erfüllt, bevor Sie den KACE Agent auf Geräten installieren.

Verwaltete Geräte müssen die folgenden Systemanforderungen erfüllen und Zugriff auf die erforderlichen Ports besitzen:

- Weitere Informationen finden Sie in den *technischen Spezifikationen* auf der Produktdokumentation-Seite: https://support.quest.com/kace-systems-management-appliance/technical-documents.
- Siehe Überprüfen von Port-Einstellungen, NTP-Dienst und Website-Zugriff.

Windows Geräte für die Agenteninstallation vorbereiten

Damit Sie den KACE Agent auf Windows-Geräten installieren können, müssen Sie zunächst die Dateifreigabe und die Benutzerkontensteuerung korrekt konfigurieren.

- **Gerät unter Windows Vista™, Windows 7 oder Windows 8 vorbereiten**

  Geben Sie Administratoranmeldedaten für alle Geräte an. Zur Installation des KACE Agent auf mehreren Geräten müssen die Administratoranmeldedaten für alle Geräte dieselben sein.

  Führen Sie einen der folgenden Schritte aus, um die Benutzerkontensteuerung zu konfigurieren:

  - Legen Sie für die Option **Benutzerkontensteuerung: Alle Administratoren im Administratorbestätigungsmodus ausführen** die Einstellung **Deaktiviert** fest. Quest empfiehlt diese Option, da sie mehr Sicherheit bietet und zentral mittels GPO konfiguriert werden kann. Zu dieser Einstellung gelangen Sie, indem Sie im *Suchfeld* des **Start**menüs die Zeichenfolge secpol.msc eingeben, um die **Gruppenrichtlinie** zu öffnen, und dann zu **Lokale Richtlinien** > **Sicherheitsoptionen** navigieren. Starten Sie nach dem Übernehmen der Einstellungen das Gerät neu.
  - Deaktivieren Sie die Benutzerkontensteuerung. Navigieren Sie unter Windows 7 zu **Systemsteuerung** > **System und Sicherheit** > **Wartungscenter** > **Einstellungen der Benutzerkontensteuerung ändern**. Navigieren Sie unter Windows 8 zu **Systemsteuerung** > **System und Sicherheit** > **Verwaltung** > **Lokale Sicherheitsrichtlinie**. Wählen Sie dann in den *Sicherheitsoptionen* im Abschnitt *Lokale Richtlinien* die Option **Deaktiviert** für jedes mit *Benutzerkontensteuerung* gekennzeichnete Element aus.

  Aktivieren Sie auf der Seite *Erweiterte Freigabeeinstellungen* die Netzwerkerkennung und die Datei- und Druckerfreigabe.

- **Windows Firewall vorbereiten**

  Wenn die Windows Firewall aktiviert ist, muss **Datei- und Druckerfreigabe** in der *Ausnahmeliste* der Firewall-Konfiguration aktiviert sein. Anweisungen hierzu finden Sie auf der Website von Microsoft Support.

- **Port-Verfügbarkeit überprüfen**

  Vergewissern Sie sich, dass die Ports 139 und 445 verfügbar sind.

  Vor der Durchführung von Remote-Installationsvorgängen überprüft die Appliance auf allen Zielgeräten, ob die Ports 139 und 445 verfügbar sind.

  HINWEIS: Auf Windows-Geräten sind die Ports 139 und 445 sowie die Datei- und Druckerfreigabe und Administratoranmeldedaten nur während der Installation des Agenten erforderlich. Nach der Installation können Sie den Zugriff auf diese Ports und Dienste gegebenenfalls wieder deaktivieren. Der Agent verwendet für die weitere Kommunikation Port 443.

  HINWEIS: Nach der Installation wird der Agent im Kontext des lokalen Systemkontos ausgeführt. Dies ist ein von Windows Betriebssystemen genutztes integriertes Konto.

KACE Agent auf einem Gerät oder auf mehreren Geräten installieren

Sie können den KACE Agent mithilfe des Assistenten für die Agenten-Provisionierung auf einem einzelnen Gerät oder auf mehreren Geräten installieren. In letzterem Fall müssen Sie als Ziel für die Installation einen IP-Adressbereich angeben. Mit dieser Methode sind Provisionierungen für Windows, Mac und Linux Geräte möglich.

- Sie haben alle Zielgeräte vorbereitet. Siehe Installation des KACE Agent vorbereiten.
- Sie besitzen Informationen für das Administratorkonto, das über die erforderlichen Berechtigungen für die Agenteninstallation auf den Zielgeräten verfügt.

Mit dem Assistenten für die Agenten-Provisionierung können Sie Provisionierungszeitpläne erstellen, um anzugeben, wie und wann der KACE Agent auf Geräten in Ihrem Netzwerk installiert werden soll. Mit der zeitplanbasierten Provisionierung können Sie sicherstellen, dass der Agent auf Geräten innerhalb eines IP-Adressbereichs installiert ist.

Provisionierungszeitpläne konfigurieren die Appliance so, dass sie Geräte in einem bestimmten IP-Adressbereich regelmäßig überprüft und den KACE Agent bei Bedarf installiert, neu installiert oder deinstalliert.

Für die Provisionierung von Windows-Geräten können Sie auch das Tool für die Gruppenrichtlinienobjekt-Provisionierung verwenden. Dadurch verringert sich der Aufwand für die vorbereitende Konfiguration des Zielgeräts. Siehe KACE Agent mithilfe des Tools für die Gruppenrichtlinienobjekt-Agenten-Provisionierung für Windows Geräte bereitstellen.

1. Rufen Sie den Assistenten für die Agenten-Provisionierung auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie auf der linken Navigationsleiste auf **Einstellungen** und anschließend auf **Provisionierung**.
   c. Klicken Sie im Bereich *Provisionierung* auf **Assistent für die Agenten-Provisionierung**.

      Die Seite *Assistent für die Agenten-Provisionierung: Schritt 1 von 3* wird angezeigt.
2. Wählen Sie *Provisionierung unter Verwendung des IP-Bereichs (Windows, Mac, Linux)* aus und klicken Sie auf **Weiter**, um die *Detailseite für den Provisionierungszeitplan* anzuzeigen.
3. Benennen Sie den Zeitplan im Abschnitt *Konfigurieren*, aktivieren Sie die Provisionierung und geben Sie Informationen zur Plattform an:

Option	Beschreibung
Name	Ein eindeutiger Name, der diese Konfiguration identifiziert. Der Name wird auf der Seite *Provisionierungszeitpläne* angezeigt.
Aktiviert	Provisionierungszeitpläne aktivieren. Zeitpläne werden nur ausgeführt, wenn dieses Kontrollkästchen aktiviert ist.
Installieren/Deinstallieren	Gibt an, ob es sich um einen Provisionierungszeitplan für die Installation oder Deinstallation von Agenten handelt.
Agent-Token	Das Token, das der Agent für die Verbindung mit der Appliance verwendet. Wählen Sie ein vorhandenes Agent-Token aus oder fügen Sie ein neues hinzu: a. Wählen Sie *Add Agent Token (Agent-Token hinzufügen)*.

Option	Beschreibung
	b. Geben Sie im Dialogfenster *Add Agent Token (Agent-Token hinzufügen)* die folgenden Informationen an: ◦ **Name**: ◦ **Enable Expiration (Ablauf aktivieren)**: Wenn das Token für eine begrenzte Zeit gültig sein soll, aktivieren Sie dieses Kontrollkästchen, und geben Sie das Ablaufdatum und die Ablaufzeit nach Bedarf an. Um das angegebene Datum und die angegebene Uhrzeit zu ändern, klicken Sie auf **Löschen**, und geben Sie das neue Ablaufdatum ein. ◦ **Enable Use Limit (Verwendungslimit aktivieren)**: Wenn Sie angeben möchten, wie oft das Token verwendet werden kann, um einen oder mehrere Agenten bei der Appliance zu registrieren, aktivieren Sie dieses Kontrollkästchen, und geben Sie im angezeigten Feld die maximale Verwendungsanzahl an. Sofern die Historie eines Agenten nicht aus der Appliance gelöscht wird, registriert sich der Agent nur einmal bei der Appliance, sodass diese Zahl die Gesamtzahl der Anmeldungen eines oder mehrerer Agenten bei der Appliance darstellt. c. Klicken Sie auf **Speichern**. Wenn Sie kein Agent-Token auswählen, verbleibt es bei der ersten Verbindung des Agenten mit der Appliance in der Quarantäneliste, bis der Appliance-Administrator seine Verbindungsanforderung genehmigt. Weitere Informationen hierzu finden Sie unter Registrieren des KACE Agent bei der Appliance.
Anmeldeinformationen	Separate Zeilen für die Anmeldeinformationen werden benötigt, um das Geräte und die auszuführenden Befehle für die jeweilige Plattform zu verbinden, wie es der Zeitplan vorsieht. Die erste Spalte enthält das Betriebssystem. Die zweite Spalte enthält die Agentenversion für die Installation. Die dritte Spalte enthält eine Dropdown-Liste zum Auswählen der vorhandenen Anmeldeinformationen. Sie können **Neue Anmeldeinformationen hinzufügen** auswählen, um nicht bereits aufgeführte Anmeldeinformationen zu ergänzen. Siehe Hinzufügen und Bearbeiten von Benutzer-/Kennwort-Anmeldeinformationen.

4. Geben Sie im Abschnitt *Bereitstellen* die in den Zeitplan einzubeziehenden Geräte an:

Option	Beschreibung
Ziel-IP-Adressen oder Hostnamen	Eine durch Kommas getrennte Liste mit den IP-Adressen oder Hostnamen der Zielgeräte. Verwenden Sie Bindestriche, um einzelne Bereiche von IP-Adressklassen anzugeben. **TIPP:** Die Appliance unterstützt sowohl IPv6- (Internet Protocol Version 6) als auch IPv4-Adressen. Der Link **Hilfe beim Auswählen von Geräten** ermöglicht das Hinzufügen von Geräten zur Liste *Ziel-IP-Adressen oder Hostnamen*: • **Provisionierung des IP-Bereichs**: Verwenden Sie Bindestriche, um einzelne Bereiche von IP-Adressklassen anzugeben. Beispiel: ◦ **IPv6**: fdef:22b9:e8ae:14a9::1a0:f000-f0aa ◦ **IPv4**: 192.168.2-5.1-200 Klicken Sie nach dem Angeben eines Bereichs auf **Alle hinzufügen** • **Geräte aus Erkennung auswählen**: Die Angaben in dieser Dropdown-Liste werden aus den **Erkennungsergebnissen** übernommen. Verwenden Sie das Eingabefeld, um den Inhalt zu filtern. Klicken Sie nach dem Auswählen eines Geräts auf **Alle hinzufügen**.

5. Legen Sie die Ausführungszeit für den Zeitplan fest.

Option	Beschreibung
Kein(e)	Die Ausführung erfolgt im Zusammenhang mit einem Ereignis anstatt zu einem bestimmten Datum oder zu einem bestimmten Zeitpunkt.
jede Stunde	Der Vorgang wird im angegebenen Intervall durchgeführt.
Täglich/an einem bestimmten Tag um HH:MM	Die Erfassung wird täglich zu einem bestimmten Zeitpunkt oder an einem bestimmten Wochentag um eine bestimmte Uhrzeit ausgeführt.
Ausführen am n-ten jedes Monats/eines bestimmten Monats um HH:MM	Die Erfassung wird jeden Monat oder in einem bestimmten Monat an einem festgelegten Datum zu einer festgelegten Uhrzeit ausgeführt.
Ausführen am n-ten Wochentag **jedes Monats/ eines bestimmten Monats um HH:MM**	Die Erfassung wird jeden Monat oder in einem bestimmten Monat an einem festgelegten Wochentag zu einer festgelegten Uhrzeit ausgeführt.

Option	Beschreibung

Benutzerdefiniert	Führen Sie die Erfassung nach einem benutzerdefinierten Zeitplan aus.
	Verwenden Sie das Standard-5-Feld-Cron-Format (das erweiterte Cron-Format wird nicht unterstützt):
	`* * * * *`
	`| | | | +————————Wochentag (0-6) (Sonntag=0)`
	`| | | +————————Monat (1-12)`
	`| | +————————Monatstag (1-31)`
	`| +————————Stunde (0-23)`
	`+————————Minute (0-59)`
	Verwenden Sie bei der Angabe von Werten die folgenden Zeichen:
	• **Leerzeichen( )**: Die einzelnen Felder mit einem Leerzeichen trennen.
	• **Sternchen (*)**: Ein Sternchen repräsentiert den gesamten Wertebereich in einem Feld. Zum Beispiel repräsentiert ein Sternchen im Stundenfeld eine beliebige Stunde.
	• **Kommas (,)**: Mehrere Werte in einem Feld werden mit einem Komma getrennt. Zum Beispiel werden mit `0,6` im Feld „Wochentag“ Sonntag und Samstag angegeben.
	• **Bindestriche (-)**: Mit einem Bindestrich wird ein Wertebereich in einem Feld angegeben. Zum Beispiel entspricht `1-5` im Feld „Wochentag“ `1,2,3,4,5`, d. h. Montag bis Freitag.
	• **Schrägstriche (/)**: Die Angabe der Zeitabstände, mit denen eine Aktion wiederholt werden soll, erfolgt mit einem Schrägstrich. Zum Beispiel entspricht `*/3` im Feld Stunde `0,3,6,9,12,15,18,21`. Das Sternchen (`*`) gibt jede Stunde an, mit `/3` erfolgt aber eine Einschränkung auf durch drei teilbare Stunden.
	Beispiele:
	• `15 * * * * Jeden Tag 15 Minuten nach jeder vollen Stunde ausführen`
	• `0 22 * * * Jeden Tag um 22:00 Uhr ausführen`
	• `0 0 1 1,6 * Am 1. Januar und 1. Juni um 00:00 Uhr ausführen`
	• `30 8,12 * * 1-5 An Wochentagen um 08:30 Uhr und 12:30 Uhr ausführen`
	• `0 2 */2 * * Jeden zweiten Tag um 02:00 Uhr ausführen`

Aufgabenplan anzeigen	Klicken Sie, um den Aufgabenplan anzuzeigen. Im Dialogfeld *Aufgabenplan* wird eine Liste der

Option	Beschreibung
	geplanten Aufgaben angezeigt. Klicken Sie auf eine Aufgabe, um die Aufgabendetails anzuzeigen. Weitere Informationen hierzu finden Sie unter Aufgabenpläne anzeigen.

6. **Optional**: Verwenden Sie die *erweiterten Einstellungen* für Folgendes:
   - Anpassen der Ports, die die Appliance zum Bereitstellen des Agenten verwendet
   - Festlegen einer alternativen Download-Quelle für das Agent-Installationsprogramm

     HINWEIS: Neuere Versionen von MS Windows wie Windows 10 unterstützen das Herunterladen von Dateien von Dateifreigaben nicht, sodass die WinRM-Bereitstellung an einem alternativen Speicherort nicht wie erwartet funktioniert.
   - Geben Sie den WinRM-Port an, der für die Agenten-Provisionierung auf Windows-Geräten verwendet wird. Für diese Zeitpläne, die eine Legacy-Methode zum Bereitstellen von Windows-Geräten verwenden, haben Sie die Möglichkeit, diese in WinRM zu ändern. Weitere Informationen zur WinRM-Konfiguration finden Sie unter https://support.quest.com/kb/260699/agent-provisioning-with-winrm.
   - Wählen Sie die Informationsebene aus, die im Protokoll angezeigt werden soll. Um nur die wichtigsten Meldungen angezeigt zu bekommen, wählen Sie *Kritisch* aus. Um alle Meldungen zu sehen, wählen Sie *Debug* aus. Weitere Optionen sind *Fehler*, *Warnung*, *Hinweis* und *Info*.
   - Geben Sie das Gerät an, das als Relay für die agentenlose Geräteinventarisierung verwendet werden soll. Ein Relay-Gerät, das während der Ermittlung verwendet wird, wenn ein neues Gerät von den Ermittlungsergebnissen automatisch durch ein neues Gerät bereitgestellt wird. Weitere Informationen hierzu finden Sie unter Erkennungszeitplan für die Durchführung eines schnellen „Was und wo“-Scans in Ihrem Netzwerk hinzufügen.
   - Ermöglichen der vollständigen Deinstallation des Agenten. Die Auswahl von *KUID bei der Deinstallation entfernen* führt dazu, dass ein bestehender Agent vom Gerät entfernt wird, bevor der Agent neu installiert wird. In diesem Fall generiert die Appliance eine neue KUID für das Asset, die als neues Gerät in der Appliance angezeigt wird.
7. Klicken Sie auf **Jetzt ausführen**, um die Seite *Provisionierungszeitpläne* und die neue Konfiguration anzuzeigen.

   Die Appliance speichert die Konfiguration unter dem angegebenen Namen und führt die Konfiguration für die Ziel-IP-Adressen aus.

Auf der Seite *Provisionierungszeitpläne* wird der Status erfolgreicher Installationen nach Beginn des Zeitplans angezeigt.

Verwandte Themen

Einschalten der Appliance und Anmelden bei der Administratorkonsole

KACE Agent mithilfe des Tools für die Gruppenrichtlinienobjekt-Agenten-Provisionierung für Windows Geräte bereitstellen

Manuelle Bereitstellung des KACE Agent

Provisionierungszeitpläne verwalten

Um den Installationsvorgang des Agenten zu vereinfachen, können Sie Provisionierungszeitpläne hinzufügen, die angeben, wie und wann der KACE Agent auf Geräten installiert werden soll. Sie können Provisionierungszeitpläne hinzufügen, anzeigen, bearbeiten, ausführen, duplizieren und löschen.

Provisionierungszeitpläne anzeigen, ausführen, bearbeiten oder duplizieren

Auf der Seite *Provisionierungszeitpläne* können Sie den Status von Provisionierungszeitplänen und andere Details anzeigen. Auf dieser Seite können Sie die Provisionierungszeitpläne bei Bedarf auch ausführen und bearbeiten.

Wenn Sie einen Provisionierungszeitplan duplizieren, werden seine Eigenschaften in die neue Konfiguration kopiert. Ähnelt die zu erstellende Konfiguration einer bereits vorhandenen Konfiguration, kann sich dieser Vorgang als schneller erweisen als die Erstellung einer gänzlich neuen Konfiguration.

1. Rufen Sie die Liste *Provisionierungszeitpläne* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie auf der linken Navigationsleiste auf **Einstellungen** und anschließend auf **Provisionierung**.
   c. Klicken Sie im *Provisionierungsbereich* auf **Zeitpläne**.

   Die Liste enthält folgende Spalten:

Option	Beschreibung
Name	Der Name des Provisionierungszeitplans (ist mit der Seite *Detail zum Provisionierungszeitplan* verknüpft).
Zielgerichtet	Die Gesamtzahl der Zielgeräte in der Konfiguration (ist mit der Seite *Provisionierungsergebnisse* verknüpft).
Wird ausgeführt	Die Gesamtzahl der Zielgeräte, auf denen die Provisionierung ausgeführt wird (verknüpft mit der Seite *Provisionierungsergebnisse*).
Ausstehend	Die Gesamtzahl der Zielgeräte, auf denen die Provisionierung noch nicht gestartet wurde (ist mit der Seite *Provisionierungsergebnisse* verknüpft).
Erfolgreich	Die Gesamtzahl der Zielgeräte, auf denen die Provisionierung erfolgreich abgeschlossen wurde (ist mit der Seite *Provisionierungsergebnisse* verknüpft).
Fehler	Die Gesamtzahl der Zielgeräte, auf denen die Provisionierung fehlgeschlagen ist (ist mit der Seite *Provisionierungsergebnisse* verknüpft).
Erfolgsrate	Die Gesamtzahl der Zielgeräte, auf denen die Provisionierung erfolgreich durchgeführt wurde, in Prozent.
IP-Bereich	Der IP-Adressbereich des Zielgeräts
Planen	Der angegebene Provisionierungszeitplan. Beispiel: Alle **n** Minuten, Alle **n** Stunden oder Nie.

Option	Beschreibung
Aktiviert	Eine Angabe, ob die Konfiguration aktiviert ist oder nicht. Ein Häkchen gibt an, dass der Provisionierungszeitplan aktiviert ist.

2. Ausführen von Provisionierungszeitplänen:
   a. Aktivieren Sie die Kontrollkästchen für die Zeitpläne, die ausgeführt werden sollen.
   b. Wählen Sie **Aktion auswählen > Jetzt ausführen**.
3. Bearbeiten von Zeitplänen:
   a. Klicken Sie auf den Namen eines Zeitplans.
   b. Bearbeiten Sie den Provisionierungszeitplan auf der Seite *Detail zum Provisionierungszeitplan* und klicken Sie auf **Speichern**.

   Siehe KACE Agent auf einem Gerät oder auf mehreren Geräten installieren.
4. Duplizieren von Zeitplänen:
   a. Klicken Sie auf den Namen eines Zeitplans.
   b. Klicken Sie im Abschnitt *Erweitert* auf **Duplizieren**, um die Seite *Provisionierungszeitpläne* anzuzeigen. Der neue Zeitplan wird als **Kopie von Zeitplanname** aufgeführt.

Provisionierungszeitpläne löschen

Sie können Provisionierungszeitpläne löschen, um Zeitpläne aus der Appliance zu entfernen.

Beim Löschen von Provisionierungszeitplänen werden auch die zu diesen Zeitplänen gehörigen Ergebnisse gelöscht. Geräte, die mithilfe dieser Zeitpläne provisioniert werden, werden jedoch nicht aus dem Inventar entfernt.

1. Rufen Sie die Liste *Provisionierungszeitpläne* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie auf der linken Navigationsleiste auf **Einstellungen** und anschließend auf **Provisionierung**.
   c. Klicken Sie im *Provisionierungsbereich* auf **Zeitpläne**.
2. Aktivieren Sie das Kontrollkästchen neben einem oder mehreren Zeitplänen.
3. Wählen Sie **Aktion auswählen > Löschen** und klicken Sie dann zum Bestätigen auf **Ja**.

Provisionierungsergebnisse anzeigen

Sie können die Ergebnisse der von Provisionierungszeitplänen durchgeführten Aktionen anzeigen.

1. Rufen Sie die Liste *Provisionierungszeitpläne* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie auf der linken Navigationsleiste auf **Einstellungen** und anschließend auf **Provisionierung**.
   c. Klicken Sie im *Provisionierungsbereich* auf **Zeitpläne**.
2. Klicken Sie in der Spalte *Wird ausgeführt, Ausstehend, Erfolgreich oder Fehler* auf eine Verknüpfung.

   Auf der Seite *Provisionierungsergebnisse* werden folgende Informationen angezeigt:

Element	Beschreibung
Status	Der Status der Agentenverbindung mit der Appliance: : Ein über den Agent verwaltetes Gerät ist mit der Appliance verbunden. : Ein über den Agent verwaltetes Gerät ist nicht mit der Appliance verbunden.
Zeitplanname	Der Name des Provisionierungszeitplans.
IP-Adresse	Die IP-Adresse des Zielgeräts.
Hostname	Der Hostname des Zielgeräts. Klicken Sie auf die Schaltfläche **Remote-Verbindung**, um eine Remote-Desktop-Verbindung zum Zielgerät zu öffnen (nur Microsoft Edge):
Ergebnis	Der Status des letzten Provisionierungsversuchs.
Aktion	**I** zeigt eine erfolgreiche Installation an. **U** zeigt eine erfolgreiche Deinstallation an.
Fehler	Der Fehler, z. B. wenn TCP-Ports nicht erreichbar sind.
Letzte Ausführung	Zeitpunkt, zu dem der Zeitplan zuletzt ausgeführt wurde.

3. Um weitere Informationen zu einem Zielgerät anzuzeigen, klicken Sie auf die entsprechende **IP-Adresse**.

   Die Seite *KACE Agent Provisioning (KACE Agent-Provisionierung)* wird angezeigt.

   Auf dieser Seite werden die Ergebnisse aus der zuletzt ausgeführten Provisionierung angezeigt. Hierzu zählen Informationen wie IP-Adresse, Port-Konfiguration sowie die Protokolle der einzelnen Provisionierungsschritte.

4. Um Inventarinformationen anzuzeigen, klicken Sie auf die Verknüpfung **[Computerinventar]** neben der **MAC-Adresse**.

   HINWEIS: Der Link **[Computerinventar]** wird nur angezeigt, wenn die MAC-Adresse des Zielgeräts beim Provisionierungsprozess mit den aktuellen Inventardaten abgeglichen werden kann. Siehe Verwalten ausstehender Geräte.

Kommunikation des Agenten verwalten

Die Kommunikation zwischen der Appliance und den auf verwalteten Geräten installierten Agenten umfasst Inventarberichte, Warnungen, Patches, Skripte und Absturzberichte. Sie können Kommunikationsvorgänge, die sich in der Warteschlange befinden oder ausstehend sind, konfigurieren und anzeigen.

Agentenkommunikation und Protokolleinstellungen konfigurieren

Agenten, die auf verwalteten Geräten installiert sind, melden sich regelmäßig bei der Appliance an, um Inventarinformationen zu melden, Skripte zu aktualisieren und andere Aufgaben auszuführen.

Sie können die Agenten-Einstellungen einschließlich des Anmeldeintervalls der Agenten, der Meldungen, die Benutzern angezeigt werden, sowie der Dauer der Aufbewahrung des Protokolls wie in diesem Abschnitt beschrieben konfigurieren. Wenn Sie mehrere Organisationen haben, werden die Agenten-Einstellungen für jede Organisation separat konfiguriert.

1. Führen Sie einen der folgenden Schritte aus:
   - **Wenn die Organisationskomponente für die Appliance aktiviert ist, melden Sie sich bei der Systemverwaltungskonsole der Appliance an: `https://appliance_hostname/system`. Oder wählen Sie in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen den Eintrag System aus. Klicken Sie anschließend auf Organisationen. Klicken Sie auf den Namen einer Organisation, um Informationen dazu anzuzeigen.**

     Die Seite *Detail zu Organisation* wird angezeigt. Suchen Sie hier nach dem Abschnitt *Kommunikations- und Agenten-Einstellungen*.
   - **Wenn die Organisationskomponente nicht für die Appliance aktiviert ist, melden Sie sich bei der Administratorkonsole der Appliance an: `https://appliance_hostname/admin`. Wählen Sie anschließend Einstellungen > Provisionierung und klicken Sie im Fensterbereich** *Provisionierung* **auf Kommunikationseinstellungen.**

     Die Seite *Kommunikationseinstellungen* wird angezeigt.
2. Legen Sie die folgenden Einstellungen fest:

> **HINWEIS:** Um die Auslastung der Appliance zu reduzieren, sollten Sie die Anzahl der Agenten-Verbindungen auf 500 pro Stunde begrenzen. Die Anzahl der Verbindungen, die neben den Inventarisierungs-, Skripterstellungs- und Erfassungsintervallen angezeigt wird, gilt nur für die aktuelle Organisation. Wenn die Organisationskomponente in Ihrer Appliance aktiviert ist, sollte die Gesamtzahl der Agenten-Verbindungen für alle Organisationen maximal 500 pro Stunde betragen.

Option	Empfohlene Einstellung	Anmerkungen
Agentenprotokollierung	Aktiviert	Gibt an, ob die Appliance Skriptergebnisse speichert, die von Agenten auf verwalteten Geräten übermittelt wurden. Agenten-Protokolle können in der Datenbank bis zu 1GB Speicherplatz benötigen. Wenn Speicherplatz keine Rolle spielt, aktivieren Sie die *Agentenprotokollierung*, um alle Protokollinformationen für vom Agenten verwaltete Geräte zu speichern. Diese Protokolle können bei der Fehlerbehebung nützlich sein. Um Speicherplatz zu sparen und eine schnellere Kommunikation mit dem Agenten zu ermöglichen, deaktivieren Sie die *Agentenprotokollierung*.
Agent Debug Trace	Aktiviert	Wenn ausgewählt, ermöglicht Ihnen diese Option, den Debug-Verlauf des Agenten aufzuzeichnen. Anhand dieser Informationen können Administratoren die Leistung des Agenten überwachen und häufige Probleme diagnostizieren.

Option	Empfohlene Einstellung	Anmerkungen
Agenten-Inventar	12 Stunden	Die Häufigkeit, mit der Agenten auf verwalteten Geräten das Inventar melden. Diese Informationen werden im Abschnitt *Inventar* angezeigt.
Inventar ohne Agent	1 Tag	Die Häufigkeit, mit Geräte ohne Agent Inventar melden. Diese Informationen werden im Abschnitt *Inventar* angezeigt.
Kataloginventarisierung	24 Stunden	Die Häufigkeit, mit der verwaltete Geräte der Seite *Softwarekatalog* das Inventar melden sollen.
Erfassung der Nutzung	4 Stunden	Die Häufigkeit, mit der verwaltete Geräte der Appliance Erfassungsinformationen melden sollen. Damit dies möglich ist, muss die Erfassung auf Geräten und in Anwendungen aktiviert sein.
Skriptaktualisierung	4 Stunden	Die Häufigkeit, mit der Agenten auf den verwalteten Geräten aktualisierte Skriptkopien anfordern sollen, die auf verwalteten Geräten verfügbar sind. Dieses Intervall hat keine Auswirkungen darauf, wie häufig ein Skript ausgeführt wird.
Maximale Download-Geschwindigkeit	Nach Bedarf	Die maximale Download-Geschwindigkeit, nach Bedarf. Wählen Sie aus den verfügbaren Optionen.
Prozess-Zeitüberschreitung	1 Stunde	Die maximale Dauer, während der der Agent-Prozess vor dem Beenden ausgeführt wird. Weitere Details finden Sie unter https://support.quest.com/kb/177093/how-to-allow-more-time-for-a-kace-script-to-run-before-it-times-out-.
Warten auf Startaufgaben deaktivieren	Deaktiviert	Ist diese Option ausgewählt, wird der Agent bei der Ausführung von Startaufgaben gestoppt.

Option	Empfohlene Einstellung	Anmerkungen
Warten auf Anmeldeaufgaben deaktivieren	Deaktiviert	Ist diese Option ausgewählt, wird der Agent bei der Ausführung von Anmeldeaufgaben gestoppt.

3. Geben Sie im Abschnitt *Agent Status Icon Settings (Einstellungen des Agentenstatussymbols)* folgende Einstellungen an:

Option	Empfohlene Einstellung	Anmerkungen
Agentenstatus-Symbol für Gerät	Aktiviert	Wenn ausgewählt, ermöglicht Ihnen diese Option, den Agentenstatus für verwaltete Geräte anzuzeigen.
Agent auf Gerät im Snooze-Modus	Aktiviert	Wenn diese Option ausgewählt ist, können Sie die Aktivität des Agenten auf verwalteten Geräten über die Taskleiste (Windows) oder die Menüleiste (Mac OS) vorübergehend aussetzen. **HINWEIS:** Einige kritische Hintergrundaufgaben können weiterhin ausgeführt werden, einschließlich Inventarisierung, Replikationsaufgaben und dringende Warnungen.
Max. Snooze-Anzahl für Agent (pro Tag)	1 Snooze	Gibt an, wie oft Sie die Snooze-Funktion für den Agenten auf verwalteten Geräten pro Tag verwenden können.
Agent Status Icon Shortcuts (Verknüpfungen für das Agentenstatussymbol)	Nach Bedarf	Verwenden Sie diesen Abschnitt, um Links im Menü "KACE Agent" auf von Agenten verwalteten Geräten anzuzeigen. Sie können bis zu zehn Links angeben. Standard-URI-Links (Uniform Resource Identifier) werden unterstützt, wie z. B. `https`-, `ssh`- und `ftp`-URLs. So fügen Sie einen Link hinzu: a. Klicken Sie auf +. b. Geben Sie in die Spalte *Anzeigename* den Text ein, der im Menü angezeigt werden soll. Zum Beispiel *My FTP link (Mein FTP-Link)*. c. Geben Sie in die Spalte "URL" die vollständig qualifizierte URL-Adresse ein. Zum

Option	Empfohlene Einstellung	Anmerkungen
		Beispiel `https://www.quest.com/`. Die URL unterstützt die folgenden Ersetzungsvariablen: ◦ $(KACE_SYS_DIR) ◦ $(KACE_MAC_ADDRESS) ◦ $(KACE_IP_ADDRESS) ◦ $(KACE_SERVER_URL) ◦ $(KACE_SERVER) ◦ $(KACE_COMPANY_NAME) ◦ $(KACE_KUID) ◦ $(KACE_APP_DIR) ◦ $(KACE_DATA_DIR) ◦ $(KACE_AGENT_VERSION) Vollständige Informationen zu diesen und anderen Ersetzungsvariablen finden Sie unter Token-Ersetzungsvariablen. Mithilfe der Spaltenüberschriften können Sie die Liste sortieren. Im Menü "KACE Agent" werden die Links in der Reihenfolge angezeigt, in der sie auf dieser Seite aufgeführt sind.

HINWEIS: Alle Änderungen, die Sie in diesem Abschnitt vornehmen, werden erst wirksam, nachdem der KACE Agent auf dem verwalteten Gerät erneut eine Verbindung zur Appliance herstellt, entweder durch einen Neustart jedes einzelnen Agenten oder der Appliance.

4. Geben Sie im Abschnitt *Benachrichtigen* die Mitteilung für die Agenten-Kommunikation ein:

Option	Empfohlene Einstellung	Anmerkungen
Meldung auf der Begrüßungsseite des Agenten	Standardtext: **KACE Systemverwaltungs-Appliance** `überprüft die Aktualisierungen für die Konfigurations- und Verwaltungssoftware auf Ihrem PC. Bitte warten...`	Die Meldung, die Benutzern angezeigt wird, wenn Agenten Aufgaben ausführen, z.B. die Ausführung von Skripten auf ihren Geräten.
Agenten-Splash-Bitmap	Nach Bedarf	Der Pfad zu einer vorhandenen .bmp-Datei, die Sie als Splash-Logo verwenden möchten.
Start-Splash deaktivieren	Deaktiviert	Ist diese Option ausgewählt, wird der Agent bei der Anzeige des Start-Splash-Logos gestoppt.

Option	Empfohlene Einstellung	Anmerkungen
Anmelde-Splash deaktivieren	Deaktiviert	Ist diese Option ausgewählt, wird der Agent bei der Anzeige des Anmelde-Splash-Logos gestoppt.

5. Legen Sie im Abschnitt *Einstellungen für die Verarbeitung ohne Agent* die Kommunikationseinstellungen für Geräte ohne Agent fest:

Option	Beschreibung
SSH-Timeout	Die Zeit in Sekunden, nach der eine Verbindung geschlossen wird, wenn keine Aktivität stattfindet.
SNMP-Timeout	Die Zeit in Sekunden, nach der eine Verbindung geschlossen wird, wenn keine Aktivität stattfindet.
Wiederholungsversuche	Die Anzahl der Verbindungsversuche.
WinRM-Timeout	Die Zeit in Sekunden, nach der eine Verbindung geschlossen wird, wenn keine Aktivität stattfindet.
VMware-Timeout	Die Zeitspanne in Sekunden, die auf eine Verbindung zum VMware vSphere API Service gewartet wird, der auf einem VMware-Host ausgeführt wird.

6. Wenn die Organisationskomponente auf der Appliance nicht aktiviert ist, geben Sie die Einstellungen für den *Agenten* an.

> **HINWEIS:** Wenn die Organisationskomponente in Ihrer Appliance aktiviert ist, befinden sich die *Agenten-Einstellungen* auf der Seite *Allgemeine Einstellungen* der Systemadministratorkonsole der Appliance.

Option	Beschreibung
Letzte Aktualisierung des Aufgabendurchsatzes	Dieser Wert gibt Datum und Uhrzeit der letzten Aktualisierung des Aufgabendurchsatzes der Appliance an.
Aktueller Lastdurchschnitt	Der Wert in diesem Feld steht für die Last einer Appliance zu einem bestimmten Zeitpunkt. Damit die Appliance normal läuft, muss der Feldwert zwischen 0,0 und 10,0 liegen.
Aufgabendurchsatz	Der Wert, der steuert, wie geplante Aufgaben, z.B. Inventarerfassung, Skripterstellung und Patch-Aktualisierungen, durch die Appliance ausbalanciert werden. **HINWEIS:** Dieser Wert kann nur erhöht werden, wenn der Wert im Feld Aktueller Lastdurchschnitt nicht über 10,0 liegt und die Zeit für die letzte Aktualisierung des Aufgabendurchsatzes mehr als 15 Minuten beträgt.

7. Klicken Sie auf **Speichern**.

Die Änderungen werden wirksam, wenn sich Agenten bei der Appliance anmelden.

8. Wenn Sie mehrere Organisationen haben, wiederholen Sie die oben aufgeführten Schritte für jede Organisation.

Verwandte Themen

Appliance-Protokolle anzeigen

Allgemeine Appliance-Einstellungen bei aktivierter Organisationskomponente konfigurieren

Status von Agenten-Aufgaben anzeigen

Sie können den Status von Aufgaben, die gerade auf vom Agenten verwalteten Geräten ausgeführt werden oder deren Ausführung auf diesen Geräten geplant ist, anzeigen.

1. Navigieren Sie zur *Systemsteuerung* der Appliance:
   - **Wenn die Organisationskomponente nicht für die Appliance aktiviert ist, melden Sie sich bei der Administratorkonsole an: `https://appliance_hostname/admin`, und wählen Sie dann Einstellungen > Systemsteuerung aus.**
   - **Wenn die Organisationskomponente für die Appliance aktiviert ist, melden Sie sich bei der Systemverwaltungskonsole der Appliance an: `https://appliance_hostname/system`. Oder wählen Sie in der Dropdown-Liste rechts oben auf der Seite den Eintrag System aus, und klicken Sie dann auf Einstellungen > Systemsteuerung.**
2. Klicken Sie auf der linken Navigationsleiste auf **Support**, um die Seite *Support* anzuzeigen.
3. Klicken Sie im Bereich *Tools zur Fehlerbehebung* auf **Aufgabenstatus des Agenten anzeigen**, um die Seite *Agenten-Aufgaben* anzuzeigen.

   Standardmäßig werden Aufgaben mit dem Status *Vorgang wird durchgeführt* angezeigt. Um andere Aufgaben anzuzeigen, wählen Sie über der Liste auf der rechten Seite aus der Dropdown-Liste *Anzeigen nach* andere Filteroptionen aus. Die Aufgabeninformationen umfassen:

Spalte	Beschreibung
Gerätename	Der Name des Geräts, das Ziel der Aufgabe ist.
Typ	Aufgabentyp. Abhängig von der Konfiguration der Appliance gibt es folgende Aufgabentypen: Benachrichtigungen, Inventar, kbot, Absturz-Upload und Skriptaktualisierungen.
Gestartet	Die Startzeit der Aufgabe.
Abgeschlossen	Die Abschlusszeit der Aufgabe.
Nächste Ausführung	Die Zeit der nächsten geplanten Ausführung der Aufgabe.
Ausführungszeit	Die Zeit, die zum Ausführen der Aufgabe benötigt wurde.
Timeout	Die Frist zum Abschluss der Aufgabe.
Priorität	Die Wichtigkeit oder der Rang der Aufgabe.

Die angezeigten Optionen hängen von den in Ihrer Appliance verfügbaren Aufgaben ab. Typische Optionen sind:

- **Bereit zur Ausführung (verbunden)**: Aufgaben, für die eine Verbindung über das Messaging-Protokoll besteht und die bereit zur Ausführung sind.
- **Bereit zur Ausführung**: Aufgaben, die ausgeführt werden sollen, sobald eine Verbindung über das Messaging-Protokoll hergestellt wurde.
- **Länger als 10 Minuten**: Aufgaben, die länger als 10 Minuten auf eine Protokollverbindung gewartet haben.

4. Klicken Sie in der Spalte *Gerätename* auf den Namen eines Geräts, um Details zu diesem Gerät anzuzeigen.

   Die Seite *Gerätedetail* wird angezeigt.

Befehlswarteschlange des Agenten anzeigen

In der Agenten-Befehlswarteschlange werden Meldungen wie Popup-Fenster und Warnungen angezeigt, die für die Verteilung von der Appliance an vom Agenten verwaltete Geräte in die Warteschlange gestellt wurden.

1. Navigieren Sie zur *Systemsteuerung* der Appliance:

   - **Wenn die Organisationskomponente nicht für die Appliance aktiviert ist, melden Sie sich bei der Administratorkonsole an: `https://appliance_hostname/admin`, und wählen Sie dann Einstellungen > Systemsteuerung aus.**
   - **Wenn die Organisationskomponente für die Appliance aktiviert ist, melden Sie sich bei der Systemverwaltungskonsole der Appliance an: `https://appliance_hostname/system`. Oder wählen Sie in der Dropdown-Liste rechts oben auf der Seite den Eintrag System aus, und klicken Sie dann auf Einstellungen > Systemsteuerung.**

2. Klicken Sie auf der linken Navigationsleiste auf **Support**, um die Seite *Support* anzuzeigen.
3. Klicken Sie im Bereich *Tools zur Fehlerbehebung* auf **Befehlswarteschlange des Agenten anzeigen**, um die Seite *Agenten-Befehlswarteschlange* anzuzeigen.

   Ausstehende Meldungen werden nur dann in dieser Warteschlange angezeigt, wenn eine ständige Verbindung zwischen dem Agenten und der Appliance besteht.

   HINWEIS: Ausstehende Warnungen werden auch dann in der *Agenten-Befehlswarteschlange* angezeigt, wenn keine Verbindung zwischen dem Agenten und der Appliance besteht.

   Die Seite mit der *Agenten-Befehlswarteschlange* enthält folgende Felder:

Option	Beschreibung
Gerätename	Der Name des Geräts. Klicken Sie auf einen Namen, um Gerätedetails anzuzeigen.
Typ [Plug-in, Quelle]	Der Typ der Nachricht, beispielsweise *Vorgang ausführen*.
Befehl	Der Inhalt und die Informationen in der Nachricht.
Ablauf	Das Datum und die Uhrzeit des Ablaufs der Nachricht, auch als *Gültigkeitsdauer* bezeichnet. Nachrichten werden automatisch aus der Warteschlange gelöscht, wenn ihre Gültigkeitsdauer abgelaufen ist.

Option	Beschreibung
Status	Der Status der Nachricht wie *Abgeschlossen* oder *Erhalten*.

Verwandte Themen

Senden von Warnungen an verwaltete Geräte

Nachrichten aus der Agenten-Befehlswarteschlange löschen

Sie können nicht mehr benötigte Nachrichten aus der Agenten-Befehlswarteschlange löschen.

1. Navigieren Sie zur *Systemsteuerung* der Appliance:
   - **Wenn die Organisationskomponente nicht für die Appliance aktiviert ist, melden Sie sich bei der Administratorkonsole an: `https://appliance_hostname/admin`, und wählen Sie dann Einstellungen > Systemsteuerung aus.**
   - **Wenn die Organisationskomponente für die Appliance aktiviert ist, melden Sie sich bei der Systemverwaltungskonsole der Appliance an: `https://appliance_hostname/system`. Oder wählen Sie in der Dropdown-Liste rechts oben auf der Seite den Eintrag System aus, und klicken Sie dann auf Einstellungen > Systemsteuerung.**
2. Klicken Sie auf der linken Navigationsleiste auf **Support**, um die Seite *Support* anzuzeigen.
3. Klicken Sie im Bereich *Tools zur Fehlerbehebung* auf **Befehlswarteschlange des Agenten anzeigen**, um die Seite *Agenten-Befehlswarteschlange* anzuzeigen.
4. Aktivieren Sie das Kontrollkästchen neben einem oder mehreren Nachrichten.
5. Wählen Sie **Aktion auswählen** > **Löschen** und klicken Sie dann zum Bestätigen auf **Ja**.

KACE Agent auf verwalteten Geräten aktualisieren

Die Appliance überprüft jeden Tag gegen 03:40 Uhr automatisch bei Quest, ob Aktualisierungen für den KACE Agent verfügbar sind. Außerdem überprüft die Appliance bei jedem Neustart Quest auf Aktualisierungen des Agenten.

Wenn Agent-Aktualisierungen verfügbar sind, werden sie automatisch auf die Appliance heruntergeladen, sofern die Appliance mit dem Internet verbunden ist. Zusätzlich wird eine Warnung auf der *Startseite* der Appliance **Administratorkonsole** angezeigt. Bis Sie jedoch entsprechende Bereitstellungseinstellungen festlegen, werden Agenten-Aktualisierungen nicht automatisch auf verwalteten Geräten bereitgestellt. Klicken Sie auf den Link in der Warnung, um die Bereitstellungseinstellungen zu konfigurieren.

Darüber hinaus können Sie zu jedem beliebigen Zeitpunkt nach Aktualisierungen für die Agenten-Software suchen, Agenten-Aktualisierungen manuell herunterladen und die Einstellungen der Agenten-Aktualisierungen ändern. Das manuelle Beziehen der Aktualisierungen kann hilfreich sein, wenn Ihre Appliance nicht mit dem Internet verbunden ist.

KACE Agent-Updates anzeigen

KACE Agent-Updates können Sie in der **Administratorkonsole** anzeigen.

1. Navigieren Sie zur *Systemsteuerung* der Appliance:
   - **Wenn die Organisationskomponente nicht für die Appliance aktiviert ist, melden Sie sich bei der Administratorkonsole an: `https://appliance_hostname/admin`, und wählen Sie dann Einstellungen > Systemsteuerung aus.**
   - **Wenn die Organisationskomponente für die Appliance aktiviert ist, melden Sie sich bei der Systemverwaltungskonsole der Appliance an: `https://appliance_hostname/system`. Oder**

wählen Sie in der Dropdown-Liste rechts oben auf der Seite den Eintrag System aus, und klicken Sie dann auf Einstellungen > Systemsteuerung.

2. Klicken Sie in der linken Navigationsleiste auf **Appliance-Aktualisierungen**.

   Die Seite *Appliance-Aktualisierungen* wird angezeigt. Das aktuelle Agenten-Bundle wird im Bereich *Agent* angezeigt.

3. **Optional**: So überprüfen Sie, ob Aktualisierungen verfügbar sind: Klicken Sie im Bereich *Agent* auf **Auf Aktualisierungen prüfen**.

   Die Appliance prüft, ob Aktualisierungen verfügbar sind, und die Ergebnisse werden auf der Seite *Protokolle* angezeigt.

Agenten-Aktualisierungseinstellungen konfigurieren

Nach der Installation der Agenten auf den Geräten aktualisieren sich diese auf der Grundlage der von Ihnen auf der Seite *Agenten-Einstellungen für Aktualisierungen* gewählten Agenten-Aktualisierungseinstellungen automatisch selbst. Das gilt unabhängig von den für die Bereitstellung der Agenten verwendeten Provisionierungsmethoden, einschließlich Appliance-Bereitstellung, GPO-Assistent, anderer GPO- und Bildbereitstellungen.

Wenn Sie mehrere Organisationen haben, werden die Agenten-Aktualisierungseinstellungen für jede Organisation separat konfiguriert.

1. Rufen Sie die Seite *Agenten-Einstellungen für Aktualisierungen* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie auf der linken Navigationsleiste auf **Einstellungen** und anschließend auf **Provisionierung**.
   c. Klicken Sie im *Provisionierungsbereich* auf **Agenten-Aktualisierung**.

   Wenn eine neue Agenten-Aktualisierung verfügbar ist, wird diese im Abschnitt *Verfügbares Agenten-Bundle* angezeigt.

2. Klicken Sie im Abschnitt *Verfügbares Agenten-Bundle* auf **Übernehmen**.

   Die neue Versionsnummer des Agenten wird im Abschnitt *Beworbene Aktualisierungen* angezeigt und das Kontrollkästchen *Aktiviert* im Abschnitt *Agenten-Einstellungen* wird deaktiviert, sodass automatische Aktualisierungen deaktiviert sind. Dadurch können Sie die Aktualisierungen auf ausgewählten Geräten testen, bevor sie systemweit bereitgestellt werden.

3. Überprüfen Sie die folgenden Agenten-Aktualisierungseinstellungen bzw. geben Sie sie an:

Option	Beschreibung
Aktiviert	Bereitstellung der Aktualisierung auf den ausgewählten Appliance-Geräten während des nächsten geplanten Inventarisierungsintervalls. Deaktivieren Sie das Kontrollkästchen, um zu verhindern, dass Aktualisierungen installiert werden.
Geändert	Schreibgeschützt: Die Uhrzeit, zu der das aktuellste Agenten-Bundle heruntergeladen wurde
Alle Geräte	Aktualisierung auf allen Geräten bereitstellen, auf denen der KACE Agent installiert ist. Ist diese Option aktiviert, erscheinen die Elemente *Geräte* und *Labels* nicht auf der Seite.

Option	Beschreibung
Geräte	Nur bestimmte Geräte aktualisieren. Wählen Sie in der Dropdown-Liste, die nach dem Klicken auf das Feld erscheint, die Gerätenamen aus oder geben Sie die ersten Zeichen des Gerätenamens ein, um die Liste zu sortieren. Wenn Sie beispielsweise Dev eingeben, werden in der Liste Gerätenamen wie Device-1, Device-2 usw. aufgeführt. Diese Option ist nicht verfügbar, wenn Sie **Alle Geräte** auswählen.
Verknüpfte Labels verwalten	Anzeige des Dialogfelds *Labels bearbeiten*. Suchen Sie nach Labels, wählen Sie sie aus und aktualisieren Sie die den ausgewählten Labels zugewiesenen Geräte. Diese Option ist nicht verfügbar, wenn Sie **Alle Geräte** auswählen.
Anmerkungen	Geben Sie nach Bedarf beliebige weitere Informationen ein.

4. Klicken Sie auf **Speichern**.

   Die Aktualisierung wird während des nächsten geplanten Inventarisierungsintervalls auf den ausgewählten Geräten bereitgestellt. Wenn Sie Replikationsfreigaben verwenden und das Failover zur Appliance nicht ausgewählt ist, werden die Agenten nach der Aktualisierung der Replikationsfreigaben aktualisiert.
5. Wenn Sie die Bereitstellung zu Testzwecken auf bestimmte Geräte beschränkt haben, wählen Sie im Abschnitt *Agenten-Einstellungen* auf der Seite *Agenten-Einstellungen für Aktualisierungen* zusätzliche Geräte aus, wenn die Tests abgeschlossen sind.

   Die Aktualisierung wird während des nächsten geplanten Inventarisierungsintervalls auf den ausgewählten Geräten bereitgestellt.
6. Wenn Sie mehrere Organisationen haben, wiederholen Sie die oben aufgeführten Schritte für jede Organisation.

Verwandte Themen

Einrichten und Verwenden von Labels für die Verwaltung von Elementgruppen

Agenten-Aktualisierungen manuell hochladen

Wenn Agenten-Aktualisierungen verfügbar sind, werden sie in den meisten Fällen automatisch auf die Appliance heruntergeladen. Sie können aber auch Aktualisierungen von Quest herunterladen und die Agenten-Aktualisierungen manuell bei Bedarf auf die Appliance hochladen. Das ist nützlich, wenn Ihre Appliance nicht mit dem Internet verbunden ist oder wenn vorhandene Agenten-Aktualisierungen noch nicht automatisch auf die Appliance heruntergeladen wurden.

Zum Herunterladen von Agenten-Updates von Quest benötigen Sie die Kundenanmeldeinformationen. Diese erhalten Sie vom **Quest Support** unter https://support.quest.com/contact-support.

1. Zum manuellen Suchen nach Aktualisierung rufen Sie die *Systemsteuerung* der Appliance auf:
   - **Wenn die Organisationskomponente nicht für die Appliance aktiviert ist, melden Sie sich bei der Administratorkonsole an: `https://appliance_hostname/admin`, und wählen Sie dann Einstellungen > Systemsteuerung aus.**
   - **Wenn die Organisationskomponente für die Appliance aktiviert ist, melden Sie sich bei der Systemverwaltungskonsole der Appliance an: `https://appliance_hostname/system`. Oder wählen Sie in der Dropdown-Liste rechts oben auf der Seite den Eintrag System aus, und klicken Sie dann auf Einstellungen > Systemsteuerung.**
2. Klicken Sie auf der linken Navigationsleiste auf **Appliance-Aktualisierungen**, um die Seite *Appliance-Aktualisierungen* anzuzeigen.

Die Version des aktuellen Agenten-Bundles wird im Bereich *Agent* angezeigt.

3. Klicken Sie im Abschnitt *Agent* auf **Auf Aktualisierungen prüfen**.

   Die Appliance prüft, ob Aktualisierungen verfügbar sind, und die Ergebnisse werden auf der Seite *Protokolle* angezeigt.

4. So erhalten Sie Aktualisierungen:
   a. Melden Sie sich mit Ihren Kundenanmeldeinformationen auf der Quest Support Website an:

      https://support.quest.com/kace-systems-management-appliance/download-new-releases.

   b. Laden Sie das Bundle für die Agenten-Aktualisierung herunter und speichern Sie es lokal.

5. Rufen Sie die Seite *Agenten-Einstellungen für Aktualisierungen* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie auf der linken Navigationsleiste auf **Einstellungen** und anschließend auf **Provisionierung**.
   c. Klicken Sie im *Provisionierungsbereich* auf **Agenten-Aktualisierung**.

6. Führen Sie einen der folgenden Schritte aus:

   - **Wenn eine neue Aktualisierung angezeigt wird, klicken Sie im Abschnitt** *Verfügbares Agenten-Bundle* **auf Übernehmen.**
   - **Wenn Sie eine Aktualisierung manuell heruntergeladen haben, klicken Sie im Abschnitt** *Agenten-Bundle manuell hochladen* **auf Durchsuchen oder Datei auswählen und navigieren Sie zu der heruntergeladenen Datei. Klicken Sie dann auf Hochladen.**

   Die neue Versionsnummer des Agenten wird im Abschnitt *Beworbene Aktualisierungen* angezeigt und das Kontrollkästchen *Aktiviert* im Abschnitt *Agenten-Einstellungen* wird deaktiviert, sodass automatische Aktualisierungen deaktiviert sind. Dadurch können Sie die Aktualisierungen auf ausgewählten Geräten testen, bevor sie systemweit bereitgestellt werden.

7. Legen Sie die Bereitstellungsoptionen im Abschnitt *Agenten-Einstellungen* fest. Siehe Agenten-Aktualisierungseinstellungen konfigurieren.

8. Wenn Sie mehrere Organisationen haben, wiederholen Sie 6 und 7 für jede Organisation.

Manuelle Bereitstellung des KACE Agent

Die manuelle Bereitstellung ist hilfreich, wenn die automatisierte Agenten-Provisionierung nicht praktikabel ist oder Sie die KACE Agent-Software per E-Mail oder mithilfe von Anmeldeskripten, einem Gruppenrichtlinienobjekt oder Active Directory bereitstellen möchten.

- **E-Mail**: Bei der E-Mail-basierten Bereitstellung von KACE Agenten senden Sie den Benutzern eine E-Mail mit einem der folgenden Inhalte:
  - Die Installationsdatei für den Agenten.
  - Einen Link zu der Appliance, von der die Agenten-Datei heruntergeladen werden kann.
  - Einen Webspeicherort zum Download der erforderlichen Installationsdatei.
- **Logon-Skripte**: Mithilfe von Anmeldeskripten können Sie den KACE Agent bereitstellen, wenn sich der Benutzer bei einem Gerät anmeldet. Bei Verwendung von Logon-Skripten laden Sie die entsprechende Datei in ein zugängliches Verzeichnis hoch und erstellen ein Logon-Skript, um die Datei abzurufen.

Agenteninstallationsdateien abrufen

Die Agenteninstallationsdateien stehen auf der Appliance zur Verfügung.

Die KACE Agent-Agenteninstallationsdateien für Windows, Mac OS X und Linux Geräte finden Sie im folgenden Verzeichnis der Appliance:

`\\`**appliance_hostname**`\client\agent_provisioning`

> **HINWEIS:** Die Dateifreigabe muss aktiviert sein, um auf die Installationsdateien zugreifen zu können. Siehe Dateifreigabe auf Systemebene aktivieren.

Die Appliance verwendet einen Registrierungsprozess, der authentifizierten KACE Agenten ermöglicht, sich mit der Appliance zu verbinden. Dies kann entweder durch Verknüpfung eines Tokens mit einem Agenten oder durch Genehmigung einer Verbindungsanforderung durch einen Geräteadministrator erfolgen. Agent-Installationsprogramme, die auf diese Weise abgerufen wurden, enthalten kein gültiges Token. Sie können das Agent-Token manuell an das Installationsprogramm übergeben, indem Sie eine der folgenden Optionen verwenden:

- **Windows-Geräte:**
  - Verwenden Sie beim Starten des Installationsprogramms die folgenden Parameter: `HOST=<appliance_hostname> TOKEN=<agent_token>` oder:
  - Ändern Sie den Namen der Installationsdatei manuell mithilfe der folgenden Syntax: `AMPAgent-xx.xx.xx-x86_<appliance_hostname>+<agent_token>.msi`
- **Nicht-Windows-Geräte**:
  - Verwenden Sie die Umgebungsvariablen `KACE_HOST` und `KACE_TOKEN`, um den Hostnamen und das Agent-Token der Appliance anzugeben, bevor Sie die Installationsdatei ausführen. Oder:
  - Ändern Sie den Namen der Installationsdatei manuell mithilfe der folgenden Syntax: `<agent_installation_filename>_<appliance_hostname>+<agent_token>.<extension>`

Wenn Sie während der Agent-Installation keine gültige Tokenzeichenfolge angeben, führen alle Verbindungsanforderungen dazu, dass der Agent unter Quarantäne gestellt wird.

Alternativ können Sie Installationspakete für Agent-Token für Ihr Betriebssystem von der Seite *Agent Token Detail (Details zu Agent-Token)* herunterladen. Weitere Informationen hierzu finden Sie unter Registrieren des KACE Agent bei der Appliance.

KACE Agent auf Windows-Geräten manuell bereitstellen

Sie können den KACE Agent mithilfe des Installationsassistenten oder über die Befehlszeile des jeweiligen Geräts manuell auf Windows-Geräten bereitstellen.

Bei der manuellen Installation des Agenten müssen die ausführbaren Dateien des Agenten an folgenden Speicherorten installiert werden:

- Windows 32-Bit-Geräte: `C:\Programme\Quest\KACE\`
- Windows 64-Bit-Geräte: `C:\Programme (x86)\Quest\KACE\`

Die Konfigurationsdateien, Protokolle und anderen Daten des Agenten befinden sich in folgenden Verzeichnissen:

- Windows 32-Bit-Geräte: `C:\Dokumente und Einstellungen\All Users\Quest\KACE`
- Windows 64-Bit-Geräte: `C:\ProgramData\Quest\KACE`

KACE Agent auf Windows-Geräten mithilfe des Installationsassistenten manuell bereitstellen

Sie können den KACE Agent manuell auf Windows-Geräten bereitstellen, indem Sie auf den Geräten den Installationsassistenten ausführen.

1. Wechseln Sie zum freigegebenen Verzeichnis der Appliance:

   `\\`**appliance_hostname**`\client\agent_provisioning\windows_platform`

2. Kopieren Sie die Datei `ampagent-x.x.xxxxx-x86.msi` auf das Gerät.
3. Doppelklicken Sie auf die Datei, um die Installation zu starten, und befolgen Sie die Anweisungen im Installationsassistenten.
4. Wenn Sie den Agenten bei der Appliance registrieren möchten:
   - Verwenden Sie beim Starten des Installationsprogramms die folgenden Parameter: `HOST=<appliance_hostname> TOKEN=<agent_token>` oder:
   - Ändern Sie den Namen der Installationsdatei manuell mithilfe der folgenden Syntax: `AMPAgent-xx.xx.xx-x86_<appliance_hostname>+<agent_token>.msi`

   Sie können die Zeichenfolge des Agent-Tokens auf der Seite *Agent Token Detail (Details zum Agent-Token)* abrufen. Weitere Informationen finden Sie unter Registrieren des KACE Agent bei der Appliance.

Die Geräteinformationen werden innerhalb weniger Minuten im **Inventar** der Appliance angezeigt. Siehe Verwalten von Anwendungen auf der Seite "Software".

KACE Agent auf Windows-Geräten über die Befehlszeile manuell bereitstellen

Es gibt verschiedene Möglichkeiten zur Bereitstellung des Agenten mithilfe der Befehlszeile auf Windows-Geräten.

Beispiel:

- In einer Batch-Datei als Teil eines Anmeldeskripts, mit dem die Installationsdatei (`msiexec`) ausgeführt wird und verschiedene Parameter, etwa der Wert des Hosts, festgelegt werden.
- Legen Sie eine Umgebungsvariable für den Servernamen fest und führen Sie anschließend die Installationsdatei aus.
- Ändern Sie den Namen der Installationsdatei, mit der der Servername während der Installation automatisch festgelegt wird.

In der folgenden Tabelle sind die Befehlszeilenparameter zur Bereitstellung des Agenten aufgeführt.

Befehlszeilenparameter für den Agenten

Beschreibung	Parameter
Windows Installationsprogramm	`msiexec` oder `msiexec.exe`

Installationsflag	`/i`
	Beispiel:
	`msiexec /i ampagent-6.x.xxxxx-x86`

Deinstallationsflag	`/x`
	Beispiel:
	`msiexec /x ampagent-6.x.xxxxx-x86`

Installation im Hintergrund	`/qn` **Beispiel**:

Beschreibung	Parameter
	`msiexec /qn /i ampagent-6.x.xxxxx-x86`

Ausführliche Protokollausgabe	`/L*v log.txt`
	Beispiel:
	`msiexec /qn /L*v C:\temp\log.txt /i ampagent-6.x.xxxxx-x86`

Automatische Festlegung des Hostnamens: Benennt die Installationsdatei in den Namen des Servers um. So wird der Hostname automatisch festgelegt.	`rename agent_installer.msi_hostname.msi`
	Beispiel:
	`msiexec /qn /i ampagent-6.x.xxxxx-x86_kace_sma.example.com.msi`

Festlegen von Eigenschaften	`PROPERTY=value` (GROSSBUCHSTABEN verwenden) **Beispiel**: `msiexec /qn /i ampagent-6.x.xxxxx-x86.msi HOST=kace_sma.example.com`

Festlegen des Servernamens	`set KACE_SERVER=kace_sma_name`
	Hier muss eine zu installierende `msiexec`-Datei angefügt werden.
	Beispiel:
	`set KACE_SERVER=kboxmsiexec /i ampagent-6.x.xxxxx-x86`

Vermeiden Sie die Installation von Anmelde- oder Systemstart-Elementen und behalten Sie die bestehenden Dateien mit der Bezeichnung userinit.exe bei.	`NOHOOKS=1`
	Beispiel:
	`msiexec /qn /i ampagent-6.x.xxxxx-x86.msi HOST=kace_sma.example.com NOHOOKS=1`

Installiert den Agenten, startet jedoch nicht den Dienst. Dadurch kann ein Image des Agenten erstellt werden, das auf andere Geräte geklont wird.	`CLONEPREP=yes/no`
	Beispiel:
	`msiexec /qn /i ampagent-6.x.xxxxx-x86.msi HOST=kace_sma.example.com CLONEPREP=yes`

Legen Sie die Debug-Ebene für den Agenten fest, wenn dieser Protokolle generiert.	`DEBUG=true/all`
	Beispiel:
	`msiexec /qn /i ampagent-6.x.xxxxx-x86.msi HOST=kace_sma.example.com DEBUG=true`

Erzwingt die ausschließliche Kommunikation des Agenten per HTTPS. Beim Ausfall von HTTPS ist die Nutzung von HTTP nicht möglich.	`SSLREQUIRED=true` **Beispiel**:

Beschreibung	Parameter
	`msiexec /qn /i ampagent-6.x.xxxxx-x86.msi HOST=kace_sma.example.com SSLREQUIRED=true`

Das System sucht an diesen Speicherorten im angezeigten Ordner nach dem Wert des **Hosts**:

1. Die Installationsdatei
2. Der Eigenschaftswert `HOST`
3. `KACE_SERVER` (Umgebungsvariable)
4. Die Datei `amp.conf`

Wenn Sie den Agenten bei der Appliance registrieren möchten:

- Verwenden Sie beim Starten des Installationsprogramms die folgenden Parameter: `HOST=<appliance_hostname> TOKEN=<agent_token>` oder:
- Ändern Sie den Namen der Installationsdatei manuell mithilfe der folgenden Syntax: `AMPAgent-xx.xx.xx-x86_<appliance_hostname>+<agent_token>.msi`

Sie können die Zeichenfolge des Agent-Tokens auf der Seite *Agent Token Detail (Details zum Agent-Token)* abrufen. Weitere Informationen finden Sie unter Registrieren des KACE Agent bei der Appliance

VORSICHT: Wenn Sie den Wert des Hosts leer lassen, müssen Sie die Umgebungsvariable festlegen. Andernfalls stellt der Agent keine Verbindung mit der Appliance her. Quest empfiehlt, den vollständig qualifizierten Domänennamen als Hostnamen zu verwenden.

Verwalten des KACE Agent auf Windows-Geräten über die Windows-Taskleiste

Sie können über die Windows-Taskleiste den Status des KACE Agent anzeigen, eine Bestandsaufnahme erzwingen und die Agenteninformationen anzeigen.

Um den KACE Agent-Status über die Taskleiste aufzurufen, müssen Sie im Abschnitt *Agenten- und Kommunikationseinstellungen* die Option **Agenten-Status auf Gerät** aktivieren. Weitere Informationen hierzu finden Sie unter Agentenkommunikation und Protokolleinstellungen konfigurieren.

1. Klicken Sie auf dem Windows-Gerät, auf dem der KACE Agent ausgeführt wird, in der Windows-Taskleiste auf .

   Die Anzeige in der unteren rechten Ecke des Symbols gibt Auskunft über den Status des Agenten:

   - : Der Agent ist mit der Appliance verbunden.
   - : Der Agent befindet sich im Snooze-Modus.
   - : Der Agent weist ausstehende Aktionen auf.
   - : Der Agent ist von der Appliance getrennt.
2. Um herauszufinden, ob der Agent mit der Appliance verbunden ist, beachten Sie das Statussymbol im Menü.

   Hierbei handelt es sich um die gleiche Anzeige wie oben beschrieben, die auf dem Agent-Symbol angezeigt wird und darüber Auskunft gibt, ob der Agent verbunden ist, sich im Snooze-Modus befindet, ausstehende Aktionen aufweist oder von der Appliance getrennt wurde.
3. Um die Gerätebestandsaufnahme auszuführen, klicken Sie im Menü auf **Bestandsaufnahme**.
4. Um den Agenten neu zu starten, klicken Sie auf **Agent neu starten** im Menü.
5. Um die Aktivität des Agenten während eines bestimmten Zeitraums vorübergehend zu unterbrechen, klicken Sie auf **Agent im Snooze-Modus** und wählen Sie einen Zeitraum im Menü aus. Sie können den Agent für 15 Minuten, 30 Minuten, eine Stunde oder zwei Stunden lang in den Snooze-Modus versetzen.

> **HINWEIS:** Sie können die Snooze-Funktion nur dann aktivieren, wenn die Option **Agent auf Gerät im Snooze-Modus** im Abschnitt *Agent und Kommunikationseinstellungen* auf der Appliance aktiviert ist und die maximale Anzahl von Snooze-Modus-Aktivierungen noch nicht erreicht wurde. Weitere Informationen hierzu finden Sie unter Agentenkommunikation und Protokolleinstellungen konfigurieren.

Durch die Aktivierung des Snooze-Modus für einen Agenten werden keine laufenden Agentenprozesse auf dem Gerät gestoppt. Sie verhindert nur, dass der Agent einen neuen Prozess startet. Wenn die Aktivierung der Agenten-Snooze-Funktion nicht möglich ist, z. B. aufgrund der Konfiguration, wird eine Fehlermeldung angezeigt.

6. Klicken Sie zum Installieren der Patches, die auf das Agent-Gerät heruntergeladen wurden, auf **Deploy staged patches (Bereitgestellte Patches bereitstellen)**.

> **HINWEIS:** Dieses Menüelement wird nur angezeigt, wenn alle anwendbaren Patches über einen Zeitplan für Erkennung, Staging und bedarfsgerechte Bereitstellung von Patches oder Windows-Funktionen auf das Agent-Gerät heruntergeladen werden. Weitere Informationen hierzu finden Sie unter Konfigurieren von Patch-Zeitplänen.

7. Klicken Sie zum Aufrufen von Links, die sich auf Agenten beziehen, im Menü auf **Shortcuts (Verknüpfungen)** und dann ggf. auf einen Link. Alle Standard-URI-Links (Uniform Resource Identifier) werden unterstützt, wie z. B. `https`-, `ssh`- und `ftp`-URLs.

   Dieses Menüelement wird nur angezeigt, wenn der Systemadministrator einen oder mehrere Links festlegt. Weitere Informationen hierzu finden Sie unter Agentenkommunikation und Protokolleinstellungen konfigurieren.

   Wenn Sie auf diesen Link klicken, startet Ihr Betriebssystem die Anwendung, die mit der ausgewählten Ressource verknüpft ist. Wenn Sie beispielsweise auf einen Link vom Typ HTTP klicken, öffnet Ihr System den Link im Standardbrowser.

8. Um mehr über die Agentenanwendung zu erfahren, klicken Sie auf **Info**.

KACE Agent auf Linux-Geräten manuell bereitstellen und aktualisieren

Sie können den KACE Agent gegebenenfalls manuell auf Linux-Geräten bereitstellen oder aktualisieren.

KACE Agent auf Linux Geräten manuell bereitstellen

Sie können den KACE Agent auf Linux Geräten manuell bereitstellen, indem Sie die Agenteninstallationsdateien auf das Gerät kopieren und Installationsbefehle ausführen.

1. Kopieren Sie die Installationsdatei für den KACE Agent auf das Gerät.

   Siehe Agenteninstallationsdateien abrufen.

2. Wenn Sie den Agenten bei der Appliance registrieren möchten:

   - Verwenden Sie die Umgebungsvariablen `KACE_HOST` und `KACE_TOKEN`, um den Hostnamen und das Agent-Token der Appliance anzugeben, bevor Sie die Installationsdatei ausführen. Oder:
   - Ändern Sie den Namen der Installationsdatei manuell mithilfe der folgenden Syntax: `<agent_installation_filename>_<appliance_hostname>+<agent_token>.<extension>`

   Sie können die Zeichenfolge des Agent-Tokens auf der Seite *Agent Token Detail (Details zum Agent-Token)* abrufen. Weitere Informationen finden Sie unter Registrieren des KACE Agent bei der Appliance.

3. Öffnen Sie ein Terminalfenster über **Anwendungen** > **System-Tools**.
4. Legen Sie über die Eingabeaufforderung den Namen des Servers fest und installieren Sie den Agenten:

```
sudo KACE_SERVER=kace_sma_name rpm -Uvh ampagent-x.x.xxxxx-x.i386.rpm
```

Der Agent wird in den folgenden Verzeichnissen installiert:

- `/opt/quest/kace/bin/`: Hier werden die ausführbaren Dateien des Agenten installiert.
- `/var/quest/kace/`: Hier werden Konfiguration, Protokolle und andere Daten des Agenten gespeichert.

Die Geräteinformationen werden innerhalb weniger Minuten im **Inventar** der Appliance angezeigt. Siehe Verwalten von Anwendungen auf der Seite "Software".

KACE Agent auf Linux Geräten beim Systemstart oder bei der Anmeldung bereitstellen

Sie können festlegen, dass der Agent beim Start eines Linux Geräts oder bei der Anmeldung an einem Linux Gerät bereitgestellt werden soll.

- Legen Sie den Namen fest, indem Sie den folgenden Befehl zum Stammverzeichnis hinzufügen:

  ```
  export KACE_SERVER=kace_sma_name
  ```

  Der `export`-Aufruf muss dem Aufruf an die Installationsdatei vorangehen. Beispiel: `export KACE_SERVER=kace_sma_name rpm -Uvh kace_sma_agent-12345.i386.rpm`

  Das System sucht an diesen Speicherorten im angezeigten Ordner nach dem Wert des **Hosts**:

  1. Die Installationsdatei
  2. `KACE_SERVER` (Umgebungsvariable)
  3. Die Datei `amp.conf`

  Wenn Sie den Agenten bei der Appliance registrieren möchten:

  - Verwenden Sie die Umgebungsvariablen `KACE_HOST` und `KACE_TOKEN`, um den Hostnamen und das Agent-Token der Appliance anzugeben, bevor Sie die Installationsdatei ausführen. Oder:
  - Ändern Sie den Namen der Installationsdatei manuell mithilfe der folgenden Syntax: `<agent_installation_filename>_<appliance_hostname>+<agent_token>.<extension>`

  Sie können die Zeichenfolge des Agent-Tokens auf der Seite *Agent Token Detail (Details zum Agent-Token)* abrufen. Weitere Informationen finden Sie unter Registrieren des KACE Agent bei der Appliance

  VORSICHT: Wenn Sie den Wert des Hosts leer lassen, müssen Sie die Umgebungsvariable festlegen. Andernfalls stellt der Agent keine Verbindung mit der Appliance her. Quest empfiehlt, den vollständig qualifizierten Domänennamen als Hostnamen zu verwenden.

KACE Agent auf Linux Geräten aktualisieren

Sie können den KACE Agent manuell auf Linux Geräten aktualisieren, indem Sie auf den Geräten bestimmte Befehle ausführen.

1. Kopieren Sie die Installationsdatei für den KACE Agent auf das Gerät. Siehe Agenteninstallationsdateien abrufen.
2. Wenn Sie den Agenten bei der Appliance registrieren möchten:
   - Verwenden Sie die Umgebungsvariablen `KACE_HOST` und `KACE_TOKEN`, um den Hostnamen und das Agent-Token der Appliance anzugeben, bevor Sie die Installationsdatei ausführen. Oder:
   - Ändern Sie den Namen der Installationsdatei manuell mithilfe der folgenden Syntax: `<agent_installation_filename>_<appliance_hostname>+<agent_token>.<extension>`

Sie können die Zeichenfolge des Agent-Tokens auf der Seite *Agent Token Detail (Details zum Agent-Token)* abrufen. Weitere Informationen finden Sie unter Registrieren des KACE Agent bei der Appliance.

3. Öffnen Sie ein Terminalfenster über **Anwendungen > System-Tools**.
4. Geben Sie in der Eingabeaufforderung Folgendes ein:

```
rpm -uvh kace_sma_agent-linux_buildnumber.rpm
```

Agentenvorgänge auf Linux Geräten ausführen

Sie können Befehle auf Linux Geräten mit Agentenverwaltung ausführen, um verschiedene Agentenvorgänge durchzuführen.

Agent auf Linux Geräten starten und beenden

Sie können Befehle auf Linux Geräten ausführen, um den Agenten zu starten und zu beenden. Dies ist beim Beheben agentenbezogener Probleme hilfreich.

1. Öffnen Sie ein Terminalfenster über **Anwendungen > System-Tools**.
2. Geben Sie zum Starten des Agenten Folgendes ein:

```
/opt/quest/kace/bin/AMPTools start
```

3. Geben Sie zum Beenden des Agenten Folgendes ein:

```
/opt/quest/kace/bin/AMPTools stop
```

Agent manuell von Linux Geräten entfernen

Sie können den Agenten manuell von Linux Geräten entfernen, indem Sie auf den Geräten bestimmte Befehle ausführen.

1. Öffnen Sie ein Terminalfenster über **Anwendungen > System-Tools**.
2. Geben Sie in der Eingabeaufforderung Folgendes ein:

```
sudo rpm -e ampagent
```

3. **Optional**: Entfernen Sie das Verzeichnis `kace`:

```
rm -rf /var/quest/kace/
```

Linux Geräte auf Ausführung des Agenten prüfen

Durch Ausführen eines Befehls können Sie den Ausführungsstatus des Agenten auf Linux Geräten ermitteln.

1. Öffnen Sie ein Terminalfenster über **Anwendungen > System-Tools**.
2. Geben Sie in der Befehlszeile Folgendes ein:

```
ps aux | grep AMPAgent
```

Diese Ausgabe gibt an, dass der Prozess ausgeführt wird:

```
root 6100 0.0 3.9 3110640 20384 ? Ssl Mar03 0:00 /opt/quest/kace/bin/AMPAgent
--daemon
```

Agenten-Version auf Linux Geräten anzeigen

Durch Ausführen eines Befehls können Sie die auf Linux Geräten installierte Version des Agenten überprüfen.

1. Öffnen Sie ein Terminalfenster über **Anwendungen > System-Tools**.
2. Geben Sie in der Eingabeaufforderung Folgendes ein:

```
rpm -q ampagent
```

Die Versionsnummer wird angezeigt.

Inventarinformationen sammeln

Durch Erzwingen von Inventaraktualisierungen können Sie Inventar auf Linux Geräten manuell erfassen.

Siehe Erzwingen von Inventaraktualisierungen.

KACE Agent auf Mac-Geräten manuell bereitstellen und aktualisieren

Sie können den Agenten gegebenenfalls manuell auf Mac Geräten bereitstellen oder aktualisieren.

Dieser Abschnitt enthält Informationen zur manuellen Bereitstellung des KACE Agent auf Mac OS X-Geräten. Weitere Optionen werden im Abschnitt Shellskripte zum Bereitstellen des KACE Agent verwenden beschrieben.

HINWEIS: Einige Befehle müssen als **root** ausgeführt werden.
HINWEIS: Fahren Sie je nach Bedarf mit `su` oder mit `sudo` fort.

KACE Agent mithilfe des Agenten-Installationsprogramms auf Mac Geräten bereitstellen oder aktualisieren

Sie können den KACE Agent auf Mac Geräten manuell bereitstellen, indem Sie die Agenteninstallationsdateien auf das Gerät kopieren und das Installationsprogramm ausführen.

1. Kopieren Sie die Installationsdatei für den KACE Agent auf das Gerät.

   Siehe Agenteninstallationsdateien abrufen.

2. Wenn Sie den Agenten bei der Appliance registrieren möchten:

   - Verwenden Sie die Umgebungsvariablen `KACE_HOST` und `KACE_TOKEN`, um den Hostnamen und das Agent-Token der Appliance anzugeben, bevor Sie die Installationsdatei ausführen. Oder:
   - Ändern Sie den Namen der Installationsdatei manuell mithilfe der folgenden Syntax: `<agent_installation_filename>_<appliance_hostname>+<agent_token>.<extension>`

   Sie können die Zeichenfolge des Agent-Tokens auf der Seite *Agent Token Detail (Details zum Agent-Token)* abrufen. Weitere Informationen finden Sie unter Registrieren des KACE Agent bei der Appliance.

3. Doppelklicken Sie auf **ampagent-x.x.build_number.dmg**.
4. Doppelklicken Sie auf die Datei **AMPAgent.pkg**.
5. Befolgen Sie die Anweisungen des Installationsprogramms.

   Geben Sie den Namen Ihrer Appliance ein.

Das Installationsprogramm erstellt die folgenden Verzeichnisse auf dem Gerät:

- `/Library/Application Support/Quest/KACE/bin`: Hier werden die ausführbaren Dateien des Agenten installiert.
- `/Library/Application Support/Quest/KACE/data/`: Hier werden Konfiguration, Protokolle und andere Daten des Agenten gespeichert.

Agenten mithilfe des Terminalfensters auf Mac Geräten bereitstellen

Sie können den KACE Agent auf Mac Geräten manuell bereitstellen, indem Sie die Agenteninstallationsdateien auf das Gerät kopieren und bestimmte Befehle ausführen.

1. Kopieren Sie die Installationsdatei für den KACE Agent auf das Gerät.

Siehe Agenteninstallationsdateien abrufen.

2. Wenn Sie den Agenten bei der Appliance registrieren möchten:
   - Verwenden Sie die Umgebungsvariablen `KACE_HOST` und `KACE_TOKEN`, um den Hostnamen und das Agent-Token der Appliance anzugeben, bevor Sie die Installationsdatei ausführen. Oder:
   - Ändern Sie den Namen der Installationsdatei manuell mithilfe der folgenden Syntax: `<agent_installation_filename>_<appliance_hostname>+<agent_token>.<extension>`

   Sie können die Zeichenfolge des Agent-Tokens auf der Seite *Agent Token Detail (Details zum Agent-Token)* abrufen. Weitere Informationen finden Sie unter Registrieren des KACE Agent bei der Appliance.
3. Öffnen Sie ein Terminalfenster über **Anwendungen > Dienstprogramme**.
4. Geben Sie in der Eingabeaufforderung die folgenden Befehle ein, um den Namen des Servers festzulegen und den Agenten zu installieren:

```
hdiutil attach ./ampagent-x.x.xxxxx-all.dmg
```

```
sudo sh -c 'KACE_SERVER=kace_sma_name installer -pkg /Volumes/Quest_KACE/
AMPAgent.pkg -target /'
```

```
hdiutil detach '/Volumes/Quest_KACE'
```

Shellskripte zum Bereitstellen des KACE Agent verwenden

Sie können den Agenten durch Ausführen von Shellskripten auf Mac Geräten bereitstellen.

Wenn Sie Shellskripte zum Bereitstellen des Agenten verwenden, können Sie folgende Befehlszeilenoptionen verwenden:

- `hdiutil attach ./ampagent-6.x.xxxxx-all.dmg`
- `sudo sh -c 'KACE_SERVER=kace_sma_name installer -pkg`
- `/Volumes/Quest_KACE/AMPAgent.pkg -target /'`
- `hdiutil detach '/Volumes/Quest_KACE'`

> **HINWEIS:** Der export-Aufruf muss den install-Aufruf fortsetzen. Beispiel: `sudo export KACE_SERVER=kace_sma_name installer -pkg '/Volumes/Dell KACE/AMPAgent.pkg' -target /`

Das System sucht an diesen Speicherorten in der angezeigten Reihenfolge nach dem Wert des **Hosts**:

1. Die Installationsdatei
2. `KACE_SERVER` (Umgebungsvariable)
3. Die Datei `amp.conf`

Wenn Sie den Agenten bei der Appliance registrieren möchten:

- Verwenden Sie die Umgebungsvariablen `KACE_HOST` und `KACE_TOKEN`, um den Hostnamen und das Agent-Token der Appliance anzugeben, bevor Sie die Installationsdatei ausführen. Oder:
- Ändern Sie den Namen der Installationsdatei manuell mithilfe der folgenden Syntax: `<agent_installation_filename>_<appliance_hostname>+<agent_token>.<extension>`

Sie können die Zeichenfolge des Agent-Tokens auf der Seite *Agent Token Detail (Details zum Agent-Token)* abrufen. Weitere Informationen finden Sie unter Registrieren des KACE Agent bei der Appliance

Informationen zur Verwendung von Shellskripten und Befehlszeilen finden Sie unter http://developer.apple.com.

> **VORSICHT: Wenn Sie den Wert des Hosts leer lassen, müssen Sie die Umgebungsvariable festlegen. Andernfalls stellt der Agent keine Verbindung mit der Appliance her. Quest KACE empfiehlt, den vollständig qualifizierten Domänennamen als Hostnamen zu verwenden.**

Andere Agenten-Vorgänge auf Mac Geräten ausführen

Sie können Befehle auf Mac Geräten mit Agentenverwaltung ausführen, um verschiedene Vorgänge durchzuführen.

Agenten auf Mac Geräten starten und beenden

Sie können Befehle auf Mac Geräten ausführen, um den Agenten zu starten und zu beenden. Dies ist beim Beheben agentenbezogener Probleme hilfreich.

1. Öffnen Sie ein Terminalfenster über **Anwendungen > Dienstprogramme**.
2. Geben Sie Folgendes ein:

   ```
   cd "Library/Application Support/Quest/KACE/bin"
   ```

3. Geben Sie zum Starten des Agenten Folgendes ein:

   ```
   ./AMPTools start
   ```

4. Geben Sie zum Beenden des Agenten Folgendes ein:

   ```
   ./AMPTools stop
   ```

Agenten manuell von Mac Geräten entfernen

Sie können den Agenten manuell von Mac Geräten entfernen, indem Sie auf den Geräten bestimmte Befehle ausführen.

1. Öffnen Sie ein Terminalfenster über **Anwendungen > Dienstprogramme**.
2. Geben Sie Folgendes ein:

   ```
   sudo "/Library/Application Support/Quest/KACE/bin/AMPTools" uninstall
   ```

Der Agent wird entfernt.

Ausführung des Agenten auf Mac Geräten überprüfen

Durch Ausführen eines Befehls können Sie den Ausführungsstatus des Agenten auf Mac Geräten ermitteln.

1. Öffnen Sie ein Terminalfenster über **Anwendungen > Dienstprogramme**.
2. Geben Sie den folgenden Befehl ein:

   ```
   ps aux | grep AMPAgent
   ```

   Diese Ausgabe gibt an, dass der Prozess ausgeführt wird:

   ```
   root 2159 0.0 1.1 94408 12044 p2 S 3:26PM 0:10.94 /Library/Application Support/
   Quest/KACE/AMPAgent
   ```

Version des Agenten auf Mac Geräten überprüfen

Durch Ausführen eines Befehls können Sie die auf Mac Geräten installierte Version des Agenten überprüfen.

1. Öffnen Sie ein Terminalfenster über **Anwendungen > Dienstprogramme**.
2. Geben Sie den folgenden Befehl ein:

   ```
   cat /Library/Application\ Support/Quest/KACE/data/version
   ```

   Die Versionsnummer wird angezeigt.

Inventarinformationen auf Mac Geräten sammeln

Durch Erzwingen von Inventaraktualisierungen können Sie Informationen auf Mac Geräten manuell erfassen.

Siehe Erzwingen von Inventaraktualisierungen.

Verwalten des KACE Agent auf Mac-Geräten über die Menüleiste

Sie können über die Mac-Menüleiste den Status des KACE Agent anzeigen, eine Bestandsaufnahme erzwingen und die Agenteninformationen anzeigen.

Um den KACE Agent-Status über die Mac-Menüleiste aufzurufen, müssen Sie im Abschnitt *Agenten- und Kommunikationseinstellungen* die Option **Agenten-Status auf Gerät** aktivieren. Weitere Informationen hierzu finden Sie unter Agentenkommunikation und Protokolleinstellungen konfigurieren.

1. Klicken Sie auf dem Gerät, auf dem der KACE Agent ausgeführt wird, in der Mac-Menüleiste auf .

   Die Anzeige in der unteren rechten Ecke des Symbols gibt Auskunft über den Status des Agenten:

   - : Der Agent ist mit der Appliance verbunden.
   - : Der Agent befindet sich im Snooze-Modus.
   - : Der Agent weist ausstehende Aktionen auf.
   - : Der Agent ist von der Appliance getrennt.

   Das Menü „Agent“ wird angezeigt.
2. Um herauszufinden, ob der Agent mit der Appliance verbunden ist, beachten Sie das Statussymbol im Menü.

   Hierbei handelt es sich um die gleiche Anzeige wie oben beschrieben, die auf dem Agent-Symbol angezeigt wird und darüber Auskunft gibt, ob der Agent verbunden ist, sich im Snooze-Modus befindet, ausstehende Aktionen aufweist oder von der Appliance getrennt wurde.
3. Um die Gerätebestandsaufnahme auszuführen, klicken Sie im Menü auf **Bestandsaufnahme**.
4. Um den Agenten neu zu starten, klicken Sie auf **Agent neu starten** im Menü.
5. Um die Aktivität des Agenten während eines bestimmten Zeitraums vorübergehend zu unterbrechen, klicken Sie auf **Agent im Snooze-Modus** und wählen Sie einen Zeitraum im Menü aus. Sie können den Agent für 15 Minuten, 30 Minuten, eine Stunde oder zwei Stunden lang in den Snooze-Modus versetzen.

   > **HINWEIS:** Sie können die Snooze-Funktion nur dann aktivieren, wenn die Option **Agent auf Gerät im Snooze-Modus** im Abschnitt *Agent und Kommunikationseinstellungen* auf der Appliance aktiviert ist und die maximale Anzahl von Snooze-Modus-Aktivierungen noch nicht erreicht wurde. Weitere Informationen hierzu finden Sie unter Agentenkommunikation und Protokolleinstellungen konfigurieren.

   Durch die Aktivierung des Snooze-Modus für einen Agenten werden keine laufenden Agentenprozesse auf dem Gerät gestoppt. Sie verhindert nur, dass der Agent einen neuen Prozess startet. Wenn die Aktivierung der Agenten-Snooze-Funktion nicht möglich ist, z. B. aufgrund der Konfiguration, wird eine Fehlermeldung angezeigt.
6. Klicken Sie zum Aufrufen von Links, die sich auf Agenten beziehen, im Menü auf **Shortcuts (Verknüpfungen)** und dann ggf. auf einen Link. Alle Standard-URI-Links (Uniform Resource Identifier) werden unterstützt, wie z. B. `https`-, `ssh`- und `ftp`-URLs.

   Dieses Menüelement wird nur angezeigt, wenn der Systemadministrator einen oder mehrere Links festlegt. Weitere Informationen hierzu finden Sie unter Agentenkommunikation und Protokolleinstellungen konfigurieren.

   Wenn Sie auf diesen Link klicken, startet Ihr Betriebssystem die Anwendung, die mit der ausgewählten Ressource verknüpft ist. Wenn Sie beispielsweise auf einen Link vom Typ HTTP klicken, öffnet Ihr System den Link im Standardbrowser.
7. Um mehr über die Agentenanwendung zu erfahren, klicken Sie auf **Info**.
8. Um die Agentenanwendung aus der Mac-Menüleiste zu entfernen, klicken Sie auf **Beenden**.

   Das Symbol „Agent“ wird aus der Menüleiste entfernt. Um es erneut anzuzeigen, melden Sie sich ab und melden sich dann wieder an. Alternativ können Sie den Agenten auch erneut aus dem `Anwendungsverzeichnis` installieren.

Vom Agenten gesammelte Informationen anzeigen

Sie können sich die vom Agenten erfassten Inventarinformationen auf der Seite *Gerätedetail* ansehen.

Siehe Verwalten von Inventarinformationen.

Verwenden der Verwaltung ohne Agent

Verwenden Sie die Geräteverwaltung ohne Agent, wenn Sie Geräte verwalten möchten, ohne die KACE Agent-Software auf diesen Geräten bereitzustellen und zu verwalten.

Informationen zur Verwaltung ohne Agent

Die Geräteverwaltung ohne Agent ist ein Verfahren zur Verwaltung von Geräten, ohne dass dafür die KACE Agent-Software auf diesen Geräten bereitgestellt und gewartet werden muss.

Die Verwaltung ohne Agent nutzt SSH, SNMP und andere Verfahren für die Verbindung mit Geräten, die keine Agenten unterstützen, wie Drucker, Netzwerkgeräte und Speichergeräte, und meldet das Inventar in der Appliance **Administratorkonsole**. Die Verwendung der Verwaltung ohne Agent ist hilfreich bei Betriebssystemversionen und -distributionen, die vom KACE Agent nicht unterstützt werden, sowie in Fällen, in denen die Verwaltung ohne Agent der Agenteninstallation vorgezogen wird.

Es gibt einige Unterschiede bei den unterstützten Funktionen für Geräte mit und ohne Agent. Siehe Funktionen, die für jede einzelne Geräteverwaltungsmethode zur Verfügung stehen.

Von der Verwaltung ohne Agent unterstützte Betriebssysteme

Die Verwaltung ohne Agent unterstützt eine Reihe unterschiedlicher Gerätebetriebssysteme.

Die folgende Tabelle enthält die von der Verwaltung ohne Agent unterstützten Gerätebetriebssysteme:

Betriebssystem
CentOS
Chrome-Betriebssystem
Debian
Fedora
FreeBSD
Mac OS X
Oracle Enterprise Linux
Red Hat Enterprise Linux*
SUSE*
Solaris

Betriebssystem
Ubuntu*
Windows
Windows Server

*Die neuesten Versionen können auch mit dem KACE Agent verwaltet werden.

HINWEIS: Für computerfremde Geräte (beispielsweise Assets) oder Geräte ohne unterstützte Betriebssysteme können Sie bestimmten Feldern in der Inventartabelle SNMP-OIDs (Simple Network Management Protocol Object Identifiers) zuordnen. Dadurch können Sie bestimmte, zu inventarisierende Geräte identifizieren, um das Inventar von Geräten zu erweitern, die ohne Agent verwaltet werden. Siehe Erkennen bestimmter, dem Inventar hinzuzufügender SNMP-Objekte und Nicht-Computer-Geräte mithilfe von SNMP-Inventarkonfigurationen.

Informationen zur Aktivierung der Verwaltung ohne Agent auf Geräten mit Agentenverwaltung

Die Verwaltung ohne Agent kann für jedes erkannte Gerät aktiviert werden, einschließlich von Geräten, auf denen der KACE Agent installiert ist.

Es ist jedoch nicht empfehlenswert, beide Methoden auf ein und demselben Gerät einzusetzen. Bei Verwendung beider Methoden auf einem Gerät erscheinen sowohl das Gerät als auch dessen Software zweimal in den Inventarlisten. Daher empfiehlt es sich, die Verwaltung ohne Agent auf Geräten mit Agentenverwaltung nicht zu aktivieren.

Geräte ohne Agent verwalten

Um Geräte zu verwalten, ohne die KACE Agent-Software zu installieren, können Sie die Verwaltung ohne Agenten aktivieren und die Erkennungsinformationen verwenden oder indem Sie die Geräteverbindungsdetails manuell eingeben.

Die auf Geräten ohne Agent verfügbaren Funktionen unterscheiden sich von denen, die für Geräte mit Agentenverwaltung zur Verfügung stehen. Siehe Funktionen, die für jede einzelne Geräteverwaltungsmethode zur Verfügung stehen.

Verwaltung ohne Agenten unter Verwendung von Erkennungsinformationen aktivieren

Sie können die Verwaltung ohne Agenten unter Verwendung von Erkennungsinformationen aktivieren.

1. Rufen Sie die Liste *Erkennungsergebnisse* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Inventar** und anschließend auf **Erkennungsergebnisse**.
2. Aktivieren Sie das Kontrollkästchen neben einem oder mehreren Geräten.
3. Wählen Sie **Aktion auswählen** > **Provisionieren** > **Ohne Agent: Automatisch** aus.

   Für die ausgewählten Geräte wird die Verwaltung ohne Agent aktiviert und neben den Gerätenamen wird eines der folgenden Symbole angezeigt:

: Für das Gerät ist die Verwaltung ohne Agent aktiviert.

: Für das Gerät ist die Verwaltung ohne Agent aktiviert, das Gerät ist jedoch derzeit nicht erreichbar.

Je nach Gerät verwendet die Appliance unterschiedliche Verbindungstypen, um Befehle auf den ausgewählten Geräten auszuführen, Inventarinformationen abzurufen und diese auf der *Gerätedetailseite* anzuzeigen. Informationen werden gemäß dem Inventarisierungszeitplan für Geräte ohne Agent aktualisiert. Siehe:

- Verwalten von Inventarinformationen
- Inventardatensammlung für verwaltete Geräte planen

Verwaltung ohne Agent durch manuelle Eingabe von Geräteinformationen aktivieren

Sie können die Verwaltung ohne Agent aktivieren, indem Sie Geräteinformationen manuell eingeben.

Sie können unter folgenden Verbindungstypen wählen: SSH, SNMP, WinRM und VMware. WinRM ist der Verbindungstyp für Windows Geräte.

1. Rufen Sie die Liste *Geräte* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Inventar** und anschließend auf **Dashboard**.
2. Wählen Sie **Aktion auswählen** > **Neu** > **Gerät ohne Agent**, um die Seite *Details zur Geräteverbindung ohne Agent* anzuzeigen.
3. Geben Sie Informationen für die Art der Verbindung an.
   - **Um neue SSH-Verbindungen mit Geräten einzurichten, müssen Sie die folgenden Informationen eingeben:**

Option	Beschreibung
Name	Der Hostname oder die IP-Adresse des Geräts.
Asset-Untertyp	Die Asset-Unterkategorie, falls zutreffend. So können Sie Untertypen von Assets, z. B. Geräte-Assets wie Computer, Drucker, Router sowie Software-Assets, die auf Windows, Mac oder Linux Systemen im Inventar ausgeführt werden, erkennen und verwalten. Siehe Informationen zu Asset-Untertypen, benutzerdefinierten Feldern und Gerätedetail-Voreinstellungen.

Option	Beschreibung
	HINWEIS: In einer Standardinstallation umfassen die Gerätebestände zwei Asset-Untertypen für Druckergeräte: *Laserdrucker: Farb-* und *Laserdrucker: Monochrom*. Jeder dieser Untertypen bietet eine gemeinsame Gruppe von Feldern, die für die meisten Drucker gelten. Die Appliance verfügt außerdem über eine Reihe von Druckervorlagen für typische SNMP-fähige Druckermodelle, basierend auf diesen Asset-Untertypen. Sie können nach Bedarf diese Vorlagen bearbeiten oder neue hinzufügen. Wenn Sie eine Druckervorlage auf ein Gerät anwenden, werden die in der Vorlage definierten Daten, wie z. B. Tonerfüllstände oder Beschreibungen, für den Drucker im nächsten Bestandzyklus erfasst. Weitere Informationen hierzu finden Sie unter Informationen zu Druckervorlagen.
Verbindungstyp	Die Verbindungsmethode, mit der die Geräteverbindung hergestellt wird und Inventarinformationen abgerufen werden (in diesem Fall: SSH).
Port	Die Port-Nummer, über die die Appliance die Verbindung zum Gerät herstellt. Für folgende Standard-Port-Nummer (22) ist keine Eingabe erforderlich.
Anmeldeinformationen	Die Details des Dienstkontos, die erforderlich sind, um eine Verbindung zum Gerät herzustellen und Befehle auszuführen Wählen Sie vorhandene Anmeldeinformationen in der Dropdown-Liste aus oder wählen Sie **Neue Anmeldeinformationen hinzufügen** aus, um nicht bereits aufgeführte Anmeldeinformationen hinzuzufügen. Siehe Hinzufügen und Bearbeiten von Benutzer-/Kennwort-Anmeldeinformationen.
Sudo-Kennwort	Der Name eines Dienstbenutzerkontos, das berechtigt ist, die Verbindung zu Geräten herzustellen. Die Verwendung eines Dienstkontos und eines Sudo-Kennworts ist sinnvoll, wenn Sie vermeiden möchten, dass der Zugriff auf Geräte mit Root-Anmeldeinformationen erfolgt. Auf einigen Geräten kann die Appliance bei Verwendung höherer Berechtigungen jedoch detailliertere Inventarinformationen abrufen.
Betriebssystem	Das Betriebssystem des Geräts.
Shell	Die bei Verbindungen zu verwendende Shell. Siehe Shell-Unterstützung für SSH-Verbindungen.

Option	Beschreibung
Protokollebene	Die Ausführlichkeit, mit der Informationen auf der Seite *Gerätedetail* angezeigt werden sollen. Um nur die wichtigsten Meldungen angezeigt zu bekommen, wählen Sie **Kritisch** aus. Um alle Meldungen zu sehen, wählen Sie **Debug** aus.
Inventar aktivieren	Dies ist die Option zur Erfassung von Inventar. Ist diese Option ausgewählt, erfasst die Appliance Inventarinformationen für das Gerät gemäß dem Inventarisierungszeitplan des Geräts ohne Agent. Ist die Option nicht ausgewählt, werden keine Inventarinformationen erfasst. In beiden Fällen werden Geräte ohne Agent jedoch angerechnet.
DNS-Server	Der Hostname des DNS-Servers für die Identifikation des Gerätehostnamens und anderer Informationen. Durch Angabe der DNS-Serverinformationen kann die Appliance das Gerät bei Aktualisierungen anhand vorhandener Inventarinformationen abgleichen. Wenn die Appliance das Gerät aufgrund von Änderungen am Hostnamen oder der IP-Adresse des Geräts nicht erkennen kann, schlägt die Erfassung des Inventars fehl.
Relay-Gerät	Der Name des Geräts, das als Relay für die agentenlose Gerätebestandsaufnahme verwendet werden soll. Ein Relay-Gerät, das während der Ermittlung verwendet wird, wenn ein neues Gerät von den Ermittlungsergebnissen automatisch durch ein neues Gerät bereitgestellt wird. Sie können ein Relay-Gerät auf der Seite *Detail zum Erkennungszeitplan* auswählen. Weitere Informationen hierzu finden Sie unter Erkennungszeitplan für die Durchführung eines schnellen „Was und wo“-Scans in Ihrem Netzwerk hinzufügen.

- **Um neue SNMP-Verbindungen mit Geräten einzurichten, müssen Sie die folgenden Informationen eingeben:**

Option	Beschreibung
Name	Der Hostname oder die IP-Adresse des Geräts.
Asset-Untertyp	Die Asset-Unterkategorie, falls zutreffend. So können Sie Untertypen von Assets, z. B. Geräte-Assets wie Computer, Drucker oder Router sowie Software-Assets, die auf Windows, Mac oder Linux Systemen im Inventar ausgeführt werden, erkennen und verwalten. Siehe Informationen zu Asset-Untertypen, benutzerdefinierten Feldern und Gerätedetail-Voreinstellungen.

Option	Beschreibung
	HINWEIS: In einer Standardinstallation umfassen die Gerätebestände zwei Asset-Untertypen für Druckergeräte: *Laserdrucker: Farb-* und *Laserdrucker: Monochrom*. Jeder dieser Untertypen bietet eine gemeinsame Gruppe von Feldern, die für die meisten Drucker gelten. Die Appliance verfügt außerdem über eine Reihe von Druckervorlagen für typische SNMP-fähige Druckermodelle, basierend auf diesen Asset-Untertypen. Sie können nach Bedarf diese Vorlagen bearbeiten oder neue hinzufügen. Wenn Sie eine Druckervorlage auf ein Gerät anwenden, werden die in der Vorlage definierten Daten, wie z. B. Tonerfüllstände oder Beschreibungen, für den Drucker im nächsten Bestandzyklus erfasst. Weitere Informationen hierzu finden Sie unter Informationen zu Druckervorlagen.
Verbindungstyp	Die Verbindungsmethode, mit der die Geräteverbindung hergestellt wird und Inventarinformationen abgerufen werden (in diesem Fall: SNMP). SNMP (Simple Network Management Protocol) ist ein Protokoll zum Überwachen von verwalteten Geräten in einem Netzwerk. Zur Aktivierung von SNMP muss Port 161 auf der Appliance und dem Gerät geöffnet sein. Die Ergebnisse des SNMP-Scans enthalten alle SNMP-fähigen Geräte. Remote Shell-Erweiterungen versetzen die Appliance in die Lage, Verbindungen herzustellen, Befehle auszuführen sowie Informationen zu erfassen, die als Inventar verwaltet werden können. Weitere Informationen über SNMP-Optionen finden Sie unter Hinzufügen eines Erkennungszeitplans für SNMP-fähige computerfremde Geräte.
SNMP-Version	Die für Verbindungen zu verwendende SNMP-Version. SNMPv1 und SNMPv2c setzen weder Authentifizierung noch Verschlüsselung ein. SNMP v3 verwendet Authentifizierungs- und Verschlüsselungsalgorithmen zur Erhöhung der Sicherheit von SNMP-Datenübertragungen. Wenn Sie die SNMP v3-Optionen konfigurieren, führt die Appliance einen SNMP v3-Scan für ausgewählte Geräte durch. Ist der Scan nicht erfolgreich, führt die Appliance einen SNMP v1-Scan mit der angegebenen **öffentlichen Zeichenfolge** durch.
Lese-Community	(SNMP v1, SNMP v2c) Die abzufragende Community-Zeichenfolge. Der Standardwert ist **Öffentlich**. Der öffentliche String ist nur erforderlich, wenn keine Authentifizierung erforderlich ist. Ist eine

Option	Beschreibung
	Authentifizierung erforderlich, gibt der Scan SNMP aktiviert ohne Systemdaten zurück.
Anmeldeinformationen	Die Details des Dienstkontos, die erforderlich sind, um mittels SNMP v3 eine Verbindung zum Gerät herzustellen und Befehle auszuführen Wählen Sie vorhandene Anmeldeinformationen in der Dropdown-Liste aus oder klicken Sie auf **Anmeldeinformationen verwalten**, um Anmeldeinformationen hinzuzufügen. Für SNMPv1 und SNMPv2c sind keine Anmeldeinformationen erforderlich. Siehe Hinzufügen und Bearbeiten von Benutzer-/Kennwort-Anmeldeinformationen.
Inventarkonfigurationen	Eine oder mehr Inventarkonfigurationen für das neue SNMP-Gerät ohne Agent, wie z. B. *Brother Laserdrucker: Farbe* und andere.
Inventartyp	Die zur Erfassung von Inventarinformationen verwendete Methode. • **Inventar**: Bei dieser Methode wird eine Teilmenge von Informationen gesammelt, beispielsweise IP-Adresse, MAC-Adresse und Gerätename. • **Inventar/Walk**: Bei dieser Methode wird ein vollständiger SNMP-Walk durchgeführt, um Inventarinformationen zu erfassen. Die Ergebnisse des vollständigen Durchlaufs finden Sie auf der Seite *Gerätedetail*. **HINWEIS:** Beim SNMP-Inventardurchlauf werden auf Windows-Geräten keine nicht-englischen Zeichen unterstützt. Werden nicht-englische Zeichen erkannt, meldet die SNMP-Inventarisierung einen Fehler und beendet das Laden von Inventarinformationen.
Protokollebene	Die Ausführlichkeit, mit der Informationen auf der Seite *Gerätedetail* angezeigt werden sollen. Um nur die wichtigsten Meldungen angezeigt zu bekommen, wählen Sie **Kritisch** aus. Um alle Meldungen zu sehen, wählen Sie **Debug** aus.
Inventar aktivieren	Dies ist die Option zur Erfassung von Inventar. Ist diese Option ausgewählt, erfasst die Appliance Inventarinformationen für das Gerät gemäß dem Inventarisierungszeitplan des Geräts ohne Agent. Ist die Option nicht ausgewählt, werden keine Inventarinformationen erfasst. In beiden Fällen werden Geräte ohne Agent jedoch angerechnet.
DNS-Server	Der Hostname des DNS-Servers für die Identifikation des Gerätehostnamens und

Option	Beschreibung
	anderer Informationen. Durch Angabe der DNS-Serverinformationen kann die Appliance das Gerät bei Aktualisierungen anhand vorhandener Inventarinformationen abgleichen. Wenn die Appliance das Gerät aufgrund von Änderungen am Hostnamen oder der IP-Adresse des Geräts nicht erkennen kann, schlägt die Erfassung des Inventars fehl.
Relay-Gerät	Der Name des Geräts, das als Relay für die agentenlose Gerätebestandsaufnahme verwendet werden soll. Ein Relay-Gerät, das während der Ermittlung verwendet wird, wenn ein neues Gerät von den Ermittlungsergebnissen automatisch durch ein neues Gerät bereitgestellt wird. Sie können ein Relay-Gerät auf der Seite *Detail zum Erkennungszeitplan* auswählen. Weitere Informationen hierzu finden Sie unter Erkennungszeitplan für die Durchführung eines schnellen „Was und wo“-Scans in Ihrem Netzwerk hinzufügen.

- **Geben Sie zum Einrichten neuer WinRM-Verbindungen mit Geräten folgende Informationen an:**

Option	Beschreibung
Name	Der Hostname oder die IP-Adresse des Geräts.
Asset-Untertyp	Die Asset-Unterkategorie, falls zutreffend. So können Sie Untertypen von Assets, z. B. Geräte-Assets wie Computer, Drucker oder Router sowie Software-Assets, die auf Windows, Mac oder Linux Systemen im Inventar ausgeführt werden, erkennen und verwalten. Siehe Informationen zu Asset-Untertypen, benutzerdefinierten Feldern und Gerätedetail-Voreinstellungen. **HINWEIS:** In einer Standardinstallation umfassen die Gerätebestände zwei Asset-Untertypen für Druckergeräte: *Laserdrucker: Farb-* und *Laserdrucker: Monochrom*. Jeder dieser Untertypen bietet eine gemeinsame Gruppe von Feldern, die für die meisten Drucker gelten. Die Appliance verfügt außerdem über eine Reihe von Druckervorlagen für typische SNMP-fähige Druckermodelle, basierend auf diesen Asset-Untertypen. Sie können nach Bedarf diese Vorlagen bearbeiten oder neue hinzufügen. Wenn Sie eine Druckervorlage auf ein Gerät anwenden, werden die in der Vorlage definierten Daten, wie z. B. Tonerfüllstände oder Beschreibungen, für den Drucker im nächsten Bestandzyklus erfasst. Weitere Informationen hierzu finden Sie unter Informationen zu Druckervorlagen.

Option	Beschreibung
Verbindungstyp	Die Verbindungsmethode, mit der die Verbindung mit dem Windows Gerät hergestellt wird und Inventarinformationen abgerufen werden (in diesem Fall: WinRM).
Port	Die Port-Nummer, über die die Appliance die Verbindung zum Gerät herstellt. Für folgende Standard-Port-Nummer ist keine Eingabe erforderlich: 5985.
Anmeldeinformationen	Die Details des Dienstkontos, die erforderlich sind, um eine Verbindung zum Gerät herzustellen und Befehle auszuführen Wählen Sie vorhandene Anmeldeinformationen in der Dropdown-Liste aus oder wählen Sie **Neue Anmeldeinformationen hinzufügen** aus, um nicht bereits aufgeführte Anmeldeinformationen hinzuzufügen. Siehe Hinzufügen und Bearbeiten von Benutzer-/Kennwort-Anmeldeinformationen.
Kerberos voraussetzen	Bei Verwendung dieser Option ist eine Kerberos-Authentifizierung erforderlich. Wenn Kerberos nicht verfügbar ist, wird NTLM nicht als Alternative verwendet. Für die Verwendung von Kerberos muss in der Erkennungskonfiguration auch DNS-Lookup aktiviert sein. Darüber hinaus muss in den lokalen Netzwerkeinstellungen der Appliance auch der DNS-Server angegeben werden.
Protokollebene	Die Ausführlichkeit, mit der Informationen auf der Seite *Gerätedetail* angezeigt werden sollen. Um nur die wichtigsten Meldungen angezeigt zu bekommen, wählen Sie **Kritisch** aus. Um alle Meldungen zu sehen, wählen Sie **Debug** aus.
Inventar aktivieren	Dies ist die Option zur Erfassung von Inventar. Ist diese Option ausgewählt, erfasst die Appliance Inventarinformationen für das Gerät gemäß dem Inventarisierungszeitplan des Geräts ohne Agent. Ist die Option nicht ausgewählt, werden keine Inventarinformationen erfasst. In beiden Fällen werden Geräte ohne Agent jedoch angerechnet.
DNS-Server	Der Hostname des DNS-Servers für die Identifikation des Gerätehostnamens und anderer Informationen. Durch Angabe der DNS-Serverinformationen kann die Appliance das Gerät bei Aktualisierungen anhand vorhandener Inventarinformationen abgleichen. Wenn die Appliance das Gerät aufgrund von Änderungen am Hostnamen oder der IP-Adresse des Geräts nicht erkennen kann, schlägt die Erfassung des Inventars fehl.

Option	Beschreibung
Bestandsaufnahme Hyper-V oder Virtual Machine Manager	Wählen Sie diese Option aus, damit die Appliance eine Microsoft Hyper-V- oder System Center Virtual Machine Manager-Infrastruktur mit agentenloser Verwaltung importieren kann. Weitere Informationen zu dieser Funktion finden Sie unter .
Relay-Gerät	Der Name des Geräts, das als Relay für die agentenlose Gerätebestandsaufnahme verwendet werden soll. Ein Relay-Gerät, das während der Ermittlung verwendet wird, wenn ein neues Gerät von den Ermittlungsergebnissen automatisch durch ein neues Gerät bereitgestellt wird. Sie können ein Relay-Gerät auf der Seite *Detail zum Erkennungszeitplan* auswählen. Weitere Informationen hierzu finden Sie unter Erkennungszeitplan für die Durchführung eines schnellen „Was und wo“-Scans in Ihrem Netzwerk hinzufügen.

- **Liefern Sie zur Einrichtung eines VMware®-Geräts folgende Informationen:**

Option	Beschreibung
Name	Den Host-Namen oder die IP-Adresse des ESXi-Hosts oder den vCenter-Server.
Asset-Untertyp	Die Asset-Unterkategorie, falls zutreffend. Diese Informationen ermöglichen die Identifizierung und Verwaltung von Subtypen von Assets wie VMware Geräte. Zum Beispiel Hypervisoren (ESXi-Hosts). Siehe Informationen zu Asset-Untertypen, benutzerdefinierten Feldern und Gerätedetail-Voreinstellungen.
Verbindungstyp	Die Verbindungsmethode, mit der die Verbindung mit dem VMware-Gerät hergestellt und Inventarinformationen abgerufen werden.
VMware-Typ	Der VMware-Gerätetyp: **ESXi** oder **vCenter Server**. **HINWEIS:** vCenter Server Geräte zählen nicht gegen die Gesamtanzahl von Gerätelizenzen. Der Grund dafür ist, dass diese Geräteinstanzen nur verwendet werden, um Beziehungen zwischen vCenter Servern, ESXi-Hosts und virtuellen Maschinen herzustellen.
Anmeldeinformationen	Die Details des Dienstkontos, die erforderlich sind, um eine Verbindung zum Gerät herzustellen und Befehle auszuführen Wählen Sie vorhandene Anmeldeinformationen in der Dropdown-Liste aus oder wählen Sie **Neue Anmeldeinformationen hinzufügen** aus, um nicht bereits aufgeführte Anmeldeinformationen hinzuzufügen. Ein Konto

Option	Beschreibung
	mit Nur-Lese-Zugriff kann verwendet werden. Siehe Hinzufügen und Bearbeiten von Benutzer-/Kennwort-Anmeldeinformationen.
Protokollebene	Die Ausführlichkeit, mit der Informationen auf der Seite *Gerätedetail* angezeigt werden sollen. Um nur die wichtigsten Meldungen angezeigt zu bekommen, wählen Sie **Kritisch** aus. Um alle Meldungen zu sehen, wählen Sie **Debug** aus.
Inventar aktivieren	Dies ist die Option zur Erfassung von Inventar. Ist diese Option ausgewählt, erfasst die Appliance Inventarinformationen für das Gerät gemäß dem Inventarisierungszeitplan des Geräts ohne Agent. Ist die Option nicht ausgewählt, werden keine Inventarinformationen erfasst. In beiden Fällen werden Geräte ohne Agent jedoch angerechnet.
DNS-Server	Der Hostname des DNS-Servers für die Identifikation des Gerätehostnamens und anderer Informationen. Durch Angabe der DNS-Serverinformationen kann die Appliance das Gerät bei Aktualisierungen anhand vorhandener Inventarinformationen abgleichen. Wenn die Appliance das Gerät aufgrund von Änderungen am Hostnamen oder der IP-Adresse des Geräts nicht erkennen kann, schlägt die Erfassung des Inventars fehl.

4. Klicken Sie auf **Verbindungstest**.

   Der Verbindungsstatus wird angezeigt.
5. Klicken Sie auf **Speichern**.

   Das Gerät ohne Agent wird hinzugefügt. Wenn *Inventar aktivieren* aktiviert ist, werden Inventarinformationen gemäß dem Inventarisierungszeitplan des Geräts ohne Agent aktualisiert. Siehe Inventardatensammlung für verwaltete Geräte planen.

Shell-Unterstützung für SSH-Verbindungen

Die Unterstützung von Shells für SSH-Verbindungen zwischen der Appliance und verwalteten Geräten unterscheidet sich von Betriebssystem zu Betriebssystem.

Die folgende Tabelle enthält die für jedes Betriebssystem jeweils verfügbaren Shells für SSH-Verbindungen.

Shell-Unterstützung für SSH-Verbindungen nach Betriebssystem

Betriebssystem	Standard-Shell	Unterstützte Shells
CentOS	bash	bash, sh
Debian Linux	bash	bash, sh
Fedora	bash	bash, sh
FreeBSD	csh	bash, csh, sh

Betriebssystem	Standard-Shell	Unterstützte Shells
Mac OS X	sh	bash, sh
openSUSE/SLES™	bash	bash, sh
Oracle Enterprise Linux	bash	bash, sh
Red Hat® Enterprise Linux®	bash	bash, sh
Ubuntu	bash	bash, sh

Details zur Geräteverbindung ohne Agent bearbeiten oder Geräte ohne Agent löschen

Sie können nach Bedarf die Details zur Geräteverbindung ohne Agent bearbeiten oder Geräte ohne Agent löschen.

1. Rufen Sie die Liste *Geräte* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Inventar** und anschließend auf **Dashboard**.
2. Klicken Sie auf den Namen eines manuell eingegebenen Geräts ohne Agent, um die *Gerätedetailseite* anzuzeigen.
3. Klicken Sie im Abschnitt *Übersicht* in der Zeile *Geräteeintragstyp* auf **Bearbeiten**, um die Seite *Details zur Geräteverbindung ohne Agent* anzuzeigen.
4. Führen Sie einen der folgenden Schritte aus:
   - **Ändern Sie die Verbindungsdetails nach Bedarf und klicken Sie dann auf Speichern. Siehe Verwaltung ohne Agent durch manuelle Eingabe von Geräteinformationen aktivieren.**
   - **Um das Gerät zu löschen, klicken Sie auf Löschen.**
   - **Klicken Sie für agentenlose Geräte, die bei KACE Cloud Mobile Device Manager (MDM) registriert sind, zum Entfernen der Gerätezuordnung zu KACE Cloud MDM und zum Zurücksetzen auf reine Agentenbestandsdatensätze auf Agentenlose Integration entfernen.**

Erkennen bestimmter, dem Inventar hinzuzufügender SNMP-Objekte und Nicht-Computer-Geräte mithilfe von SNMP-Inventarkonfigurationen

Dadurch können Sie bestimmte, zu inventarisierende SNMP-Geräte (Simple Network Management Protocol) und Nicht-Computer-Geräte identifizieren, um das Inventar gemäß Ihren Anforderungen zu erweitern oder einzuschränken. Darüber hinaus ermöglicht es Ihnen die Appliance, SNMP-Objektbezeichner (OIDs) mithilfe von Asset-Untertypen bestimmten Feldern in der Appliance-Inventartabelle zuzuordnen.

WICHTIG: Bei SNMP-Geräten müssen Sie bei der Gerätekonfiguration den entsprechenden Asset-Untertyp zuweisen. SNMP-Asset-Untertypen können nach der Konfiguration nicht mehr hinzugefügt oder geändert werden.

SNMP ist eine der Methoden, die das Appliance-Inventar ohne Agent verwendet, um Daten für das Inventar und die Integration in die Appliance zu extrahieren. Die Appliance verwendet die RFC1213 MIB (Management Information Base) als primäre Datenerfassungsschicht, da sich hier die spezifischen Daten aller SNMP-fähigen

Geräte befinden. Alle SNMP-fähigen Geräte stellen RFC1213-Daten bereit. Weitere Informationen hierzu finden Sie unter http://tools.ietf.org/html/rfc1213.

Mit der SNMP-Inventarkonfiguration der Appliance können Sie eine zusätzliche Gruppe von OIDs definieren, die bei der Inventarisierung zusätzlich zu den RFC1213-Standarddaten erfasst werden sollen. Dadurch können Sie einen Prozess, mit dem andernfalls nur ganz bestimmte Daten der einzelnen Geräte erfasst werden könnten, problemlos erweitern und robuster gestalten.

Verwandte Themen

Informationen zu Asset-Untertypen, benutzerdefinierten Feldern und Gerätedetail-Voreinstellungen

Liste der Objektbezeichner (OIDs) mithilfe der Administratorkonsole abrufen

Falls Sie nicht über eine vom Anbieter bereitgestellte Management Information Base (MIB) oder eine allgemein verfügbare MIB für ein Objekt verfügen, können Sie eine Liste mit Objektbezeichnern abrufen, indem Sie mithilfe der Appliance das Objekt überprüfen.

Sie können eine zusätzliche Gruppe von OIDs definieren, die bei der Inventarisierung zusätzlich zu den RFC1213-Standarddaten erfasst werden sollen. Dadurch erhöht sich die Datenmenge, die für die einzelnen Geräte erfasst werden können. Zum Aufrufen dieser OIDs können Sie einen MIB-Browser in MIBs verwenden, die Sie anderswo erhalten haben. Mit der Appliance können Sie über die Geräteerkennung oder Geräteinventarisierung einen vollständigen SNMP-Durchlauf ausführen, falls Sie sonst nicht auf eine MIB zugreifen können.

1. Führen Sie einen vollständigen SNMP-Durchlauf für ein Objekt aus.
   - **Scannen Sie mithilfe eines Erkennungszeitplans. Siehe Erkennen von Geräten im Netzwerk.**
   - **Scannen Sie mithilfe der Inventardatenerfassung. Siehe Inventardatensammlung für verwaltete Geräte planen.**
2. Rufen Sie die Seite *Gerätedetail* für das gescannte Objekt auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Inventar** und anschließend auf **Dashboard**.
   c. Klicken Sie auf der Listenseite *Geräte* auf den Namen des Objekts.
3. Klicken Sie im Abschnitt *Inventar* auf **SNMP-Daten**, um die Ergebnisse des vollständigen Durchlaufs anzuzeigen.
4. Wählen Sie die relevanten OIDs in der Liste aus.

Ordnen Sie die OIDs Feldern in der Appliance-Inventartabelle zu, sodass ihre Informationen ins Inventar integriert werden können. Siehe Objektbezeichner Feldern in der Inventartabelle zuordnen.

Objektbezeichner Feldern in der Inventartabelle zuordnen

Sie können bestimmten Feldern, die Sie als Asset-Untertypen erstellt haben, SNMP-OIDs (Simple Network Management Protocol Object Identifiers) zuordnen. Mithilfe der resultierenden SNMP-Inventarkonfigurationen

können Sie die Inventarinformationen erweitern, um benutzerdefinierte Daten von Geräten aufzunehmen, bei denen es sich nicht um Computer handelt.

- Sie haben die relevanten OIDs bestimmt, die in der Konfiguration enthalten sein müssen:
  - Sie haben den MIB-Browser einer vom Anbieter bereitgestellten Management Information Base verwendet.
  - Sie haben mit der Appliance einen vollständigen SNMP-Durchlauf für ein Zielobjekt ausgeführt und die OIDs überprüft, die auf der Seite *Gerätedetail* im Abschnitt *Inventarinformationen* unter **SNMP-Daten** angezeigt werden. Siehe Erkennen von Geräten im Netzwerk.
- Sie haben entsprechende Asset-Subtypen für computerfremde Geräte erstellt, die Sie im Inventar verwalten möchten. Siehe Asset-Untertypen hinzufügen und Voreinstellungen für die Seite "Gerätedetail" auswählen.

Die Liste *SNMP-Inventarkonfigurationen* ermöglicht Ihnen das Erstellen neuer Zuordnungen bzw. das Verwalten vorhandener Zuordnungen.

Nachdem Sie die zu erfassenden OID-Daten festgelegt haben, wählen Sie einen Untertyp für das Gerät aus den Kategorien aus, bei denen es sich um die gleichen Kategorien wie auf der Seite *Gerätedetail* handelt. Anschließend wählen Sie eine Eigenschaft dieser Kategorie aus, durch deren Ergebnis die OID einem Feld in der Inventartabelle zugeordnet wird. Das SNMP-Objekt wird nach dem nächsten Scan im Geräteinventar angezeigt.

Wenn beispielsweise ein Drucker im Inventar vorhanden ist, der manuell oder über einen Erkennungszeitplan hinzugefügt wurde, können Sie mithilfe einer SNMP-Inventarkonfiguration festlegen, dass der Drucker Farbkartuschenstände an die Appliance meldet. In diesem Fall würden Sie einen Asset-Untertyp namens *Drucker* verwenden, den Sie als Geräte-Untertyp mit dem Feld *Toner-Füllstand* erstellt haben.

1. Rufen Sie die Listenseite *SNMP-Inventarkonfigurationen* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Inventar** und anschließend auf **SNMP-Inventarkonfigurationen**.
2. Wählen Sie **Aktion auswählen > Neu**.
3. Geben Sie im Feld *Name* einen Namen für die Konfiguration ein.

   WICHTIG: Bei SNMP-Geräten müssen Sie bei der Gerätekonfiguration den entsprechenden Asset-Untertyp zuweisen. Sie können SNMP-Geräteuntertypen nach ihrer Konfiguration nicht mehr hinzufügen oder ändern.
4. Wählen Sie einen Asset-Untertyp aus, der die Art des zu inventarisierenden Gerätes identifiziert.
5. Ordnen Sie eine OID einem Appliance-Inventarfeld zu:
   a. Klicken Sie auf die Schaltfläche Hinzufügen: +.

      Unter den Überschriften wird eine neue Zeile angezeigt.
   b. Geben Sie die OID ins Textfeld unter *Objektbezeichner (OID)* ein.
   c. Wählen Sie eine Kategorie in der Dropdown-Liste unter *Kategorie* aus.

   Die Kategorien entsprechen denen auf der Seite *Detail Asset-Untertyp*.

   d. Wählen Sie eine Eigenschaft in der Dropdown-Liste unter *Eigenschaft* aus.

   Die Eigenschaften hängen von dem ausgewählten Untertyp und der ausgewählten Kategorie ab.

   e. Klicken Sie am Ende der Zeile auf **Speichern**.
6. Ordnen Sie die benötigte Anzahl zusätzlicher OIDs zu und klicken Sie unten links auf der Seite auf **Speichern**.

Wenden Sie die Konfiguration auf ein Objekt an. Siehe SNMP-Inventarkonfiguration auf ein Gerät anwenden.

SNMP-Inventarkonfiguration auf ein Gerät anwenden

Sie können eine SNMP-Inventarkonfiguration auf ein Gerät anwenden, sodass die zusätzlichen Daten beim nächsten Scan des Geräts erfasst werden können.

Sie haben die Konfiguration erstellt. Siehe Objektbezeichner Feldern in der Inventartabelle zuordnen.

HINWEIS: Sie können SNMP-Inventarkonfigurationen nur auf durch SNMP verwaltete Geräte ohne Agent anwenden.

1. Rufen Sie die Seite *Geräte* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie auf der linken Navigationsleiste auf **Inventar**, um die Seite *Geräte* anzuzeigen.
2. Aktivieren Sie die Kontrollkästchen neben einem oder mehreren Geräten.
3. Wählen Sie **Aktion auswählen** > **SNMP-Konfigurationen anwenden**, um das Dialogfeld *SNMP-Konfigurationen anwenden* aufzurufen.
4. Ziehen Sie die anzuwendenden Konfigurationen ins Feld *Diese SNMP-Konfigurationen anwenden*.

   Sie können nach einer bestimmten Konfiguration suchen, indem Sie mit der Eingabe des entsprechenden Namens im Feld *SNMP-Konfigurationen suchen* beginnen.
5. Klicken Sie auf **SNMP-Konfigurationen anwenden**.

   Die Listenseite *Geräte* wird nach dem Anwenden der Konfiguration erneut angezeigt.

Die Informationen zum Gerät werden nach der nächsten regelmäßig geplanten Berichtszeit oder nach einer erzwungenen Inventaraktualisierung angezeigt.

Verwandte Themen

Inventardatensammlung für verwaltete Geräte planen

Erzwingen von Inventaraktualisierungen

Informationen zu Druckervorlagen

Die Appliance verfügt außerdem über eine Reihe von Druckervorlagen für typische SNMP (Simple Network Management Protocol)-fähige Druckermodelle. Sie können diese SNMP-Konfigurationen bei Bedarf auf Drucker anwenden.

Die Seite mit der Liste *SNMP-Inventarkonfigurationen* zeigt die verfügbaren Druckervorlagen an. Wenn Sie eine Druckervorlage auf ein Gerät anwenden, werden die in der Vorlage definierten Daten, wie z. B. Tonerfüllstände oder Beschreibungen, für den Drucker im nächsten Bestandzyklus erfasst.

Eine standardmäßige Installation umfasst einer Reihe von Vorlagen für die folgenden Laserdrucker mit zwei Varianten pro Marke, um Schwarzweiß- und Farbdrucker abzudecken: Brother, Canon, HP, Lexmark und Xerox.

Sie können diese Vorlagen nach Bedarf bearbeiten oder erstellen. Zum Erstellen oder Bearbeiten einer Druckervorlage benötigen Sie die entsprechenden SNMP-Objektbezeichner (OIDs) für die Felder, die als verknüpfte Asset-Untertypen vorhanden sind. Die Appliance verfügt über zwei Asset-Untertypen, die druckerspezifische Felder wie Tonerfüllstände erfassen: *Laserdrucker: Farb-* und *Laserdrucker: Monochrom*. Weitere Informationen zur Zuweisung von Objektbezeichnern finden Sie unter Objektbezeichner Feldern in der Inventartabelle zuordnen. Informationen zu Asset-Untertypen und deren Beziehung zu SNMP-Konfigurationen finden Sie unter Informationen zu Asset-Untertypen, benutzerdefinierten Feldern und Gerätedetail-Voreinstellungen.

Manuelles Hinzufügen von Geräten in der Administratorkonsole oder mithilfe der API

Sie können Geräte manuell zum Inventar hinzufügen. Hierzu können Sie entweder die **Administratorkonsole** oder die Inventar-API (Application Programming Interface) verwenden.

Das manuelle Hinzufügen von Geräten ist hilfreich, wenn Sie Geräteinformationen hinzufügen möchten, aber die Geräte nicht durch die Installation des KACE Agent oder über die Verwaltung ohne Agent-Software verwalten möchten.

Das Inventar für manuelle Geräte muss manuell aktualisiert oder hochgeladen werden. Die Appliance erhält von manuellen Geräten keine geplanten Inventaraktualisierungen.

Informationen zur Geräteverwaltung

Das Verwalten von Geräten mithilfe der Appliance umfasst das Sammeln und Pflegen von Informationen über die Geräte im Netzwerk und das Durchführen von Aufgaben, wie beispielsweise Gerätestatus überwachen, Berichte erstellen usw.

Sie haben folgende Möglichkeiten, um Geräte zum Appliance-Inventar hinzuzufügen:

- **KACE Agent auf Geräten installieren**. Geräte werden automatisch zum Inventar hinzugefügt, nachdem der Agent auf ihnen installiert wurde und der Agent Inventar an die Appliance meldet. Siehe Provisionierung des KACE Agent.
- **Verwaltung ohne Agent für Geräte aktivieren**. Die Verwaltung ohne Agent ist besonders bei Geräten nützlich, auf denen der KACE Agent nicht installiert werden kann, beispielsweise bei Geräten mit nicht unterstützten Betriebssystemen. Siehe Geräte ohne Agent verwalten.
- **Manuelles Hochladen von Inventarinformationen für Geräte**. Siehe Manuelles Hinzufügen von Geräten in der Administratorkonsole oder mithilfe der API.

HINWEIS: Die Produktlizenzvereinbarung berechtigt Sie zur Verwaltung einer bestimmten Anzahl von Geräten, die als verwaltete Computer, Assets und überwachte Server klassifiziert sind. Hierzu zählen auch Geräte, die als "Ausstehend" (MIA, Missing in Action) eingestuft sind oder nicht mehr verwendet werden. Geräte, die dem Inventar manuell oder über die API hinzugefügt wurden, werden bei den Lizenzlimits dagegen nicht berücksichtigt. Siehe Produktlizenzinformationen anzeigen.

Information zu den für Geräte verfügbaren Funktionen finden Sie unter Funktionen, die für jede einzelne Geräteverwaltungsmethode zur Verfügung stehen.

Erfassen von Änderungen an Inventareinstellungen

Wenn Verlaufsabonnements zur Aufbewahrung von Informationen konfiguriert wurden, können Sie Details zu den an Einstellungen, Assets und Objekten vorgenommenen Änderungen anzeigen.

Diese Informationen beinhalten auch das Datum der Änderung und den Benutzer, der diese vorgenommen hat. Dies kann bei der Fehlerbehebung nützlich sein. Siehe Informationen zu den Verlaufseinstellungen.

Informationen zum Inventaränderungsverlauf

Der Änderungsverlauf für das Geräteinventar beginnt, sobald Änderungen an den im ersten Bericht erfassten Informationen auftreten.

Bei der ersten Inventarmeldung eines verwalteten Geräts an die Appliance werden die Informationen als Grundlagenbericht betrachtet. Die Informationen werden daher nicht im Änderungsverlauf aufgezeichnet.

Geräte mit der Administratorkonsole manuell hinzufügen

Durch Eingeben von Geräteinformationen auf der *Gerätedetailseite* können Sie dem Appliance-Inventar Geräte manuell hinzufügen.

Nach der Erstellung werden manuelle Datensätze von der Appliance oder von Agenten nicht verändert. Folglich können die Felder in einem manuellen Datensatz nur manuell von einem Administrator aktualisiert werden.

1. Rufen Sie die Liste *Geräte* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Inventar** und anschließend auf **Dashboard**.
2. Wählen Sie **Aktion auswählen > Neu > Manuelles Gerät**, um die *Gerätedetailseite* anzuzeigen.
3. Führen Sie einen der folgenden Schritte aus:
   - **Klicken Sie unter** *device.xml importieren* **auf Datei auswählen, um nach einer XML-Datei mit Geräteinventarinformationen zu suchen und sie zu importieren. Siehe Gültiges XML-Schema für Windows und XML-Dateien über die Administratorkonsole hochladen.**

     Geben Sie im Abschnitt *Übersicht* einen *Namen* für das Gerät ein und fahren Sie anschließend mit Schritt 10 fort.
   - **Geben Sie im Bereich** *Übersicht* **die folgenden Informationen ein:**

Element	Beschreibung	Datenbankfeld
Systemname	Der Hostname oder die IP-Adresse des Geräts.	NAME
Systembeschreibung	Eine Beschreibung des Geräts	Systembeschreibung
Modell	Das Modell des Geräts	CS_MODEL
Gehäusetyp	Der Typ des Geräts, z.B. Desktop oder Notebook	CHASSIS_TYPE
IP-Adresse	Die IP-Adresse des Geräts	IP
MAC	Die Media Access Control (MAC)-Adressnummer des Geräts	MAC
Name des Betriebssystems	Das Betriebssystem des Geräts, z.B. Windows, Mac OS X oder Linux	OS_NAME
Service Pack	Die Versionsnummer des Service Packs (nur Windows)	SERVICE_PACK
Zeitzone des Geräts	Die vom auf dem Gerät installierten KACE Agent verwendete Zeitzone.	TZ_AGENT

Element	Beschreibung	Datenbankfeld
Benutzer	Ein mit diesem Gerät verknüpfter Benutzer	USER
Domain	Die Domäne des Geräts.	CS_DOMAIN
Anmerkungen	Geben Sie nach Bedarf beliebige weitere Informationen ein.	HINWEISE

4. Geben Sie im Bereich *Hardware* die folgenden Informationen ein:

Element	Beschreibung	Datenbankfeld
Maximaler RAM	Die Größe des maximal verfügbaren RAM (Random Access Memory)	RAM_MAX
RAM gesamt	Maximal verfügbarer RAM (Random Access Memory) des Geräts	RAM_TOTAL
Genutzter RAM	Die Größe des verwendeten RAM (Random Access Memory) auf dem Gerät	RAM_USED
Systemhersteller	Der Hersteller des Geräts	CS_MANUFACTURER
Systemmodell	Das Modell des Geräts	CS_MODEL
Service-Tag	Informationen zum Identifizieren von Geräte-Services.	SERVICE_TAG
Asset-Tag	Information zum Identifizieren von Gerätehardware.	ASSET_TAG
Primärer Bus der Hauptplatine	Der Systembus	MOTHERBOARD_PRIMARY_BUS
Sekundärer Bus der Hauptplatine	Der Peripheriebus	MOTHERBOARD_SECONDARY_BUS
Architektur	Die Architektur des Gerätebetriebssystems (beispielsweise x86 oder x64).	SYS_ARCH
Virtuelles Gerät	Identifiziert virtuelle Geräte, z.B. Geräte auf VMware Plattformen. Wird nicht für physische Geräte wie Notebooks und Server angezeigt.	VIRTUELL
Prozessoren	Die Anzahl, der Typ und der Hersteller der CPUs	PROCESSORS

Element	Beschreibung	Datenbankfeld
CD/DVD-Laufwerke	Die Konfiguration der auf dem Gerät installierten CD-ROM- und DVD-ROM-Laufwerke	CDROM_DEVICES
Audiogeräte	Informationen über Audiogeräte auf dem Gerät	SOUND_DEVICES
Monitore	Typ und Hersteller des an das Gerät angeschlossenen Monitors Dieses Feld wird für virtuelle Geräte nicht angezeigt.	MONITOR
Videocontroller	Informationen über Videocontroller auf dem Gerät	VIDEO_CONTROLLERS
BIOS-Name	Der BIOS-Name	BIOS_NAME
BIOS-Herausgabedatum	Das Datum der Herausgabe der BIOS-Version	BIOS_RELEASE_DATE
BIOS-Version	Die BIOS-Version	BIOS_VERSION
BIOS-Hersteller	Der BIOS-Hersteller	BIOS_MANUFACTURER
BIOS-Beschreibung	Die BIOS-Beschreibung	BIOS_Beschreibung
BIOS-Identifikationscode	Der BIOS-Identifikationscode.	BIOS_IDENTIFICATION_CODE
BIOS-Seriennummer	Die BIOS-Seriennummer	BIOS_SERIAL_NUMBER

5. Geben Sie im Bereich *Drucker* die Druckerinformationen für das Gerät an.
6. Geben Sie im Bereich *Agent* die Versionsnummer des auf dem Gerät installierten KACE Agent an.
7. Geben Sie im Bereich *Benutzer* die Benutzerinformationen an.

Element	Beschreibung	Datenbankfeld
Benutzer angemeldet	Der Benutzer, der derzeit bei dem Gerät angemeldet ist Dieser Eintrag umfasst den Namen des Benutzers sowie die Domäne, zu der der Benutzer gehört.	USER_LOGGED
Vollständiger Benutzername	Der vollständige Name des Benutzers, der das Gerät besitzt.	USER_FULLNAME
Benutzerdomäne	Die Domäne, zu der der Benutzer gehört	USER_DOMAIN
Letzter Benutzer	Der Name des letzten Benutzers, der sich beim Gerät angemeldet hat Einige Geräte werden	USER

Element	Beschreibung	Datenbankfeld
	möglicherweise von mehreren Benutzern verwendet.	

8. Geben Sie im Bereich *Betriebssystem* die Informationen zu dem auf dem Gerät installierten Betriebssystem an.

Element	Beschreibung	Datenbankfeld
Betriebssystemversion	Die Versionsnummer des Betriebssystems	OS_VERSION
Betriebssystem-Buildversion	Die Build-Nummer des Betriebssystems	OS_BUILD
Nummer	Die Nummer des Betriebssystems	OS_NUMBER
Betriebssystemhauptversion	Die Hauptversionsnummer des Betriebssystems.	OS_MAJOR
Betriebssystemnebenversion	Die Nebenversionsnummer des Betriebssystems.	OS_MINOR
Nebenversion (2)	Zusätzliche Informationen zur Betriebssystemversion.	OS_MINOR2
Internet Explorer-Version	Die auf dem Gerät installierte Version des Internet Explorer	IE_VERSION
.NET-Versionen	Die auf dem Gerät installierten .NET-Versionen.	DOT_NET_VERSIONS
Betriebssystemarchitektur	Die Architektur des Gerätebetriebssystems (beispielsweise x86 oder x64).	OS_ARCH
Betriebssystemname	Der Name des auf dem Gerät verwendeten Betriebssystems.	OS_NAME
Edge-Version	Die auf dem Gerät installierte Version von Microsoft Edge.	EDGE_VERSION
Familie	Die Produktfamilie des Betriebssystems.	OS_FAMILY
Service Pack		
Datum der Betriebssysteminstallation	Das Datum der Installation des Betriebssystems	OS_INSTALLED_DATE
Letzter Start	Die Uhrzeit, zu der das Betriebssystem zuletzt ausgeschaltet wurde	LAST_REBOOT

Element	Beschreibung	Datenbankfeld
System wurde zuletzt heruntergefahren am	Die Uhrzeit, zu der das Betriebssystem zuletzt ausgeschaltet wurde	LAST_SHUTDOWN
Betriebszeit seit letztem Neustart	Die Dauer der Ausführung des Betriebssystems	LAST_REBOOT
Domain	Die Domäne des Geräts.	CS_DOMAIN
Systemverzeichnis	Der Speicherort des Systemverzeichnisses	SYSTEM_DIRECTORY
Registrierungsgröße	Die Größe der Registrierung	REGISTRY_SIZE
Maximale Registrierungsgröße	Die maximale Größe der Registrierung	REGISTRY_MAX_SIZE
WMI-Status	Der Status des Windows Verwaltungsinstrumentationsdienstes (WMI) (nur Windows Geräte).	WMI_STATUS

9. Klicken Sie auf **Speichern**.

   Das Symbol des manuellen Geräts wird in der Spalte **Status** auf der Seite *Geräte* angezeigt: . Das Inventar für manuelle Geräte muss manuell aktualisiert werden.

Geräte mithilfe der API manuell hinzufügen

Sie können der Appliance manuell Geräte hinzufügen, indem Sie eine XML-Datei erstellen und diese über die API (Anwendungsprogrammierschnittstelle) auf die Appliance hochladen. Diese Methode ist hilfreich bei Geräten, die den KACE Agent aus Sicherheitsgründen nicht ausführen oder keine Verbindung mit dem lokalen Netzwerk (LAN) herstellen können, um Inventar zu melden.

Bei der Erstellung der XML-Datei können Sie sich am Beispielskript in diesem Abschnitt orientieren.

Geräte, die über die API zum Inventar hinzugefügt werden, werden nicht auf das Lizenzlimit angerechnet. Siehe Produktlizenzinformationen anzeigen.

Über die API hochgeladenes Anwendungsinventar wird auf der Seite *Software*, aber nicht auf der Seite *Softwarekatalog* angezeigt. Siehe:

- Verwalten von Anwendungen auf der Seite "Software"
- Verwalten des Softwarekataloginventars

> **HINWEIS:** Die Inventar-API unterstützt HTTP- und HTTPS-Kommunikation, je nach Konfiguration der Appliance. Verwenden Sie zum Hochladen von Inventarinformationen die folgende URL: `http://`**appliance_hostname**`/service/wsapi.php`, wobei **appliance_hostname** für den Hostnamen Ihrer Appliance steht.

Inventarinformationen mithilfe der API senden

Wenn Sie Inventar mithilfe der API übermitteln möchten, müssen Sie zunächst eine XML-Datei mit diesen Informationen generieren.

Beispiele finden Sie unter:

- Gültiges XML-Schema für Windows
- Beispiel zur Verwendung des XML-Schemas für Windows Geräte
- Gültiges XML-Schema für Linux und Mac Geräte

Nachdem Sie eine XML-Datei mit den gewünschten Inhalten erstellt haben, können Sie Inventarinformationen über die API senden.

1. (Erforderlich) Einen Sitzungsschlüssel anfordern:

   Senden Sie `keyreq=true` im Text der Anforderung, um als Antwort eine Sitzungszeichenfolge zu erhalten.

2. (Erforderlich) Erstellen Sie den Authentifizierungstoken:
   a. Erstellen Sie die `auth`-Zeichenfolge wie folgt:

   ```
   session_string + '|' + MD5 of API password
   ```

   b. Führen Sie MD5 an der `auth`-Zeichenfolge aus.

3. (Für neue Geräte erforderlich) Fordern Sie eine Geräte-UUID an:

   Senden Sie `req=newuuid&key=$auth` im Text der Anforderung, um als Antwort einen UUID zu erhalten.

4. (Erforderlich) Senden Sie Inventar-XML-Daten:

   Senden Sie `req=loadxml&key=$auth&KUID=$uuid&version=6.0` in der `GET`-Zeile und Inventar-XML im Text der Anforderung.

   Siehe Perl-Beispielskript.

Perl-Beispielskript

Mithilfe von Perl-Skripts können Sie XML-Dateien mit Geräteinventarinformationen an die Appliance hochladen.

Nachfolgend finden Sie ein Perl-Beispielskript, mit dem eine von Benutzer erstellte XML-Datei auf die Appliance hochgeladen werden kann. Informationen zur Verwendung dieses Skripts erhalten Sie vom **Quest Support** unter https://support.quest.com/contact-support.

```
#!/usr/bin/perl
use strict;
use warnings;
use WWW::Curl::Easy;
use XML::Simple;
use Data::Dumper;
use Digest::MD5 qw(md5 md5_hex md5_base64);
    # Curl Output Handler ...
    my $response;
    sub write_data($$$$) {
       $response = shift;
       return length($response);
    }
    # -----------------------------------------------------
    # Appliance Configuration ...
    # -----------------------------------------------------
    my $password = "xxx"; # password set in Settings -> Security Settings
    my $host = "hostname";       # hostname or IP address here
    my $http = "https";        # HTTP or HTTPS
    # -------------------------------------------------------
    # Build XML Package ...
    # -------------------------------------------------------
    my $simple = new XML::Simple(keeproot => 1, forcearray => 1);
    my $data = $simple->XMLin("machine.xml");
    my $uuid = $data->{MachineStruct}->[0]->{MAC}->[0];
```

```
# -------------------------------------------------------
# Setup CURL stuff ...
# -------------------------------------------------------
my $url = "$http://$host/service/wsapi.php";
my $ch = WWW::Curl::Easy->new;
$ch->setopt(CURLOPT_URL, $url);  # set url to post to
$ch->setopt(CURLOPT_SSL_VERIFYPEER, 0);  # ok for self-signed ca
$ch->setopt(CURLOPT_VERBOSE, 0);
$ch->setopt(CURLOPT_WRITEFUNCTION, \&write_data); # return into a variable
$ch->setopt(CURLOPT_HEADER, 0);
$ch->setopt(CURLOPT_TIMEOUT, 40);  # times out after 4s
$ch->setopt(CURLOPT_POST, 1);
$ch->setopt(CURLOPT_COOKIEFILE, '/tmp/cookiefile.txt');
# -------------------------------------------------------
# STEP 1 - Request Session from the appliance ...
# -------------------------------------------------------
$ch->setopt(CURLOPT_POSTFIELDS, "keyreq=true"); # add POST fields
my $out = $ch->perform;
if ( $out != 0 ) {
        die ("Error: $out " .
        $ch->strerror($out) .
        " " .
        $ch->errbuf . "\n");
}
my $sess = $response;
# -------------------------------------------------------
# STEP 2 - Build Authorization Token ...
# -------------------------------------------------------
my $auth = md5_hex("$sess|".md5_hex($password));
# -------------------------------------------------------
# STEP 3 - Request new UUID from the appliance (if creating a new
#          device record.  If editing an existing device
#          be sure it is set in the XML ...
# -------------------------------------------------------
if ( 1 ) {
        print "Using UUID From XML File: $uuid\n";
} else {
        $ch->setopt(CURLOPT_POSTFIELDS,"req=newuuid&key=$auth");
        $out = $ch->perform;
        if ( $out != 0 ) {
              die ("Error: $out " .
                    $ch->strerror($out) .
                    " " .
                    $ch->errbuf . "\n");
        }
        $uuid = $response;
        $data->{MachineStruct}->[0]->{MAC}->[0] = $uuid;
        $data->{MachineStruct}->[0]->{NAME}->[0] = "WSAPI-" . $uuid;
        print "Created New UUID: $uuid\n";
        }
# convert Simple XML hash back to XML string ...
my $xml = $simple->XMLout(
        $data,
        KeepRoot => 1,
        NoAttr => 1,
);
# -------------------------------------------------------
# STEP 4 - Send XML to the appliance ...
# -------------------------------------------------------
my @curlHeader = ("Content-Type: text/xml");
```

```
$url = "$http://$host/service/wsapi.php?req=loadxml&key=$auth&KUID=
 $uuid&version=6.0";
$ch->setopt(CURLOPT_URL, $url); # set url to post to
$ch->setopt(CURLOPT_HTTPHEADER, \@curlHeader);
$ch->setopt(CURLOPT_POSTFIELDS, $xml);
$out = $ch->perform;
if ( $out != 0 ) {
        die ("Error: $out " . $ch->strerror($out) . " " . $ch->errbuf . "\n");
}
print "Loaded $uuid to the appliance ($host)\n";
```

Gültiges XML-Schema für Windows

Dateien, mit denen Inventarinformationen für Windows Geräte hochgeladen werden, müssen ein gültiges XML-Schema besitzen.

Im Folgenden finden Sie ein Beispiel für ein gültiges XML-Schema für unter Windows laufende Geräte.

```
<?xml version="1.0" encoding="utf-8"?>
<MachineStruct xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi=">
  http://www.w3.org/2001/XMLSchema-instance"
<NAME>@@__m_computerSystemName__@@</NAME>
<IP>@@__m_IPAddress__@@</IP>
<MAC>@@__m_versionKaceId__@@</MAC>
<OS_NAME>@@__m_operatingSystemCaption__@@</OS_NAME>
<OS_NUMBER>@@__m_operatingSystemVersion__@@</OS_NUMBER>
<OS_MAJOR>@@__m_operatingSystemVersionMajor__@@</OS_MAJOR>
<OS_MINOR>@@__m_operatingSystemVersionMinor__@@</OS_MINOR>
<SERVICE_PACK>@@__m_operatingSystemCsdVersion__@@</SERVICE_PACK>
<USER>@@__m_userAccountName__@@</USER>
<USER_FULLNAME>@@__m_userAccountFullName__@@</USER_FULLNAME>
<DOMAIN>@@__m_computerSystemDomain__@@</DOMAIN>
<OS_VERSION>@@__m_operatingSystemVersion__@@</OS_VERSION>
<OS_BUILD>@@__m_operatingSystemBuildNumber__@@</OS_BUILD>
<OS_INSTALLED_DATE>@@__m_operatingSystemInstallDate__@@</OS_INSTALLED_DATE>
<LAST_REBOOT>@@__m_operatingSystemLastBootupTime__@@</LAST_REBOOT>
<LAST_SHUTDOWN>@@__m_operatingSystemLastBootupTime__@@</LAST_SHUTDOWN>
<UPTIME>@@__m_operatingSystemUptime__@@</UPTIME>
<SYSTEM_DIRECTORY>@@__m_operatingSystemWindowsDirectory__@@</SYSTEM_DIRECTORY>
<SYSTEM_DESCRIPTION>@@__m_operatingSystemDescription__@@</SYSTEM_DESCRIPTION>
<RAM_TOTAL>@@__m_physicalMemoryTotalSize__@@</RAM_TOTAL>
<RAM_USED>@@__m_operatingSystemUsedPhysicalMemory__@@</RAM_USED>
<CS_MANUFACTURER>@@__m_computerSystemManufacturer__@@</CS_MANUFACTURER>
<CS_MODEL>@@__m_computerSystemModel__@@</CS_MODEL>
<CHASSIS_TYPE>@@__m_systemEnclosureChassisType__@@</CHASSIS_TYPE>
<TZ_AGENT>@@__m_versionTimeZone__@@</TZ_AGENT>
<USER_LOGGED>@@__m_computerSystemUserName__@@</USER_LOGGED>
<CS_DOMAIN>@@__m_computerSystemDomain__@@</CS_DOMAIN>
<USER_NAME>@@__m_userAccountName__@@</USER_NAME>
<USER_DOMAIN>@@__m_userAccountDomain__@@</USER_DOMAIN>
<BIOS_NAME>@@__m_biosName__@@</BIOS_NAME>
<BIOS_VERSION>@@__m_biosVersion__@@</BIOS_VERSION>
<BIOS_MANUFACTURER>@@__m_biosManufacturer__@@</BIOS_MANUFACTURER>
<BIOS_DESCRIPTION>@@__m_biosDescription__@@</BIOS_DESCRIPTION>
<BIOS_SERIAL_NUMBER>@@__m_biosSerialNumber__@@</BIOS_SERIAL_NUMBER>
<MOTHERBOARD_PRIMARY_BUS>@@__m_motherboardDevicePrimaryBusType__@@
  </MOTHERBOARD_PRIMARY_BUS>
<MOTHERBOARD_SECONDARY_BUS>@@__m_motherboardDeviceSecondaryBusType__@@
  </MOTHERBOARD_SECONDARY_BUS>
<PROCESSORS>CPU Chip Count: @@__m_processorCount__@@
CPU Core Count: @@__m_processorCoreCount__@@
```

```
@@__m_processorList__@@ </PROCESSORS>
<SOUND_DEVICES>@@__m_soundDeviceDescription__@@</SOUND_DEVICES>
<CDROM_DEVICES>@@__m_CDROMDeviceName__@@</CDROM_DEVICES>
<VIDEO_CONTROLLERS>@@__m_videoControllerName__@@</VIDEO_CONTROLLERS>
<REGISTRY_SIZE>@@__m_registryCurrentSize__@@</REGISTRY_SIZE>
<REGISTRY_MAX_SIZE>@@__m_registryMaximumSize__@@</REGISTRY_MAX_SIZE>
<DISK_DRIVES>
@@__m_logicalDiskDriveList__@@ </DISK_DRIVES>
<NETWORK_INTERFACES>
@@__m_networkAdapterConfigurationList__@@ </NETWORK_INTERFACES>
<PRINTERS>@@__m_printerList__@@</PRINTERS>
<STARTUP_PROGRAMS>
@@__m_startupProgramsList__@@ </STARTUP_PROGRAMS>
<PROCESSES>
@@__m_processList__@@ </PROCESSES>
<NT_SERVICES>
@@__m_servicesList__@@ </NT_SERVICES>
<INSTALLED_software>
@@__m_installedProgramsList__@@ </INSTALLED_software>
<CLIENT_VERSION>@@__m_appVersion__@@</CLIENT_VERSION>
</MachineStruct>
```

Beispiel zur Verwendung des XML-Schemas für Windows Geräte

Sie können sich ein Beispiel für eine Datei ansehen, die dem gültigen XML-Schema für Windows Geräte entspricht.

Nachfolgend sehen Sie ein Beispiel für eine gültige XML, die unter Verwendung des Schemas in Gültiges XML-Schema für Windows erstellt wurde.

```
<?xml version="1.0" encoding="utf-8"?>
<MachineStruct xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <NAME>TestComputer</NAME>
  <IP>10.10.10.10</IP>
  <MAC>F1234567-C2D2-4055-85BB-294E6A3D22D9</MAC>
  <OS_NAME>Microsoft Windows 7 Professional</OS_NAME>
  <OS_NUMBER>6.1.7601.17514</OS_NUMBER>
  <OS_MAJOR>6</OS_MAJOR>
  <OS_MINOR>1</OS_MINOR>
  <SERVICE_PACK>Service Pack 1</SERVICE_PACK>
  <USER>Administrator</USER>
  <USER_FULLNAME>Tom Silver</USER_FULLNAME>
  <DOMAIN>WORK</DOMAIN>
  <OS_VERSION>6.1.7601</OS_VERSION>
  <OS_BUILD>17514</OS_BUILD>
  <OS_INSTALLED_DATE>2017-08-30 14:22:39 -0400</OS_INSTALLED_DATE>
  <LAST_REBOOT>2017-08-30 14:25:05 -0400</LAST_REBOOT>
  <LAST_SHUTDOWN>2017-08-30 14:25:05 -0400</LAST_SHUTDOWN>
  <UPTIME>4 days </UPTIME>
  <SYSTEM_DIRECTORY>C:\WINDOWS</SYSTEM_DIRECTORY>
  <SYSTEM_DESCRIPTION>Windows 7 Machine</SYSTEM_DESCRIPTION>
  <RAM_TOTAL>512.00MB</RAM_TOTAL>
  <RAM_USED>180MB</RAM_USED>
  <CS_MANUFACTURER>VMware, Inc.</CS_MANUFACTURER>
  <CS_MODEL>VMware Virtual Platform</CS_MODEL>
  <CHASSIS_TYPE>Other</CHASSIS_TYPE>
  <USER_LOGGED>Tom</USER_LOGGED>
  <CS_DOMAIN>WORK</CS_DOMAIN>
  <USER_NAME>Administrator</USER_NAME>
  <USER_DOMAIN>Work</USER_DOMAIN>
```

```
  <BIOS_NAME>PhoenixBIOS 4.0 Release 5.5     </BIOS_NAME>
  <BIOS_VERSION>INTEL  - 6040000</BIOS_VERSION>
  <BIOS_MANUFACTURER>Phoenix Technologies LTD</BIOS_MANUFACTURER>
  <BIOS_DESCRIPTION>PhoenixBIOS 4.0 Release 5.5  </BIOS_DESCRIPTION>
  <BIOS_SERIAL_NUMBER>VMware-56 4d bd d3 5e 4f a5 4e-6a ce a0 d3 39 bd ae 02
    </BIOS_SERIAL_NUMBER>
  <MOTHERBOARD_PRIMARY_BUS>PCI</MOTHERBOARD_PRIMARY_BUS>
  <MOTHERBOARD_SECONDARY_BUS>ISA</MOTHERBOARD_SECONDARY_BUS>
  <PROCESSORS>CPU Chip Count: 1
CPU Core Count: 0
CPU0: Intel Celeron processor (0 cores)  </PROCESSORS>
  <SOUND_DEVICES>Creative AudioPCI (ES1371,ES1373) (WDM)
</SOUND_DEVICES>
  <CDROM_DEVICES>TSSTcorp DVD+-RW TS-U633F
</CDROM_DEVICES>
  <VIDEO_CONTROLLERS>VMware SVGA II
</VIDEO_CONTROLLERS>
  <REGISTRY_SIZE>1MB</REGISTRY_SIZE>
  <REGISTRY_MAX_SIZE>86MB</REGISTRY_MAX_SIZE>
  <DISK_DRIVES>
    <DiskDrive>
      <NAME>Drive C: (Physical Disk) FileSystem: NTFS Used: 2.08GB Total: 39.99GB</NAME>
      <DISK_SIZE>39.9906</DISK_SIZE>
      <DISK_USED>2.07966</DISK_USED>
      <DISK_FREE>37.9109</DISK_FREE>
      <PERCENT_USED>5.2</PERCENT_USED>
    </DiskDrive>
  </DISK_DRIVES>
  <NETWORK_INTERFACES>
    <NetworkInterface>
      <NIC>AMD PCNET Family PCI Ethernet Adapter - Packet Scheduler
Miniport</NIC>
      <MAC>00:0C:29:BD:AE:03</MAC>
      <IP>192.168.220.132</IP>
      <DHCP_ENABLED>True</DHCP_ENABLED>
    </NetworkInterface>
  </NETWORK_INTERFACES>
  <PRINTERS></PRINTERS>
  <STARTUP_PROGRAMS>
    <StartupProgram>
      <NAME>desktop</NAME>
    </StartupProgram>
    <StartupProgram>
      <NAME>VMware Tools</NAME>
      <COMMAND_EXE>C:\Program Files\VMware\VMware Tools\VMwareTray.exe</COMMAND_EXE>
      <COMMAND_ARGS />
      <FILE_INFO>
        <FILE_NAME>VMwareTray.exe</FILE_NAME>
        <FILE_DESCRIPTION>VMware Tools tray application</FILE_DESCRIPTION>
        <FILE_VERSION>8.4.6.16648</FILE_VERSION>
        <PRODUCT_NAME>VMware Tools</PRODUCT_NAME>
        <PRODUCT_VERSION>8.4.6 build-385536</PRODUCT_VERSION>
        <COMPANY_NAME>VMware, Inc.</COMPANY_NAME>
      </FILE_INFO>
    </StartupProgram>
    <StartupProgram>
      <NAME>VMware User Process</NAME>
      <COMMAND_EXE>C:\Program Files\VMware\VMware Tools\VMwareUser.exe</COMMAND_EXE>
      <COMMAND_ARGS />
      <FILE_INFO>
```

```
        <FILE_NAME>VMwareUser.exe</FILE_NAME>
        <FILE_DESCRIPTION>VMware Tools Service</FILE_DESCRIPTION>
        <FILE_VERSION>8.4.6.16648</FILE_VERSION>
        <PRODUCT_NAME>VMware Tools</PRODUCT_NAME>
        <PRODUCT_VERSION>8.4.6 build-385536</PRODUCT_VERSION>
        <COMPANY_NAME>VMware, Inc.</COMPANY_NAME>
      </FILE_INFO>
    </StartupProgram>
  </STARTUP_PROGRAMS>
  <PROCESSES>
    <MachineProcess>
      <NAME>AMPAgent.exe</NAME>
      <COMMAND_EXE>C:\Program Files\Quest\KACE\AMPAgent.exe</COMMAND_EXE>
      <COMMAND_ARGS />
      <FILE_INFO>
        <FILE_NAME>AMPAgent.exe</FILE_NAME>
        <FILE_DESCRIPTION>AMP Service</FILE_DESCRIPTION>
        <FILE_VERSION>5.2.38916</FILE_VERSION>
        <PRODUCT_NAME>KACE Agent</PRODUCT_NAME>
        <PRODUCT_VERSION>5.2.38916</PRODUCT_VERSION>
        <COMPANY_NAME>Quest Software Inc.</COMPANY_NAME>
      </FILE_INFO>
    </MachineProcess>
  </PROCESSES>
  <NT_SERVICES>
    <NtService>
      <NAME>Alerter</NAME>
      <DISPLAY_NAME>Alerter</DISPLAY_NAME>
      <STATUS>SERVICE_STOPPED</STATUS>
      <STARTUP_TYPE>SERVICE_DISABLED</STARTUP_TYPE>
      <DESCRIPTION />
      <LOGON_AS_USER>NT AUTHORITY\LocalService</LOGON_AS_USER>
      <CAN_INTERACT_WITH_DESKTOP>False</CAN_INTERACT_WITH_DESKTOP>
      <COMMAND_EXE>C:\WINDOWS\system32\svchost.exe</COMMAND_EXE>
      <COMMAND_ARGS> -k LocalService</COMMAND_ARGS>
      <FILE_INFO>
        <FILE_NAME>svchost.exe</FILE_NAME>
        <FILE_DESCRIPTION>Generic Host Process for Win32 Services</FILE_DESCRIPTION>
        <FILE_VERSION>6.1.7600.16385 (win7_rtm.090713-1255)</FILE_VERSION>
        <PRODUCT_NAME>Microsoft® Windows® Operating System</PRODUCT_NAME>
        <PRODUCT_VERSION>6.1.7600.16385</PRODUCT_VERSION>
        <COMPANY_NAME>Microsoft Corporation</COMPANY_NAME>
      </FILE_INFO>
    </NtService>
  </NT_SERVICES>
  <INSTALLED_software>
    <software>
      <DISPLAY_VERSION>5.2.38916</DISPLAY_VERSION>
      <HELP_LINK />
      <README />
      <INSTALL_DATE>20170830</INSTALL_DATE>
      <PUBLISHER>Quest Software Inc.</PUBLISHER>
      <UNINSTALL_STRING />
      <URLINFO_ABOUT />
      <DISPLAY_NAME>Quest KACE Agent</DISPLAY_NAME>
   </software>
  </INSTALLED_software>
  <CLIENT_VERSION>8.0.xxxxx</CLIENT_VERSION>
</MachineStruct>
```

Gültiges XML-Schema für Linux und Mac Geräte

Dateien, mit denen Inventarinformationen für Linux und Mac Geräte hochgeladen werden, müssen ein gültiges XML-Schema besitzen.

Nachfolgend sehen Sie ein Beispiel für ein gültiges XML-Schema für Linux und Mac Geräte.

```
<?xml version="1.0" encoding="utf-8"?>
            <MachineStruct>
                  <NAME>@@__m_versionHostName__@@</NAME>
                  <CLIENT_VERSION>@@__m_appVersion__@@</CLIENT_VERSION>
                  <IP>@@__m_IPAddress__@@</IP>
                  <MAC>@@__m_versionKaceId__@@</MAC>
                  <OS_NAME>@@__m_operatingSystemCaption__@@</OS_NAME>
                  <OS_NUMBER>@@__m_operatingSystemVersion__@@</OS_NUMBER>
                  <OS_MAJOR>@@__m_operatingSystemVersionMajor__@@</OS_MAJOR>
                  <OS_MINOR>@@__m_operatingSystemVersionMinor__@@</OS_MINOR>
                  <SERVICE_PACK></SERVICE_PACK>
                  <INSTALL_DATE></INSTALL_DATE>
  <OS_ARCH>@@__m_operatingSystemOSArchitecture__@@</OS_ARCH>
                  <OS_FAMILY>@@__m_operatingSystemOSFamily__@@</OS_FAMILY>
                  <OS_VERSION>@@__m_operatingSystemVersion__@@</OS_VERSION>
                  <OS_BUILD>@@__m_operatingSystemBuildNumber__@@</OS_BUILD>
                  <DOMAIN>@@__m_userAccountDomain__@@</DOMAIN>
                  <CS_DOMAIN>@@__m_userAccountDomain__@@</CS_DOMAIN>
  <LAST_REBOOT>@@__m_operatingSystemLastBootupTime__@@</LAST_REBOOT>
                  <TZ_AGENT>@@__m_versionTimeZone__@@</TZ_AGENT>
                  <UPTIME>@@__m_operatingSystemUptime__@@</UPTIME>
  <RAM_TOTAL>@@__m_operatingSystemTotalVisibleMemorySize__@@</RAM_TOTAL>
  <RAM_USED>@@__m_operatingSystemUsedPhysicalMemory__@@</RAM_USED>
                  <CS_MANUFACTURER>@@__m_biosManufacturer__@@</CS_MANUFACTURER>
                  <CS_MODEL></CS_MODEL>
                  <USER_LOGGED>@@__m_userAccountName__@@</USER_LOGGED>
                  <USER>@@__m_userAccountName__@@</USER>
                  <USER_NAME>@@__m_userAccountName__@@</USER_NAME>
                  <USER_FULLNAME>@@__m_userAccountFullName__@@</USER_FULLNAME>
                  <USER_DOMAIN>@@__m_userAccountDomain__@@</USER_DOMAIN>
                  <BIOS_NAME>@@__m_biosName__@@</BIOS_NAME>
                  <BIOS_VERSION>@@__m_biosVersion__@@</BIOS_VERSION>
                  <BIOS_MANUFACTURER>@@__m_biosManufacturer__@@</BIOS_MANUFACTURER>
                  <BIOS_DESCRIPTION>@@__m_biosName__@@</BIOS_DESCRIPTION>
      <BIOS_SERIAL_NUMBER>@@__m_biosSerialNumber__@@</BIOS_SERIAL_NUMBER>
                  <MOTHERBOARD_PRIMARY_BUS></MOTHERBOARD_PRIMARY_BUS>
                  <MOTHERBOARD_SECONDARY_BUS></MOTHERBOARD_SECONDARY_BUS>
                  <PROCESSORS>@@__m_processorList__@@</PROCESSORS>
                  <SOUND_DEVICES>@@__m_soundDeviceDescription__@@</SOUND_DEVICES>
                  <CDROM_DEVICES>@@__m_CDROMDeviceName__@@</CDROM_DEVICES>
                  <MONITOR>@@__m_desktopMonitorDescription__@@</MONITOR>
  <VIDEO_CONTROLLERS>@@__m_videoControllerName__@@</VIDEO_CONTROLLERS>
                  <DISK_DRIVES>
 @@__m_logicalDiskDriveList__@@</DISK_DRIVES>
     <NETWORK_INTERFACES>
 @@__m_networkAdapterConfigurationList__@@</NETWORK_INTERFACES>
      <PRINTERS>@@__m_printerList__@@</PRINTERS>
      <STARTUP_PROGRAMS>
 @@__m_startupProgramsList__@@</STARTUP_PROGRAMS>
      <PROCESSES>
 @@__m_processList__@@</PROCESSES>
      <INSTALLED_software>
 @@__m_installedProgramsList__@@</INSTALLED_software>
```

```
</MachineStruct>
```

XML-Dateien über die Administratorkonsole hochladen

Sie können eine XML-Datei mit Geräteinventarinformationen mithilfe der **Administratorkonsole** hochladen. Diese Informationen werden als manuelle Inventarinformationen bezeichnet.

Der KACE Agent ist auf dem Gerät installiert, für das Inventarinformationen hinzugefügt werden.

Sie erstellen die XML-Datei auf dem zu inventarisierenden Gerät und laden die Datei anschließend über die Appliance hoch.

Die manuellen Inventardaten werden auf der Seite *Software* angezeigt, jedoch nicht auf der Seite *Softwarekatalog*. Siehe:

- Verwalten von Anwendungen auf der Seite "Software"
- Verwalten des Softwarekataloginventars

1. Generieren Sie eine XML-Datei mit den Informationen.
   a. Öffnen Sie auf einem Gerät, auf dem der KACE Agent installiert ist, ein Eingabeaufforderungs- oder Terminalfenster.
   b. Öffnen Sie das Installationsverzeichnis von Quest KACE.

   Beispiel:

   - Windows 32-Bit-Systeme: `C:\Programme\Quest\KACE`
   - Windows 64-Bit-Systeme: `C:\Programme (x86)\Quest\KACE\`
   - Mac OS X Systeme: `/Library/Application Support/Quest/KACE/bin`
   - Linux Systeme: `/opt/quest/kace/bin/`

   c. Geben Sie den folgenden Befehl ein:

   `KInventory -machine -output` **Dateiname**

   Dabei steht **Dateiname** für den Pfad zu der XML-Datei, die Sie erstellen wollen. Wenn der Pfad Leerzeichen enthält, geben Sie den gesamten Pfad in doppelten Anführungszeichen an.

   Der Agent erfasst die Inventardaten und erstellt die XML-Datei.
2. Rufen Sie in der Administratorkonsole der Appliance die Liste *Geräte* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Inventar** und anschließend auf **Dashboard**.
3. Wählen Sie **Aktion auswählen** > **Neu** > **Manuelles Gerät**, um die *Gerätedetailseite* anzuzeigen.
4. Klicken Sie unter *Gerät importieren* auf **Durchsuchen**.
5. Wählen Sie die Datei und klicken Sie dann auf **Öffnen** oder **Auswählen**.
6. Klicken Sie auf **Speichern**.

Die Geräteinformationen werden dem Inventar hinzugefügt. Wenn Sie eine XML-Datei hochladen, ignoriert die Appliance alle anderen Informationen auf der Seite und verwendet die XML-Datei für die Inventarinformationen.

Erzwingen von Inventaraktualisierungen

Sie können erzwingen, dass verwaltete Geräte ihre Inventarinformationen außerhalb der regelmäßig geplanten Berichtszeiten aktualisieren.

Um Aktualisierungen des Inventars zu erzwingen, muss eine der folgenden Bedingungen erfüllt sein:

- Der KACE Agent muss auf den Geräten installiert sein und es muss eine aktive AMP-Verbindung (Active Messaging Protocol) zwischen der Appliance und den Geräten bestehen.
- Die Verwaltung ohne Agent muss für die Geräte aktiviert sein.

Sie können keine Aktualisierung auf Geräten erzwingen, die weder über den Agent noch ohne Agent verwaltet werden.

Alle verwalteten Installationen, die ausgewählten Geräten zugeordnet sind, werden immer der Reihenfolge nach bereitgestellt, unabhängig davon, ob die angegebenen Softwarepakete aus dem Softwarekatalog oder aus der Softwareliste stammen.

Inventaraktualisierungen von der Appliance erzwingen

Sie können die **Administratorkonsole** der Appliance verwenden, um Inventarmeldungen der Geräte zu erzwingen.

1. Rufen Sie die Liste *Geräte* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Inventar** und anschließend auf **Dashboard**.
2. Aktivieren Sie die Kontrollkästchen neben den Geräten, deren Inventar Sie aktualisieren möchten.

   Um eine Überlastung der Appliance zu vermeiden, sollten Sie nicht mehr als 50 Geräte gleichzeitig aktualisieren.
3. Wählen Sie **Aktion auswählen** > **Inventar erzwingen**.

Die Inventarinformationen werden aktualisiert.

Inventaraktualisierungen von Windows-Geräten erzwingen

Sie können Inventarmeldungen für Windows Geräte erzwingen, indem Sie auf den Geräten bestimmte Befehle ausführen.

1. Melden Sie sich beim Windows Gerät an und öffnen Sie eine Eingabeaufforderung.
2. Wechseln Sie zu einem der folgenden Verzeichnisse:
   - 32-Bit-Systeme: `C:\Programme\Quest\KACE\`
   - 64-Bit-Systeme: `C:\Programme (x86)\Quest\KACE\`

   HINWEIS: Verwenden Sie unter Windows Vista und neueren Windows Betriebssystemen zur Ausführung des Befehls die Option *Als Administrator ausführen*.
3. Geben Sie den folgenden Befehl ein:

   ```
   runkbot 4 0
   ```

Die Inventarinformationen werden aktualisiert.

Inventaraktualisierungen von Mac OS X Geräten erzwingen

Sie können Inventarmeldungen für Mac OS X Geräte erzwingen, indem Sie auf den Geräten bestimmte Befehle ausführen.

1. Melden Sie sich bei dem Mac OS X Gerät an und öffnen Sie über **Anwendungen** > **Dienstprogramme** ein Terminal.
2. Wechseln Sie in das folgende Verzeichnis:

   ```
   /Library/Application Support/Quest/KACE/bin/
   ```

3. Geben Sie den folgenden Befehl ein:

   ```
   sudo ./runkbot 2 0
   ```

Die Inventarinformationen werden aktualisiert.

Inventaraktualisierungen von unter Linux laufenden Geräten erzwingen

Sie können Inventarmeldungen für Linux Geräte erzwingen, indem Sie auf den Geräten bestimmte Befehle ausführen.

1. Melden Sie sich bei dem Linux Gerät an und öffnen Sie über **Anwendungen** > **System-Tools** ein Terminal.
2. Wechseln Sie in das folgende Verzeichnis:

   ```
   /opt/quest/kace/bin/
   ```

3. Geben Sie den folgenden Befehl ein:

   ```
   sudo ./runkbot 2 0
   ```

Die Inventarinformationen werden aktualisiert.

Verwalten ausstehender Geräte

Verwaltete Geräte, die in den letzten 90 Tagen nicht mit der Appliance kommuniziert haben, werden als "ausstehend" (MIA, Missing in Action) oder nicht erreichbar betrachtet. Sie können ausstehende Geräte nach Bedarf konfigurieren und verwalten.

HINWEIS: Die Lizenzvereinbarung berechtigt Sie zur Verwaltung einer bestimmten Anzahl von Geräten, die als verwaltete Computer, überwachte Geräte und Assets klassifiziert sind. Beachten Sie, dass Geräte auf diese Limits angerechnet werden, selbst wenn die Geräte als "Ausstehend" (MIA, Missing in Action) eingestuft sind oder nicht mehr verwendet werden. Geräte, die dem Inventar manuell oder über die API hinzugefügt wurden, werden bei den Lizenzlimits dagegen nicht berücksichtigt. Siehe Produktlizenzinformationen anzeigen.

HINWEIS: Rufen Sie zum Erhöhen der Lizenzkapazität die Quest Website auf: https://quest.com/buy.

Einstellungen ausstehender Geräte konfigurieren

Sie können die Appliance so konfigurieren, dass Geräte automatisch aus dem Inventar gelöscht werden, die sich während einer bestimmten Anzahl von Tagen nicht angemeldet haben. Durch automatisches Löschen ausstehender Geräte können Sie den Bedarf, ausstehende Geräte manuell zu löschen, verringern.

Beachten Sie, dass der Prozess zum Löschen ausstehender Geräte täglich um 03:45 Uhr ausgeführt wird und dabei bei einer Ausführung bis zu 100 Geräte gelöscht werden können. Wenn mehr als 100 ausstehende Geräte

zu löschen sind oder Sie Geräte sofort löschen müssen, empfiehlt es sich unter Umständen, die Geräte manuell zu löschen.

1. Rufen Sie die Liste *Geräte* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Inventar** und anschließend auf **Dashboard**.
2. Wählen Sie **Aktion auswählen > Einstellungen für 'Ausstehend' konfigurieren**, um die Seite *Einstellungen für 'Ausstehend'* aufzurufen.
3. Geben Sie die folgenden Informationen an:

Option	Beschreibung
Ausstehende Geräte automatisch entfernen	Verwaltete Geräte im Zustand "Ausstehend" sollten nach Ablauf des festgelegten Zeitraums archiviert oder gelöscht werden. Deaktivieren Sie das Kontrollkästchen, wenn ausstehende Geräte nicht automatisch archiviert oder gelöscht werden sollen.
Nach n Tagen	Die Anzahl der Tage, die ausstehende Geräte im Inventar verbleiben, wenn *Ausstehende Geräte automatisch löschen* ausgewählt ist. Geräte, die nicht innerhalb der angegebenen Anzahl von Tagen mit der Appliance kommunizieren, werden automatisch archiviert oder gelöscht.
MIA Asset-Geräte archivieren	Aktivieren Sie diese Option, um die MIA-Geräte nach der angegebenen Anzahl von Tagen zu archivieren.
Ausstehende Geräte löschen	Aktivieren Sie diese Option, um die MIA-Geräte nach der angegebenen Anzahl von Tagen dauerhaft zu löschen.

4. Klicken Sie auf **Speichern**.

   Geräte werden gelöscht, wenn der Löschvorgang täglich um 03:45 Uhr ausgeführt wird. Der Vorgang kann bis zu 100Geräte während eines Durchgangs löschen.

Wenn mehr als 100 ausstehende Geräte zu löschen sind oder Sie Geräte sofort löschen müssen, empfiehlt es sich unter Umständen, die Geräte manuell zu löschen. Siehe Ausstehende Geräte manuell löschen.

Labels ausstehenden Geräten zuweisen

Mit Labels können Sie Gruppen von ausstehenden Geräten verwalten.

1. Rufen Sie die Liste *Geräte* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Inventar** und anschließend auf **Dashboard**.
2. **Optional**: So können Sie ausstehende Geräte anzeigen: Wählen Sie rechts oberhalb der Tabelle in der Dropdown-Liste *Anzeigen nach* die Option **Ausstehend** und dann die Anzahl der Synchronisierungen

aus, die das Gerät verpasst hat (oder die Anzahl der Tage, seit denen das Gerät den Status "Ausstehend" aufweist).

3. Aktivieren Sie das Kontrollkästchen neben einem oder mehreren Geräten.
4. Wählen Sie **Aktion auswählen** > **Labels zuweisen**, um das Dialogfeld *Labels zuweisen* aufzurufen.
5. Suchen Sie nach Labels oder ziehen Sie ein aufgeführtes Label in den Bereich *Diese Labels übernehmen* und klicken Sie anschließend auf **Labels zuweisen**.

Ausstehende Geräte manuell löschen

Sie können ausstehende Geräte auch manuell löschen, wenn dies erforderlich wird.

Wie Sie die Appliance so konfigurieren können, dass alle ausstehenden Geräte automatisch gelöscht werden, erfahren Sie unter Einstellungen ausstehender Geräte konfigurieren.

1. Rufen Sie die Liste *Geräte* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Inventar** und anschließend auf **Dashboard**.
2. **Optional**: So können Sie ausstehende Geräte anzeigen: Wählen Sie rechts oberhalb der Tabelle in der Dropdown-Liste *Anzeigen nach* die Option **Ausstehend** und dann die Anzahl der Synchronisierungen aus, die das Gerät verpasst hat (oder die Anzahl der Tage, seit denen das Gerät den Status "Ausstehend" aufweist).
3. Aktivieren Sie das Kontrollkästchen neben einem oder mehreren Geräten.
4. Wählen Sie **Aktion auswählen** > **Löschen** und klicken Sie dann zum Bestätigen auf **Ja**.

Fehler beheben an Geräten, die nicht im Inventar angezeigt werden

Wenn über den Agent verwaltete Geräte nicht im Inventar angezeigt werden, überprüfen Sie den Agent und die Konfiguration der Appliance.

Standardmäßig tauschen KACE Agenten, die auf verwalteten Geräten installiert sind, Daten mit der Appliance aus. Hierzu nutzen sie das Protokoll HTTP über die Ports 80 und 443. Wenn Netzwerkkonnektivität vorhanden ist, aber neu installierte Agenten sich nicht mit der Appliance verbinden, gibt es u. U. Probleme mit dem Standard-Hostnamen `kbox` im DNS.

1. Installieren Sie den Agenten. Achten Sie dabei auf die korrekte Angabe des Hostnamens und der IP-Adresse:

   Windows

   ```
   msiexec /qn /i ampagent-6.x.xxxxx-x86.msi HOST=my_kace_sma
   ```

   Mac OS X

   ```
   hdiutil attach ampagent-6.x.xxxxx-all.dmg
   sudo sh -c 'KACE_SERVER=my_kace_sma installer -pkg /Volumes/Quest_KACE/AMPAgent.pkg
    -target /'
   hdiutil detach /Volumes/Quest_KACE
   ```

   Linux (RHEL und SLES)

   ```
   export KACE_SERVER=my_kace_sma
   export KACE_SERVER=my_kace_smasudo rpm -ivh ampagent-6.x.xxxxx.xxxx.xx.rpm
   ```
2. Um den Servernamen für ein bereits installiertes Gerät zu korrigieren, verwenden Sie das Dienstprogramm AMPTools:

Windows

32-Bit-Systeme: `"C:\Programme\Quest\KACE\AMPTools" host=myk1000`

64-Bit-Systeme: `"C:\Program Files (x86)\Quest\KACE\AMPTools" host=my_kace_sma`

Mac OS X

`/Library/Application\ Support/Quest/KACE/bin/AMPTools host=myk1000`

Linux

`/opt/quest/kace/bin/AMPTools host=my_kace_sma`

3. Überprüfen Sie, ob die Appliance auf Ping-Anfragen reagiert und über einen Webbrowser unter `http://`**appliance_hostname** erreichbar ist.
4. Achten Sie darauf, dass in den Internetoptionen nicht die Verwendung eines Proxy-Servers eingerichtet ist. Vergewissern Sie sich, dass der Proxy für das lokale Netzwerk oder **appliance_hostname** ausgeschlossen ist.
5. Stellen Sie sicher, dass keine Firewall oder Anwendungen zum Schutz vor Spyware die Kommunikation zwischen der Appliance und den Agenten-Komponenten behindern, beispielsweise:

KACE Agent-Komponenten für das jeweilige Betriebssystem

Betriebssystem	Komponenten des Agenten
Windows	ACUConfig.exe AMPAgent.exe AMPKickstart.exe AMPTools.exe AMPWatchDog.exe Inventory.exe KCopy.exe KDeploy.exe KInventory.exe konea.exe kpatch.exe KSWMeterSvc.exe KUserAlert.exe runkbot.exe
Mac OS X und Linux	AMPAgent AMPAgentBootup AMPctl AMPTools AMPWatchDog Inventar KBoxClient KCopy KDeploy KInventory konea kpatch

Betriebssystem	Komponenten des Agenten
	KSWMeterSvc KUpdater KUserAlert runkbot

6. Überprüfen Sie, ob die folgenden Prozesse ausgeführt werden:
   - **Windows: AMPAgent.exe, AMPWatchDog.exe, konea.exe.**
   - **Mac und Linux: AMPAgent, konea.**

Wenn der Agent nach der Überprüfung dieser Elemente immer noch keine Verbindung mit der Appliance herstellen kann, wenden Sie sich an den **Quest Support** unter https://support.quest.com/contact-support.

Abrufen von Informationen zum Service von Dell

Die Appliance führt regelmäßig einen Hintergrunddienst aus, der für die zum Inventar gehörenden Dell Geräte Informationen zum Service von Dell erfasst und aktualisiert.

Dieser Dienst läuft alle vier Stunden. Wenn mehrere Organisationen vorhanden sind, wählt der Dienst eine andere Organisation in einem Rundlauf-Verfahren aus und sammelt Serviceinformationen zu ca. 100 Geräten pro Organisation. So werden über einen längeren Zeitraum Serviceinformationen für alle Geräte von Dell gesammelt und aktualisiert.

Sie können Serviceinformationen von Dell jederzeit aktualisieren, und Sie können Berichte ausführen, um Serviceinformationen nachzuverfolgen.

HINWEIS: Die Informationen zum Service von Dell sind nur bei Computern von Dell verfügbar, die Bestandteil des Inventars sind. Die Appliance muss außerdem folgende Domäne erreichen können, um die Serviceinformationen abzurufen: **api.dell.com**. Siehe Erforderliche Websites für die Appliance verfügbar machen.

Sofortiges Abrufen von Informationen zum Service von Dell für ein einzelnes Gerät von Dell

Über die **Administratorkonsole** können Sie Serviceinformationen für ein beliebiges verwaltetes Gerät von Dell in Ihrem Inventar abrufen.

Wenn Sie viele Geräte von Dell besitzen, dauert es unter Umständen einige Zeit, bis die Serviceinformationen über den Hintergrunddienst der Appliance aktualisiert wurden.

1. Rufen Sie die Liste *Geräte* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Inventar** und anschließend auf **Dashboard**.
2. Klicken Sie in der Geräteliste auf den Namen eines Geräts von Dell, um die Seite *Gerätedetail* anzuzeigen.
3. Erweitern Sie im Abschnitt *Inventarinformationen* den Bereich **Hardware**.

   Die Dell Garantieinformationen werden im Abschnitt *Dell Serviceinformationen* angezeigt.
4. Klicken Sie auf **Aktualisieren**.

Die Serviceinformationen werden sofort aktualisiert.

Services von Dell erneuern

Auf der Dell Support-Website können Sie Services für in Ihrem Inventar enthaltene Geräte von Dell erneuern.

1. Rufen Sie die Liste *Geräte* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Inventar** und anschließend auf **Dashboard**.
2. Klicken Sie in der Geräteliste auf den Namen eines Geräts von Dell, um die Seite *Gerätedetail* anzuzeigen.
3. Erweitern Sie im Abschnitt *Inventarinformationen* den Bereich **Hardware**.
4. Klicken Sie im Abschnitt *Dell Serviceinformationen* auf den Link **support.dell.com**.

   Sie werden zu der Dell Support-Website weitergeleitet, wo Sie Ihre Informationen zum Service von Dell erneuern können, falls sie veraltet sind, oder weitere Informationen anzeigen können.

Berichte über den Service von Dell ausführen

Sie können Berichte ausführen, die den Servicestatus der Geräte von Dell im Inventar anzeigen. Wenn auf Ihrer Appliance die Organisationskomponente aktiviert wurde, können Sie diese Berichte sowohl auf Ebene der Organisation wie auch auf Systemebene ausführen.

1. Rufen Sie die Liste *Berichte* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Berichterstellung** und anschließend auf **Berichte**.
2. Wählen Sie rechts oberhalb der Tabelle in der Dropdown-Liste *Anzeigen nach* die Option **Service von Dell** aus, um die Berichte zum Service von Dell anzuzeigen.
3. Klicken Sie in der Spalte *Bericht generieren* auf einen Berichttyp, um den Bericht auszuführen.

   Siehe Informationen zu Berichten.

Verwalten von Anwendungen auf der Seite "Software"

Auf verwalteten Geräten gefundene Anwendungen werden auf der Seite *Software* aufgeführt.

Informationen zur Seite "Software"

Auf der Seite *Software* finden Sie alle auf verwalteten Geräten installierten Anwendungen sowie alle Anwendungen, die dem Inventar manuell oder durch Hochladen über die Inventar-API hinzugefügt wurden.

Wenn auf der Appliance die Organisationskomponente aktiviert wurde, verwalten Sie die Anwendungen für jede Organisation einzeln.

Die auf der Seite *Software* verfügbaren Informationen und Funktionen unterscheiden sich von den Informationen und Funktionen auf der Seite *Softwarekatalog*. Siehe Unterschiede zwischen den Seiten "Software" und "Softwarekatalog".

Elemente im Inventar der Seite "Software" anzeigen

Auf der Seite *Software* können Sie dem Inventar hinzugefügte Elemente anzeigen. Ist auf der Appliance die Organisationskomponente aktiviert, können Sie das Inventar der Seite *Software* für jede Organisation einzeln anzeigen.

1. Rufen Sie die Liste *Software* auf:
    a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
    b. Klicken Sie in der linken Navigationsleiste auf **Inventar** und anschließend auf **Software**.

Erfassen von Änderungen an Inventareinstellungen

Wenn Verlaufsabonnements zur Aufbewahrung von Informationen konfiguriert wurden, können Sie Details zu den an Einstellungen, Assets und Objekten vorgenommenen Änderungen anzeigen.

Diese Informationen beinhalten auch das Datum der Änderung und den Benutzer, der diese vorgenommen hat. Dies kann bei der Fehlerbehebung nützlich sein. Siehe Informationen zu den Verlaufseinstellungen.

Hinzufügen und Löschen von Anwendungen im Inventar der Seite "Software"

Anwendungen werden dem Inventar der Seite *Software* automatisch hinzugefügt, wenn verwaltete Geräte Inventarinformationen auf die Appliance hochladen. Außerdem können Sie der Seite *Software* bei Bedarf auch manuell Anwendungen hinzufügen.

Anwendungen manuell dem Inventar der Seite "Software" hinzufügen

Sie können Anwendungen bei Bedarf manuell der Inventarliste der Seite *Software* hinzufügen.

In der Regel ist es besser, Anwendungen automatisch zum Inventar der Appliance hinzufügen zu lassen, anstatt sie der Appliance manuell hinzuzufügen. Allerdings kann das manuelle Hinzufügen von Anwendungen nützlich sein, wenn Sie eine Anwendung hinzufügen möchten, die aktuell nicht auf verwalteten Geräten installiert ist. Sie können die Anwendung manuell hinzufügen, dann eine verwaltete Installation für diese erstellen und sie anschließend auf verwalteten Geräten bereitstellen.

Wenn Sie Anwendungen manuell hinzufügen, kann es sinnvoll sein, eine Regel für die benutzerdefinierte Inventarisierung zu verwenden, damit die Informationen zu den Anwendungen aktuell sind und die Pakete nicht jedes Mal neu installiert werden, wenn sich Agenten anmelden. Weitere Informationen finden Sie unter Erstellen benutzerdefinierter Inventarregeln.

TIPP: Manuell hinzugefügte Anwendungen werden auf der Seite *Software* angezeigt, nicht jedoch auf der Seite *Softwarekatalog*. Der Seite *Softwarekatalog* können Sie Anwendungen nicht manuell hinzufügen.

1. Rufen Sie die *Softwaredetailseite* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Inventar** und anschließend auf **Software**.
   c. Wählen Sie **Aktion auswählen** > **Neu**.
2. Machen Sie allgemeine Angaben: *Name*, *Version* und *Herausgeber*.

   Stellen Sie für die ordnungsgemäße nachgelagerte Berichterstellung sicher, dass diese Informationen im gesamten Softwareinventar einheitlich eingegeben werden.
3. Geben Sie die folgenden Informationen an:

Option	Beschreibung
Zuweisen zu Label	(Optional) Das Label, das dem Element zugewiesen wurde.
Anmerkungen	Geben Sie nach Bedarf beliebige weitere Informationen ein.
Unterstützte Betriebssysteme	Das Betriebssystem, auf dem die Anwendung ausgeführt wird. Die Bereitstellung der Anwendungen erfolgt nur auf Geräten mit den ausgewählten Betriebssystemen. a. Klicken Sie auf **Betriebssysteme verwalten**. b. Wählen Sie im daraufhin angezeigten Dialogfeld **Betriebssysteme** die Betriebssystemversionen in der Navigationsstruktur aus. Sie haben die Möglichkeit, Betriebssystemversionen nach Familie, Produkt, Architektur, Versions-ID oder Build-Version auszuwählen. Je nach Bedarf können Sie eine bestimmte Build-Version oder einen übergeordneten Knoten auswählen. Wenn Sie einen übergeordneten Knoten im Baum auswählen, werden die zugehörigen untergeordneten Knoten automatisch mit ausgewählt. Aufgrund dieses Verhaltens können Sie beliebige zukünftige Betriebssystemversionen auswählen, da Geräte in Ihrer verwalteten Umgebung hinzugefügt oder aktualisiert werden. Wenn Sie beispielsweise alle aktuellen und zukünftigen Versionen auswählen möchten, die mit der Windows 10 x64-Architektur verbunden sind, wählen Sie unter **Alle** > **Windows** > **Windows 10** die Option **x64** aus.
Regel für benutzerdefinierte Inventarisierung	(Optional) Die auf die Anwendung anzuwendenden Regeln für benutzerdefinierte Inventarisierung. Mithilfe von Regeln für benutzerdefinierte Inventarisierung können Sie Anwendungen und

Option	Beschreibung
	andere Elemente auf einem Gerät erkennen und Details für die Berichterstellung erfassen. So prüft die Appliance beispielsweise vor der Bereitstellung einer Anwendung zunächst, ob die Anwendung auf dem Gerät bereits vorhanden ist. Manchmal werden installierte Programme jedoch nicht unter *Software* oder in den Standardbereichen der Registrierung registriert. In diesen Fällen kann die Appliance die Software ohne zusätzliche Informationen vom Administrator möglicherweise nicht erkennen. Deshalb wiederholt die Appliance die Installation unter Umständen jedes Mal, wenn das Gerät eine Verbindung herstellt. Regeln für benutzerdefinierte Inventarisierung können dies verhindern. Die folgende Regel überprüft, ob die auf einem Gerät installierte Version von Network Associates VirusScan neuer ist als eine angegebene Version, bevor diese bereitgestellt wird. `RegistryValueGreaterThan(HKEY_LOCAL_MACHINE \Software\Network Associates\TVD \Shared Components\VirusScan Engine \4.0.xx,szDatVersion,4.0.44)` Siehe Abrufen von Werten von einem Gerät (Benutzerdefiniertes Inventarfeld).

4. Klicken Sie neben *Datei hochladen und verknüpfen* auf **Durchsuchen** oder **Datei auswählen**, um eine Datei zu finden. Klicken Sie dann auf **Öffnen** oder **Auswählen**.

   Zur Verteilung von Anwendungen mithilfe verwalteter Installationen oder Dateisynchronisierungen müssen die jeweiligen Anwendungsdateien mit der Anwendung verknüpft werden.

5. Damit die Datei nicht in die Replikationsfreigabe kopiert wird, wählen Sie **Zugehörige Datei nicht replizieren** aus.

   Dies ist bei großen Dateien sinnvoll, die die Benutzer nicht von Replikationsfreigaben installieren sollen, so z. B. Software Suites.

6. **Optional**: Wählen Sie eine *Kategorie* und eine *Bedrohungsstufe* für die Software aus.
7. Klicken Sie auf **Speichern**.

Verwandte Themen

Verwenden von Bedrohungsstufen und Kategorien für Software

Anwendungen löschen

Beim Löschen von Anwendungen von der Seite *Software* werden sie auch aus dem Inventar der Seite *Software* entfernt. Außerdem werden verwaltete Installationen oder Dateisynchronisationen entfernt, die mit Anwendungen verknüpft waren.

Wenn die gelöschten Anwendungen jedoch auf verwalteten Geräten installiert sind, werden die Datensätze für die Anwendungen mit neuen IDs neu erstellt, sobald die Geräte Inventarinformationen aktualisieren. Verwaltete Installationen und Dateisynchronisierungen, die mit den gelöschten Anwendungen verknüpft waren, werden jedoch nicht neu erstellt.

1. Rufen Sie die Liste *Software* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen

Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.

b. Klicken Sie in der linken Navigationsleiste auf **Inventar** und anschließend auf **Software**.

2. Aktivieren Sie das Kontrollkästchen neben einer oder mehreren Anwendungen.
3. Wählen Sie **Aktion auswählen** > **Löschen** und klicken Sie dann zum Bestätigen auf **Ja**.

Erstellen von Software-Assets

Zur Einrichtung der Lizenz-Compliance für Anwendungen, die auf der Seite *Software* angezeigt werden, müssen Sie zunächst Software-Assets für diese Anwendungen hinzufügen. Nachdem Sie Software-Assets erstellt haben, können Sie sie Lizenz-Assets zuordnen.

Sie können Assets für Anwendungen erstellen, die automatisch oder manuell zur Appliance hinzugefügt wurden.

HINWEIS: Software-Assets sind nicht erforderlich, um die Lizenz-Compliance für Anwendungen auf der Seite *Softwarekatalog* einzurichten.

Wenn auf der Appliance die Organisationskomponente aktiviert wurde, erstellen Sie Software-Assets für jede Organisation separat.

Software-Assets im Abschnitt "Inventar" hinzufügen

Sie können Software-Assets für Anwendungen hinzufügen, indem Sie die Anwendungen im Abschnitt *Inventar* der Liste *Software* auswählen.

Software-Assets können auch im Abschnitt *Assets* hinzugefügt werden. Siehe Software-Assets im Abschnitt "Assets" hinzufügen.

1. Rufen Sie die Liste *Software* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Inventar** und anschließend auf **Software**.
2. Aktivieren Sie das Kontrollkästchen neben einer oder mehreren Anwendungen.
3. Wählen Sie **Aktion auswählen** > **Asset erstellen**.

   Die Assets werden erstellt und erscheinen auf der Seite *Assets*.

Software-Assets im Abschnitt "Assets" hinzufügen

Im Abschnitt *Assets* können Sie einzelne Software-Assets hinzufügen.

Software-Assets können auch im Abschnitt *Inventar* hinzugefügt werden. Siehe Software-Assets im Abschnitt "Inventar" hinzufügen.

1. Rufen Sie die Liste *Assets* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.

b. Klicken Sie in der linken Navigationsleiste auf **Asset Management** und anschließend auf **Assets**.

2. Wählen Sie **Aktion auswählen** > **Neu** > **Software**, um die *Software-Asset-Detailseite* anzuzeigen.
3. Füllen Sie die Asset-Felder wie folgt aus:
   a. Geben Sie im Feld *Name* einen Namen für das Asset ein:

   z. B. Office Pro SW-Asset.

   b. **Optional**: Wählen Sie im Feld *Software* den Namen der Anwendung aus, die mit dem Asset verknüpft werden soll. Um nach einem Element zu suchen, tippen Sie dessen Namen in die Liste.
   c. **Optional**: Wählen Sie im Feld *Softwarelabel* aus der Dropdown-Liste *Label auswählen* ein Label aus. Die Liste ist anfangs noch leer, bis Sie ein Smart Label erstellt haben. Wenn Sie die Labelliste filtern möchten, geben Sie im Feld *Filter* einige Zeichen des Labelnamens ein.
4. Klicken Sie auf **Speichern**.

Das neue Asset wird auf der Seite *Assets* angezeigt.

Digitale Assets an Anwendungen anhängen und unterstützte Betriebssysteme auswählen

Um Anwendungen mithilfe von verwalteten Installationen oder **Benutzerkonsole**-Downloads an verwaltete Geräte zu verteilen, müssen Sie die entsprechenden digitalen Assets an Anwendungen anhängen. Digitale Assets sind die Dateien, die für die Bereitstellung erforderlich sind (z. B. Installationsprogramme). Darüber hinaus müssen Sie die unterstützten Betriebssysteme für die Anwendung auswählen. Sie können diese Aufgaben über die Detailseite *Software* durchführen.

Um einer Anwendung mehrere Dateien zuzuweisen, erstellen Sie eine ZIP-Datei mit den Dateien und weisen diese Archivdatei anschließend der Anwendung zu.

TIPP: Digitale Assets können an auf der Seite *Software* angezeigte Anwendungen angehängt werden, nicht jedoch an Elemente auf der Seite *Softwarekatalog*.

1. Rufen Sie die *Softwaredetailseite* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Inventar** und anschließend auf **Software**.
   c. Klicken Sie auf den Namen einer Softwareanwendung.
2. Führen Sie einen der folgenden Schritte aus:
   - **Klicken Sie neben** *Datei hochladen und verknüpfen* **auf Durchsuchen oder Datei auswählen.**
   - **Klicken Sie neben** *Client-Drop-Datei hochladen und verknüpfen* **auf Durchsuchen oder Datei auswählen. Diese Option ist nur verfügbar, wenn Sie Dateien zur Appliance oder zum Client-Drop-Speicherort der Organisation kopiert haben und diese Dateien größer als die im** *Dateigrößenfilter für Client Drop* **der Appliance angegebene Größe bzw. als die Client-Drop-Größe der Organisation sind. Wenn auf der Appliance die Organisationskomponente aktiviert wurde, stehen Dateien nur für die ausgewählte Organisation zur Verfügung. Um Dateien für mehrere Organisationen zur Verfügung zu stellen, kopieren Sie die Dateien zum Client Drop-Speicherort jeder einzelnen Organisation. Dateien kopieren und auf dem Client-Drop-Speicherort der Appliance ablegen.**
3. Suchen Sie nach der Datei, die hochgeladen werden soll, und klicken Sie dann auf **Öffnen** oder **Auswählen**.
4. Wählen Sie im Bereich *Unterstützte Betriebssysteme* die Betriebssysteme aus, auf denen die Anwendung installiert werden kann.
   a. Klicken Sie auf **Betriebssysteme verwalten**.

b. Wählen Sie im daraufhin angezeigten Dialogfeld **Betriebssysteme** die Betriebssystemversionen in der Navigationsstruktur aus.

Wählen Sie im daraufhin angezeigten Dialogfeld **Betriebssysteme** die Betriebssystemversionen in der Navigationsstruktur aus.

Sie haben die Möglichkeit, Betriebssystemversionen nach Familie, Produkt, Architektur, Versions-ID oder Build-Version auszuwählen. Je nach Bedarf können Sie eine bestimmte Build-Version oder einen übergeordneten Knoten auswählen. Wenn Sie einen übergeordneten Knoten im Baum auswählen, werden die zugehörigen untergeordneten Knoten automatisch mit ausgewählt. Aufgrund dieses Verhaltens können Sie beliebige zukünftige Betriebssystemversionen auswählen, da Geräte in Ihrer verwalteten Umgebung hinzugefügt oder aktualisiert werden. Wenn Sie beispielsweise alle aktuellen und zukünftigen Versionen auswählen möchten, die mit der Windows 10 x64-Architektur verbunden sind, wählen Sie unter **Alle** > **Windows** > **Windows 10** die Option **x64** aus.

HINWEIS: Wenn keine Betriebssysteme ausgewählt werden, kann die Anwendung nicht auf verwaltete Geräte verteilt werden. Bereitstellungen wie verwaltete Installationen können erstellt, aber nur dann bereitgestellt werden, wenn die korrekten Betriebssysteminformationen zur Verfügung gestellt werden.

5. Ändern Sie andere Details nach Bedarf und klicken Sie dann auf **Speichern**.

HINWEIS: In der Tabelle unten auf der Seite *Softwaredetail* sehen Sie, auf welchen Geräten die Software installiert ist.

Dateien kopieren und auf dem Client-Drop-Speicherort der Appliance ablegen

Sie können große Dateien, z. B. Anwendungsdateien und Sicherungsdateien, auf die Appliance hochladen, indem Sie sie kopieren und auf dem Client-Drop-Speicherort der Appliance ablegen. Das Kopieren von Dateien auf den Client-Drop-Speicherort ist eine Alternative zum Hochladen von Dateien über die **Administratorkonsole** mit dem Standard-HTTP-Mechanismus, bei dem es bei großen Dateien zu Browser-Timeouts kommen kann.

- Dateifreigabe aktivieren (Samba). Siehe Sicherheitseinstellungen für die Appliance konfigurieren.
- Wenn auf der Appliance die Organisationskomponente aktiviert ist, aktivieren Sie die Dateifreigabe für jede Organisation. Siehe Allgemeine Einstellungen auf Verwaltungs- oder organisationsspezifischer Ebene konfigurieren.
- Wenn auf der Appliance die Organisationskomponente nicht aktiviert ist, konfigurieren Sie die Dateigrößenfilter-Einstellung für Client Drop für die Appliance. Siehe Allgemeine Appliance-Einstellungen ohne aktivierte Organisationskomponente konfigurieren.
- Wenn auf der Appliance die Organisationskomponente aktiviert ist, konfigurieren Sie die Einstellung für die Client-Drop-Größe für jede Organisation. Siehe Allgemeine Einstellungen auf Verwaltungs- oder organisationsspezifischer Ebene konfigurieren.

1. Navigieren Sie in einem Dateisystemnavigator zum Client-Drop-Speicherort auf der Appliance:
   - **Geben Sie in Windows Explorer einen UNC-Pfad mit dem Hostnamen oder der IP-Adresse der Appliance ein. Beispiel: `\\kbox\clientdrop`. Verwenden Sie zwei umgekehrte Schrägstriche, um anzugeben, dass es sich bei dem Speicherort um einen Samba Pfad handelt.**
   - **Navigieren Sie unter Mac OS X zu Gehe zu > Mit Server verbinden und geben Sie dann in das Feld** *Serveradresse* **die SMB-Adresse ein.**
   - **Wählen Sie unter Linux Suche und geben Sie dann die SMB-Adresse ein.**

   Die Ordner `client Share` und `clientdrop Share` werden angezeigt.

HINWEIS: Wenn die Organisationskomponente aktiviert ist, hat jede Organisation einen separaten Client-Drop-Speicherort. Beispiel:

- ORG1: clientdrop
- ORG2: clientdrop_2
- ORG3: clientdrop_3

2. Wenn Sie dazu aufgefordert werden, geben Sie Ihre Anmeldeinformationen für den Client-Drop-Speicherort an. Diese Anmeldeinformationen sind in den Sicherheitseinstellungen der Appliance angegeben. Siehe Sicherheitseinstellungen für die Appliance konfigurieren.

   TIPP: Wenn Sie von einem Windows Gerät aus auf die Appliance zugreifen, geben Sie \admin in das Feld *Benutzername* ein. Dadurch wird verhindert, dass das System während der Authentifizierung workgroup\admin oder domain\admin verwendet.

3. Kopieren Sie Ihre Dateien auf den Client-Drop-Speicherort. Wenn auf der Appliance die Organisationskomponente aktiviert ist, kopieren Sie die Dateien zum Client-Drop-Speicherort für die Organisation, wo Sie die Dateien auswählen möchten.

   Die Dateien werden wie folgt angeboten:

   - **Anwendungsdateien**: Die Dateien sind auf der Seite *Softwaredetail* zur Auswahl verfügbar, wenn sie größer sind als die im *Dateigrößenfilter für Client Drop* für die Appliance bzw. in der Client-Drop-Größe für die Organisation konfigurierte Dateigröße. Wenn auf der Appliance die Organisationskomponente aktiviert wurde, stehen Dateien nur für die ausgewählte Organisation zur Verfügung. Um Dateien für mehrere Organisationen zur Verfügung zu stellen, kopieren Sie die Dateien zum Client Drop-Speicherort jeder einzelnen Organisation.
   - **Appliance-Sicherungsdateien**: An einem beliebigen Client-Drop-Speicherort abgelegte Appliance-Sicherungsdateien werden automatisch als Appliance-Sicherungsdateien erkannt und innerhalb von fünf Minuten auf der Seite *Sicherungseinstellungen* für die Auswahl verfügbar.

Wenn Sie Anwendungsdateien hochladen, die auf der Seite *Softwaredetail* auswählbar sein sollen, überprüfen Sie die Filtereinstellung *Client-Drop* für den Speicherort. Mit dieser Filtereinstellung wird festgelegt, ob die Dateien auf der Seite *Softwaredetail* auf der Grundlage ihrer Größe angezeigt werden. Informationen hierzu finden Sie unter Allgemeine Appliance-Einstellungen ohne aktivierte Organisationskomponente konfigurieren bzw. Organisationen hinzufügen oder bearbeiten.

Verwenden von Bedrohungsstufen und Kategorien für Software

Mithilfe von Bedrohungsstufen können Sie die relative Sicherheit von Anwendungen angeben und Anwendungen klassifizieren.

Diese Informationen werden ausschließlich zur Nachverfolgung bereitgestellt. Die Appliance erzwingt auf der Grundlage von Bedrohungsstufen oder Kategorien keine Richtlinien.

Softwarekategorien unterteilen Software in bestimmte Gruppen wie Softwaretreiber oder Sicherheitsanwendungen. Bei auf der Seite *Software* aufgelisteten Anwendungen werden die Kategorien manuell zugewiesen. Bei auf der Seite *Softwarekatalog* aufgelisteten Anwendungen werden die Softwarekategorien den Anwendungen automatisch zugewiesen.

Anwendungen Bedrohungsstufen zuweisen

Sie können Anwendungen, die auf der Seite *Software* aufgelistet sind, Bedrohungsstufen zuweisen. Elementen auf der Seite *Softwarekatalog* können keine Bedrohungsstufen zugewiesen werden.

1. Rufen Sie die Liste *Software* auf:

a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.

b. Klicken Sie in der linken Navigationsleiste auf **Inventar** und anschließend auf **Software**.

2. Aktivieren Sie das Kontrollkästchen neben einer oder mehreren Anwendungen.
3. Wählen Sie **Aktion auswählen** > **Bedrohungsstufe festlegen** und wählen Sie eine Bedrohungsstufe aus.

Anwendungen Kategorien zuweisen

Sie können Anwendungen, die auf der Seite *Software* aufgelistet sind, Kategorien zuweisen. Anwendungen, die auf der Seite *Softwarekatalog* aufgelistet sind, werden die Kategorien automatisch zugewiesen.

1. Rufen Sie die Liste *Software* auf:

   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.

   b. Klicken Sie in der linken Navigationsleiste auf **Inventar** und anschließend auf **Software**.

2. Aktivieren Sie das Kontrollkästchen neben einer oder mehreren Anwendungen.
3. Wählen Sie **Aktion auswählen** > **Kategorie festlegen** und anschließend eine Kategorie aus.

Auffinden und Labeling von Anwendungen

Für die Verwaltung Ihres Softwareinventars können Sie die erweiterte Suche und Labels verwenden.

Informationen zum Auffinden von Anwendungen mithilfe der erweiterten Suche

Mit der erweiterten Suche können Sie Werte für jedes im Softwareinventar vorhandene Feld angeben und das gesamte Inventar nach diesem bestimmten Wert oder nach einer bestimmten Kombination von Werten durchsuchen.

Mit der erweiterten Suche können Sie beispielsweise nach Geräten mit einem bestimmten Betriebssystem und einer bestimmten installierten Anwendung suchen. Siehe Auf Seitenebene mit erweiterten Optionen suchen.

Manuelle Softwarelabels hinzufügen

Im Abschnitt *Inventar* können Sie bei Bedarf manuelle Labels hinzufügen. Dies ist hilfreich, wenn Sie Softwareanwendungen manuell Labels zuweisen möchten, um sie zu gruppieren.

1. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
2. Führen Sie einen der folgenden Schritte aus:
   - **Wählen Sie Inventar > Software aus, um die Seite** *Software* **anzuzeigen.**
   - **Wählen Sie Inventar > Softwarekatalog aus, um die Seite** *Softwarekatalog* **anzuzeigen.**
3. Wählen Sie **Aktion auswählen** > **Label hinzufügen**.
4. Geben Sie im Fenster *Label hinzufügen* einen Namen für das Label ein.

TIPP: Vermeiden Sie in Labelnamen die Verwendung des umgekehrten Schrägstrichs (\). Wenn Sie einen umgekehrten Schrägstrich in einem Labelnamen verwenden müssen, fügen Sie einen zweiten umgekehrten Schrägstrich hinzu (\\), damit er nicht als Befehl interpretiert wird.

5. Klicken Sie auf **Speichern**.

Manuelle Labels zuweisen oder Labels von Software entfernen

Sie können der Software im Inventar der Appliance bei Bedarf manuelle Labels zuweisen oder manuelle Labels entfernen.

Fügen Sie ein manuelles Label hinzu. Siehe Manuelle Softwarelabels hinzufügen.

1. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
2. Führen Sie einen der folgenden Schritte aus:
   - **Wählen Sie Inventar > Software aus, um die Seite** *Software* **anzuzeigen.**
   - **Wählen Sie Inventar > Softwarekatalog aus, um die Seite** *Softwarekatalog* **anzuzeigen.**
3. Aktivieren Sie das Kontrollkästchen neben einer oder mehreren Anwendungen.
4. Führen Sie einen der folgenden Schritte aus:
   - **Wählen Sie Aktion auswählen > Label zuweisen und anschließend das zuzuweisende Label aus.**
   - **Wählen Sie Aktion auswählen > Label entfernen und anschließend das zu entfernende Label aus.**

Weitere Informationen zu Labels finden Sie unter Verwalten manueller Labels.

Smart Labels für Software erstellen

Bei Bedarf können Sie auf der Seite *Software* Smart Labels für Software hinzufügen. Dies ist hilfreich, wenn Sie Anwendungen automatisch auf der Grundlage der Kriterien des Smart Labels gruppieren möchten.

Mit einem Smart Label können Sie beispielsweise alle Kopien einer Anwendung von einem bestimmten Anbieter gruppieren. Das Label wird in diesem Fall automatisch allen Anwendungen zugewiesen, die Sie bereits von dem Anbieter erworben haben bzw. zukünftig erwerben werden. Siehe Verwalten von Smart Labels.

HINWEIS: Smart Labels können nicht auf Anwendungen auf der Seite *Softwarekatalog* angewendet werden.

1. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
2. Wählen Sie **Inventar** > **Software** aus, um die Seite *Software* anzuzeigen.
3. Klicken Sie über der Anwendungsliste auf der rechten Seite auf die Registerkarte **Smart Label**, um den Bereich *Smart Label* anzuzeigen.

4. Geben Sie die erforderlichen Kriterien ein, um nach Anwendungen eines bestimmten Herstellers zu suchen:

   `Ansprechpartner beim Hersteller | enthält | Smith`

5. Klicken Sie auf **Testen**.

   Es werden alle Elemente angezeigt, die den festgelegten Kriterien entsprechen.

6. Passen Sie die Kriterien an, bis die Ergebnisse Ihren Erwartungen entsprechen.
7. Führen Sie im Menü *Label auswählen* einen der folgenden Schritte aus:

   - **Wählen Sie ein vorhandenes Label aus, um es mit diesem Smart Label zu verknüpfen. Geben Sie in das Feld** *Label auswählen* **einen Begriff ein, um nach vorhandenen Labels zu suchen.**

     HINWEIS: Wenn Sie statt eines Labels eine Labelgruppe auswählen, können Sie das Smart Label nicht auf einen Patching-Zeitplan anwenden. Patch-Zeitpläne können nur Smart Labels verwenden, die auf einem einzelnen Element basieren.

   - **Geben Sie einen neuen Namen für das Smart Label im Feld** *Label auswählen* **ein und drücken Sie Enter bzw. die Eingabetaste.**

     HINWEIS: Drücken Sie **Enter** bzw. die **Eingabetaste**, nachdem Sie einen neuen Smart Label-Namen eingegeben haben, um den Text aus dem Suchfeld in das Label-Feld zu verschieben.

8. Klicken Sie auf **Erstellen**.

Smart Labels werden automatisch Anwendungen zugewiesen oder von diesen entfernt, wenn die Anwendungen auf der Seite *Inventar* > *Software* aktualisiert werden und den angegebenen Kriterien entsprechen.

Verwalten des ITNinja-Feed

Mit dem ITNinja Feed können Sie systemverwaltungsbezogene Inhalte von ITNinja in der **Administratorkonsole** anzeigen. Zum Aktivieren und Deaktivieren des ITNinja-Feeds müssen Sie Ihre Datenfreigabeeinstellungen ändern.

ITNinja.com (früher AppDeploy.com) ist eine von Quest KACE gesponserte, produktübergreifende Community-Website mit dem Schwerpunkt IT. Sie ist das führende Internet-Ziel für IT-Spezialisten zum Austausch von Informationen und für Fragen auf dem Gebiet der Systemverwaltung. Die Website bietet einen Bereich mit Fragen und Antworten sowie eine Blog-Plattform. Wenn Sie sich entscheiden, anonyme Nutzungsdaten an ITNinja weiterzugeben, wird der ITNinja Feed in der **Administratorkonsole** auf den Detailseiten zu Software, verwalteter Installation oder Dateisynchronisierung angezeigt. Der Feed ist nicht auf der Detailseite des *Softwarekatalogs* verfügbar. Siehe ITNinja-Feed aktivieren.

ITNinja-Feed aktivieren

Konfigurieren Sie zum Aktivieren des ITNinja-Feeds die Appliance-Einstellungen für die Weitergabe anonymer Nutzungsdaten an Quest.

1. Navigieren Sie zur *Systemsteuerung* der Appliance:
   - **Wenn die Organisationskomponente nicht für die Appliance aktiviert ist, melden Sie sich bei der Administratorkonsole an: `https://appliance_hostname/admin`, und wählen Sie dann Einstellungen > Systemsteuerung aus.**
   - **Wenn die Organisationskomponente für die Appliance aktiviert ist, melden Sie sich bei der Systemverwaltungskonsole der Appliance an: `https://appliance_hostname/system`. Oder wählen Sie in der Dropdown-Liste rechts oben auf der Seite den Eintrag System aus, und klicken Sie dann auf Einstellungen > Systemsteuerung.**
2. Klicken Sie auf **Allgemeine Einstellungen**.
3. Aktivieren Sie im Abschnitt *An Quest weitergeben* die Kontrollkästchen *Zusammenfassung von Nutzungsdaten weitergeben* und *Detaillierte Nutzungsdaten weitergeben*.
4. Klicken Sie auf **Speichern**.

Weitere Informationen zu allgemeinen Appliance-Einstellungen finden Sie unter Allgemeine Appliance-Einstellungen bei aktivierter Organisationskomponente konfigurieren.

ITNinja-Informationen anzeigen

Bei aktiviertem ITNinja Feed können Sie ITNinja Informationen zu verwalteten Installationen und Dateisynchronisierungen sowie zu verwalteter Software auf Detailseiten in der **Administratorkonsole** anzeigen.

Siehe ITNinja-Feed aktivieren.

HINWEIS: ITNinja-Informationen stehen für Software auf der Seite *Software* zur Verfügung, nicht jedoch für Software auf der Seite *Softwarekatalog*.

ITNinja-Informationen für Software anzeigen

Sie können die ITNinja-Informationen auf der Seite *Softwaredetail* anzeigen.

Der ITNinja-Feed muss aktiviert sein. Siehe ITNinja-Feed aktivieren.

1. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
2. Wählen Sie **Inventar > Software** aus, um die Seite *Software* anzuzeigen.
3. Klicken Sie auf den Namen einer Anwendung, um die *Softwaredetailseite* anzuzeigen.
4. Scrollen Sie nach unten zum ITNinja-Abschnitt.

ITNinja-Informationen für verwaltete Installationen anzeigen

Sie können ITNinja-Informationen für verwaltete Installationen anzeigen.

Der ITNinja-Feed muss aktiviert sein. Siehe ITNinja-Feed aktivieren.

1. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in*

Verwaltungskopfzeile anzeigen aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.

2. Klicken Sie auf **Verteilung**, um die Seite *Verwaltete Installationen* anzuzeigen.
3. Klicken Sie auf den Namen einer verwalteten Installation, um die *Detailseite für die verwaltete Installation* anzuzeigen.
4. Scrollen Sie nach unten zum ITNinja-Abschnitt.

ITNinja-Informationen für Dateisynchronisierungen anzeigen

Sie können ITNinja-Informationen für Dateisynchronisierungen anzeigen.

Der ITNinja-Feed muss aktiviert sein. Siehe ITNinja-Feed aktivieren.

1. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
2. Wählen Sie **Verteilung** > **Dateisynchronisierungen** aus, um die Seite *Dateisynchronisierungen* anzuzeigen.
3. Klicken Sie auf den Namen einer Dateisynchronisierung, um die *Detailseite für die Dateisynchronisierung* anzuzeigen.
4. Scrollen Sie nach unten zum ITNinja-Abschnitt.

ITNinja-Feed deaktivieren

Soll der ITNinja-Feed nicht in der **Administratorkonsole** angezeigt werden, müssen Sie die Appliance-Einstellungen für die Weitergabe von Daten an Quest ändern. Dadurch wird der ITNinja-Feed deaktiviert.

1. Navigieren Sie zur *Systemsteuerung* der Appliance:
   - **Wenn die Organisationskomponente nicht für die Appliance aktiviert ist, melden Sie sich bei der Administratorkonsole an: `https://appliance_hostname/admin`, und wählen Sie dann Einstellungen > Systemsteuerung aus.**
   - **Wenn die Organisationskomponente für die Appliance aktiviert ist, melden Sie sich bei der Systemverwaltungskonsole der Appliance an: `https://appliance_hostname/system`. Oder wählen Sie in der Dropdown-Liste rechts oben auf der Seite den Eintrag System aus, und klicken Sie dann auf Einstellungen > Systemsteuerung.**
2. Klicken Sie auf **Allgemeine Einstellungen**.
3. Deaktivieren Sie im Abschnitt *An Quest weitergeben* das Kontrollkästchen *Detaillierte Nutzungsdaten weitergeben*.
4. Klicken Sie auf **Speichern**.

Weitere Informationen zu allgemeinen Appliance-Einstellungen finden Sie unter Allgemeine Appliance-Einstellungen bei aktivierter Organisationskomponente konfigurieren.

Verwalten des Softwarekataloginventars

Anwendungen, die auf verwalteten Geräten vorhanden sind und den Anwendungsdefinitionen im Softwarekatalog entsprechen, werden als Softwarekataloginventar bezeichnet.

Informationen zum Softwarekatalog

Der Softwarekatalog ist eine Datenbank mit standardisierten Informationen zu mehr als 60.000 Windows und Mac Anwendungen und Software-Suites. Die Informationen im Katalog umfassen den Namen, die Version, den Herausgeber sowie die Kategorie jeder Anwendung oder Suite sowie das Betriebssystem, unter dem die Anwendung oder Suite ausgeführt wird.

Der Softwarekatalog steht für alle KACE SMAs zur Verfügung, auf denen Version 5.5 oder höher ausgeführt wird. Der Katalog wird kontinuierlich aktualisiert und von Quest gepflegt, um sicherzustellen, dass er umfassend, korrekt und aktuell ist.

Wenn verwaltete Geräte, auf denen Agenten-Software der Version 5.5 oder höher installiert ist, Anwendungsinventar melden, werden diese Inventarinformationen mit den Elementen im Softwarekatalog verglichen. Auf der Registerkarte *Softwarekatalog* werden dann standardisierte Informationen zum Anwendungsinventar angezeigt.

Der Softwarekatalog bietet Ihnen folgende Möglichkeiten:

- Identifizieren der auf Geräten installierten Software und Anzeigen von standardisierten Informationen zu dieser Software. Siehe Anzeigen von Informationen im Softwarekatalog.
- Aktivieren der Erfassung zum Sammeln detaillierter Informationen über die Nutzung der Software. Siehe Verwenden der Erfassung der Softwarenutzung.
- Verknüpfen von Lizenzinformationen mit Software im Softwarekatalog. So können Sie die Softwarelizenz-Compliance und -Nutzung von Geräten überwachen. Siehe Hinzufügen von Lizenz-Assets für das Softwarekataloginventar.
- Identifizieren und Kennzeichnen von Software als Nicht zulässig. Auf diese Weise können Sie die Nutzung von Software verhindern, die als Nicht zulässig gekennzeichnet ist. Siehe Verwenden der Anwendungssteuerung.

Der Katalog enthält nur Informationen zu Software, die zur Ausführung auf Windows und Mac Betriebssystemen entwickelt wurde. Software zur Ausführung unter Linux und anderen nicht unterstützten Betriebssystemen steht im Katalog nicht zur Verfügung.

Anwendungsklassifizierungen

Anwendungen auf der Seite Softwarekatalog werden als Erkannt, Nicht erkannt (Katalogisiert) und Nicht katalogisiert klassifiziert. Die Klassifizierung einer Anwendung bestimmt, welche Aktionen Sie durchführen können und welche Art von Informationen für die Anwendungen verfügbar ist.

Erkannte Anwendungen

Erkannte Anwendungen sind ausführbare Dateien im Inventar der Appliance, die den Definitionen von Anwendungen im Softwarekatalog entsprechen. Sie können die Nutzungserfassung für erkannte Anwendungen und Suites aktivieren, diese Anwendungen als Nicht zulässig kennzeichnen und Lizenzinformationen für sie hinzufügen. Außerdem können Sie die Liste mit den erkannten Anwendungen im CSV-Format exportieren. Sie können die Liste mit erkannten Anwendungen, die Liste mit nicht katalogisierten Anwendungen und die Liste der lokal katalogisierten Anwendungen exportieren. Sie können nicht den gesamten Softwarekatalog exportieren.

Nicht erkannte Anwendungen

Anwendungen, die nicht im Appliance-Inventar, aber im Quest KACE Softwarekatalog enthalten sind, werden als nicht erkannte Anwendungen bezeichnet. Sie können die Erfassung für nicht erkannte Anwendungen aktivieren, sie als Nicht zulässig kennzeichnen und Lizenzinformationen hinzufügen. Da die Anwendungen jedoch nicht im lokalen Appliance-Inventar enthalten sind, kann die Liste nicht erkannter Anwendungen nicht ins CSV-Format exportiert werden.

Nicht katalogisierte Anwendungen

Nicht katalogisierte Anwendungen oder ausführbare Dateien, die sich im Inventar der Appliance befinden, aber nicht im Softwarekatalog aufgeführt sind. Sie können Anwendungen, die als nicht katalogisiert aufgeführt sind, auf der Seite *Softwarekatalog* anzeigen. Allerdings können Sie die Erfassung der Nutzung für nicht katalogisierte Anwendungen nicht aktivieren, sie nicht als Nicht zulässig kennzeichnen und auch keine Lizenzinformationen über sie hinzufügen.

Nicht katalogisierte Anwendungen müssen zum lokalen oder öffentlichen Softwarekatalog hinzugefügt werden, bevor ihre Nutzung erfasst werden kann und sie als Nicht zulässig gekennzeichnet oder mit Lizenzinformationen verknüpft werden können. Siehe Hinzufügen von Anwendungen zum Softwarekatalog.

HINWEIS: Wenn die Datenaufbewahrung für nicht katalogisierte Anwendungen deaktiviert ist, ist die Liste nicht katalogisierter Anwendungen leer. Siehe Allgemeine Einstellungen auf Verwaltungs- oder organisationsspezifischer Ebene konfigurieren.

Informationen zu katalogisierten Anwendungen

Katalogisierte Anwendungen sind ausführbare Dateien, die sich in der offiziellen Softwarekatalog-Datenbank befinden. Hierzu zählen sowohl Anwendungen, die im Appliance-Inventar enthalten sind (Erkannte Anwendungen), als auch Anwendungen, die nicht im Inventar enthalten sind (Nicht erkannte Anwendungen).

Informationen zu lokal katalogisierten Anwendungen

Anwendungen, die nicht in der offiziellen Version des Softwarekatalogs enthalten sind, jedoch zur lokalen Version der Appliance hinzugefügt wurden, werden als lokal katalogisierte Anwendungen bezeichnet.

Informationen zu nicht zulässigen Anwendungen

Nicht zulässige Anwendungen sind Anwendungen, die auf der Seite *Softwarekatalog* als "Nicht zulässig" gekennzeichnet wurden.

Windows und Mac Anwendungen können nur dann als Nicht zulässig gekennzeichnet werden, wenn sie als erkannte, nicht erkannte oder lokal katalogisierte Anwendungen klassifiziert sind. Nicht katalogisierte Anwendungen können erst dann als Nicht zulässig gekennzeichnet werden, wenn sie zum Softwarekatalog hinzugefügt wurden. Als "Nicht zulässig" gekennzeichnete Anwendungen können gesperrt oder ihr Zugriff auf verwalteten Geräten verweigert werden, falls diesen Geräten ein für die Anwendungssteuerung aktiviertes Label zugewiesen wurde.

Siehe Verwenden der Anwendungssteuerung.

Anwendungskategorien

Anwendungen im Softwarekatalog werden in Kategorien gruppiert, wie Produktivitätsanwendungen und Virenschutzprogramme.

Diese Kategorien sind hilfreich für die Berichterstellung und Lizenz-Compliance. Die Nutzung von Anwendungen der Kategorie *Betriebssystem* kann nicht erfasst werden.

Informationen zur Erfassung von Softwarekataloginformationen

Die Appliance erfasst in bestimmten Intervallen Informationen zu allen ausführbaren Dateien, die auf verwalteten Geräten installiert sind. Diese Informationen umfassen den Herausgeber der ausführbaren Datei, das Veröffentlichungsdatum, die Dateigröße und Registrierungsinformationen.

Diese Informationen werden mit den Informationen im Softwarekatalog verglichen, um zu ermitteln, ob die erkannten Anwendungen katalogisiert oder nicht katalogisiert sind. Siehe Intervalle für die Erfassung der Nutzung und des Inventars planen.

Informationen zur Verwendung des Softwarekatalogs mit der Organisationskomponente

Jede Appliance verfügt über einen einzigen Softwarekatalog. Wenn die Organisationskomponente in Ihrer Appliance aktiviert ist, verwenden alle Organisationen denselben Softwarekatalog, der auf der Appliance installiert ist. Darüber hinaus stehen lokal katalogisierte Anwendungen allen Organisationen zur Verfügung.

Nicht katalogisierte Anwendungen und Einstellungen wie beispielsweise zur Erfassung der Nutzung und zur Lizenzkonfiguration sind jedoch organisationsspezifisch. Wenn Sie zum Beispiel die Erfassung der Nutzung für eine Anwendung in einer Organisation aktivieren, wird sie nur für diese eine Organisation aktiviert. Die Erfassung der Nutzung und andere Einstellungen werden für jede Organisation separat aktiviert.

Ebenso sind erkannte Anwendungen organisationsspezifisch. Anwendungen werden nur dann als Erkannt gekennzeichnet, wenn sie im Inventar der Organisation gefunden wurden.

Informationen zur Lokalisierung von Softwarekataloginformationen

Die Anwendungskategorien im Softwarekatalog sind entsprechend den Gebietsschema-Einstellungen der Appliance lokalisiert. Anwendungsnamen wie Microsoft Excel werden jedoch nicht katalogisiert.

Informationen dazu, wie Sie helfen können, den Softwarekatalog zu verbessern

Der Softwarekatalog wird kontinuierlich aktualisiert, um neue Informationen oder neue Anwendungen zu ergänzen und Katalogisierungsanforderungen zu bearbeiten. Sie können dabei helfen, den Katalog zu verbessern, indem Sie die Inventarinformationen Ihrer Appliance für Quest KACE und die ITNinja Community freigeben.

Das Quest KACE Katalogteam verwendet diese Informationen, um neue Anwendungen zu identifizieren und Anwendungsnamen und -versionen zu standardisieren. Siehe Konfigurieren der Datenfreigabeeinstellungen.

Unterschiede zwischen den Seiten "Software" und "Softwarekatalog"

Sowohl die Seite "Software" als auch die Seite "Softwarekatalog" nutzt die von verwalteten Geräten gemeldeten Anwendungsinformationen. Die beiden Seiten stehen jedoch für unterschiedliche Inventarsysteme und die Vorgehensweise bei Softwareverwaltungsaufgaben variiert je nach System.

Weitere Informationen zur Verwaltung von Informationen auf der Seite *Software* finden Sie unter Verwalten von Anwendungen auf der Seite "Software". Die folgende Tabelle enthält einen Vergleich der Seiten *Software* und *Softwarekatalog*:

Aufgabe	Seite "Software"	Seite "Softwarekatalog"
Prozess für die Inventarerfassung	Verwendet den Prozess für die klassische Inventarerfassung, der in Version 5.4 der Appliance zur Verfügung steht. Verwaltete Geräte, die Version 5.4 und älter des Agenten ausführen,	Verwendet einen Prozess für die Inventarerfassung, der in Version 5.5 der Appliance eingeführt wurde. Dieser Prozess sammelt Informationen zu jeder

Aufgabe	Seite "Software"	Seite "Softwarekatalog"
	melden Inventar nur auf der Seite *Software*, nicht jedoch auf der Seite *Softwarekatalog*. Verwaltete Geräte, die mindestens Version 5.5 des Agenten ausführen, melden Inventar sowohl auf der Seite *Software* als auch auf der Seite *Softwarekatalog*.	ausführbaren Datei, die auf verwalteten Geräten installiert ist. Verwaltete Geräte müssen mindestens Version 5.5 des Agenten ausführen, um Inventar auf der Seite *Softwarekatalog* melden zu können.
Anzeigen von Informationen zum Softwareinventar	Auf der Seite *Software* werden Informationen über alle Anwendungen angezeigt, die auf verwalteten Geräten ermittelt oder manuell bzw. über WSAPI zum Inventar der Appliance hinzugefügt wurden.	Informationen zum Softwareinventar werden auf der Seite *Softwarekatalog* folgendermaßen dargestellt: • **Erkannt**: Auf verwalteten Geräten installierte Anwendungen, die den Anwendungsinformationen im Softwarekatalog entsprechen • **Nicht erkannt**: Anwendungen im Softwarekatalog, die nicht auf verwalteten Geräten installiert sind • **Nicht katalogisiert**: Anwendungen, die auf verwalteten Geräten installiert, jedoch nicht im Softwarekatalog enthalten sind Manuell oder über die WSAPI zur Appliance hinzugefügte Inventarinformationen sind auf der Seite *Softwarekatalog* nicht verfügbar.
Erfassen der Anwendungsnutzung	Nicht verfügbar	Wird für jede Anwendung auf der Seite *Softwarekatalog* oder auf der Seite *Softwarekatalogdetails* separat aktiviert.
Verfolgen von Lizenzinformationen für Anwendungen	Wird durch Erstellen eines Software-Assets und eines Lizenz-Assets für die Anwendung aktiviert. Lizenzinformationen werden im Dashboard-Widget zur Lizenz-Compliance angezeigt. Sie sind nicht auf der Seite *Lizenz-Compliance* enthalten.	Wird aktiviert, wenn ein Lizenz-Asset erstellt und einer Anwendung im Softwarekatalog zugeordnet wird. Lizenzinformation werden sowohl auf der Seite *Lizenz-Compliance* als auch im Dashboard-Widget zur Lizenz-Compliance angezeigt. Siehe Informationen zur Lizenz-Compliance für Anwendungen im Softwarekatalog.

Aufgabe	Seite "Software"	Seite "Softwarekatalog"
Kennzeichnen von Anwendungen als "Nicht zulässig"	Nicht verfügbar	Verfügbar als Kennzeichnung, die auf der Seite *Softwarekatalogdetails* vorgenommen wird. Siehe Anwendungen und Suites als "Nicht zulässig" kennzeichnen.
Anhängen digitaler Assets an Anwendungen	Verfügbar auf den Seiten mit *Softwaredetails*; wird für das Bereitstellen von Software auf verwalteten Geräten verwendet. Siehe Digitale Assets an Anwendungen anhängen und unterstützte Betriebssysteme auswählen.	Nicht verfügbar
Verteilen von Software in verwalteten Installationen oder Dateisynchronisierungen	Verfügbar bei der Verwendung von Anwendungen, die mit digitalen Assets verknüpft sind. Siehe Verteilen von Software und Verwenden von Wake on LAN.	Nicht verfügbar
ITNinja-Tipps und -Informationen anzeigen	Verfügbar auf den Seiten *Softwaredetail*. Siehe Verwalten des ITNinja-Feed.	Nicht verfügbar
Anzeigen von zusammenfassenden Lizenzinformationen	Verfügbar in den Diagrammen *Lizenz-Compliance* und *Softwarelizenz-Konfiguration* auf der Seite *Dashboard*. Siehe Informationen zu Dashboard-Widgets.	Verfügbar in den Diagrammen *Lizenz-Compliance* und *Softwarelizenz-Konfiguration* auf der Seite *Dashboard*. Siehe Informationen zu Dashboard-Widgets.
Festlegen der Bedrohungsstufen für die Software	Verfügbar in Liste *Software*. Siehe Verwenden von Bedrohungsstufen und Kategorien für Software.	Nicht verfügbar
Festlegen von Softwarekategorien	Verfügbar auf den Seiten *Softwaredetail*. Siehe Anwendungen Kategorien zuweisen.	Vordefiniert durch das Quest KACE Softwarekatalogteam.

Anzeigen von Informationen im Softwarekatalog

Sie können Anwendungsinformationen auf der Seite "Softwarekatalog" anzeigen.

Listen von erkannten und nicht erkannten Anwendungen anzeigen

In der Liste *Softwarekatalog* können Sie erkannte und nicht erkannte Anwendungen anzeigen.

Erkannte Anwendungen sind ausführbare Dateien im Inventar der Appliance, die den Definitionen von Anwendungen im Softwarekatalog entsprechen. Sie können die Nutzungserfassung für erkannte Anwendungen und Suites aktivieren, diese Anwendungen als Nicht zulässig kennzeichnen und Lizenzinformationen für sie hinzufügen. Außerdem können Sie die Liste mit den erkannten Anwendungen im CSV-Format exportieren. Sie können die Liste mit erkannten Anwendungen, die Liste mit nicht katalogisierten Anwendungen und die Liste der lokal katalogisierten Anwendungen exportieren. Sie können nicht den gesamten Softwarekatalog exportieren.

Anwendungen, die nicht im Inventar, aber im Quest KACE Softwarekatalog enthalten sind, werden als nicht erkannte Anwendungen bezeichnet. Sie können die Erfassung für nicht erkannte Anwendungen aktivieren, sie als Nicht zulässig kennzeichnen und Lizenzinformationen hinzufügen. Da die Anwendungen jedoch nicht im lokalen Inventar enthalten sind, kann die Liste nicht erkannter Anwendungen nicht ins CSV-Format exportiert werden.

1. Rufen Sie die Liste *Softwarekatalog* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Inventar** und anschließend auf **Softwarekatalog**.
2. Klicken Sie auf die Registerkarte **Erkannt**.

   Die Liste wird gefiltert, um nur die Anwendungen anzuzeigen, die als erkannt klassifiziert wurden. Die Informationen über erkannte Anwendungen umfassen Folgendes:

Element	Beschreibung
Name	Der Name und die Version der Softwareanwendung. Wenn es sich bei der Anwendung um eine Suite handelt, wird der Name fett dargestellt. Beispiel: **Microsoft Office 2010 Professional**.
Herausgeber	Der Herausgeber der Anwendung. Diese Information wird vereinheitlicht, um eine korrekte Berichterstellung zu gewährleisten. Zum Beispiel werden „Microsoft Corp.“ und „Microsoft Inc.“ als „Microsoft Corporation“ gemeldet.
Kategorie	Die vom Softwarekatalogteam festgelegte Kategorie der Anwendung
Installiert	Die Anzahl verwalteter Geräte, auf denen die Anwendung installiert ist Klicken Sie auf eine Zahl, um Geräteinformationen anzuzeigen.
Lizenzen	Die Anzahl von Lizenzen, die für die Anwendung zur Verfügung stehen. Diese Information steht nur zur Verfügung, wenn ein Lizenz-Asset mit der Anwendung verknüpft wurde. Siehe Hinzufügen von Lizenz-Assets für das Softwarekataloginventar.

Element	Beschreibung
Differenz	Die Anzahl der restlichen nicht verwendeten Lizenzen. Diese Information steht nur zur Verfügung, wenn ein Lizenz-Asset mit der Anwendung verknüpft wurde.
Kürzlich hinzugefügt	Die Anzahl von Geräten, auf denen die Anwendung im Laufe der letzten sieben Tage installiert wurde
Kürzlich entfernt	Die Anzahl von Geräten, auf denen die Anwendung im Laufe der letzten sieben Tage deinstalliert wurde

3. Klicken Sie auf die Registerkarte **Nicht erkannt**.

   Die Liste wird gefiltert, um nur die Anwendungen anzuzeigen, die als Nicht erkannt klassifiziert wurden. Die Informationen über nicht erkannte Anwendungen umfassen Folgendes:

Element	Beschreibung
Name	Der Name und die Version der Softwareanwendung. Wenn es sich bei der Anwendung um eine Suite handelt, wird der Name fett dargestellt. Beispiel: **Microsoft Office 2010 Professional**.
Herausgeber	Der Herausgeber der Anwendung. Diese Information wird vereinheitlicht, um eine korrekte Berichterstellung zu gewährleisten. Zum Beispiel werden „Microsoft Corp.“ und „Microsoft Inc.“ als „Microsoft Corporation“ gemeldet.
Kategorie	Die vom Softwarekatalogteam festgelegte Kategorie der Anwendung
Plattform	Das Betriebssystem, für das die Anwendung vorgesehen ist. Beispiel: Windows.

4. Um einen Softwarekatalogartikel aus der Seite *Lizenz-Compliance* oder aus ausgewählten Berichten ein- oder auszuschließen, wählen Sie ihn in der Liste aus, klicken Sie auf **Aktion auswählen** und wählen Sie eine der folgenden Optionen aus:
   - **Aus Lizenz-Compliance ausschließen**
   - **In Lizenz-Compliance einschließen**
   - **Von Berichten ausschließen**
   - **In Berichte einschließen**
5. Klicken Sie auf den Anwendungsnamen, wenn Sie weitere Details anzeigen möchten.

   Siehe Details zu Anwendungen im Softwarekatalog anzeigen.

TIPP: Auf der Seite *Softwarekatalog* können Sie über die erweiterte Suche und benutzerdefinierte Ansichten basierend auf Kriterien für die erweiterte Suche nach Anwendungen suchen. Siehe Auf Seitenebene mit erweiterten Optionen suchen.

Liste der nicht katalogisierten Anwendungen anzeigen

In der Liste *Softwarekatalog* können Sie nicht katalogisierte Anwendungen anzeigen.

Nicht katalogisierte Anwendungen oder ausführbare Dateien, die sich im Inventar der Appliance befinden, aber nicht im Softwarekatalog aufgeführt sind. Sie können Anwendungen, die als nicht katalogisiert aufgeführt sind, in der Liste *Softwarekatalog* anzeigen. Allerdings können Sie die Erfassung der Nutzung für nicht katalogisierte Anwendungen nicht aktivieren, sie nicht als Nicht zulässig kennzeichnen und auch keine Lizenzinformationen über sie hinzufügen. Nicht katalogisierte Anwendungen müssen zum lokalen oder öffentlichen Softwarekatalog hinzugefügt werden, bevor ihre Nutzung erfasst werden kann und sie als Nicht zulässig gekennzeichnet oder mit Lizenzinformationen verknüpft werden können.

Die Informationen über nicht katalogisierte Anwendungen unterscheiden sich von Informationen über Anwendungen, deren Titel in der öffentlichen Version des Softwarekatalogs aufgelistet sind. Zum Beispiel stehen manche Informationen, die bei katalogisierten Anwendungen verfügbar sind, für nicht katalogisierte Anwendungen nicht zur Verfügung. Über nicht katalogisierte Anwendungen sind lediglich die Informationen verfügbar, die aus verwalteten Geräten erfasst wurden.

1. Rufen Sie die Liste *Softwarekatalog* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Inventar** und anschließend auf **Softwarekatalog**.
2. Klicken Sie auf die Registerkarte **Nicht katalogisiert**.

   Die Liste wird gefiltert, um nur die Anwendungen anzuzeigen, die als Erkannt klassifiziert wurden. Die Informationen über nicht katalogisierte Anwendungen umfassen Folgendes:

Element	Beschreibung
Name	Der Name und die Version der Softwareanwendung.
Installiert	Die Anzahl verwalteter Geräte, auf denen die Anwendung installiert ist
Dateiname	Der Name der ausführbaren Anwendungsdatei
Dateiversion	Die Versionsnummer der Anwendung
Herausgeber	Der Herausgeber der Anwendung.

3. Um einen Softwarekatalogartikel aus der Seite *Lizenz-Compliance* oder aus ausgewählten Berichten ein- oder auszuschließen, wählen Sie ihn in der Liste aus, klicken Sie auf **Aktion auswählen** und wählen Sie eine der folgenden Optionen aus:
   - **Aus Lizenz-Compliance ausschließen**
   - **In Lizenz-Compliance einschließen**
   - **Von Berichten ausschließen**
   - **In Berichte einschließen**
4. Klicken Sie auf den Anwendungsnamen, wenn Sie weitere Details anzeigen möchten.

   Siehe Details zu Anwendungen im Softwarekatalog anzeigen.

Liste der lokal katalogisierten Anwendungen anzeigen

Mit der erweiterten Suche können Sie die Seite *Softwarekatalog* sortieren, um Anwendungen anzuzeigen, die der lokalen Version des Softwarekatalogs hinzugefügt wurden.

Anwendungen, die nicht in der offiziellen Version des Softwarekatalogs enthalten sind, jedoch zur lokalen Version der Appliance hinzugefügt wurden, werden als lokal katalogisierte Anwendungen bezeichnet. Die Nutzung lokal katalogisierter Anwendungen kann erfasst werden und sie können als "Nicht zulässig" gekennzeichnet und mit Lizenz-Assets verknüpft werden.

1. Rufen Sie die Liste *Softwarekatalog* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Inventar** und anschließend auf **Softwarekatalog**.
2. Klicken Sie rechts oberhalb der Liste auf **Erweiterte Suche** und legen Sie die Suchkriterien für lokal katalogisierte Anwendungen fest:

   `Softwarekatalog: Nur lokaler Katalog | ist | Wahr`
3. Klicken Sie auf **Suchen**.

   Die Liste wird gefiltert, um nur die Anwendungen anzuzeigen, die als Lokal katalogisiert klassifiziert wurden. Die Informationen über lokal katalogisierte Anwendungen umfassen Folgendes:

Element	Beschreibung
Name	Der Name und die Version der Softwareanwendung. Wenn es sich bei der Anwendung um eine Suite handelt, wird der Name fett dargestellt. Beispiel: **Microsoft Office 2010 Professional**.
Typ	Die Klassifizierung der Anwendung im Softwarekatalog. Lokal katalogisierte Anwendungen werden als Erkannt klassifiziert.
Installiert	Die Anzahl verwalteter Geräte, auf denen die Anwendung installiert ist
Herausgeber	Der Herausgeber der Anwendung. Diese Information wird vereinheitlicht, um eine korrekte Berichterstellung zu gewährleisten. Zum Beispiel werden „Microsoft Corp.“ und „Microsoft Inc.“ als „Microsoft Corporation“ gemeldet.
Kategorie	Die vom Softwarekatalogteam festgelegte Kategorie der Anwendung
Plattform	Das Betriebssystem, für das die Anwendung vorgesehen ist. Beispiel: Windows.

4. Klicken Sie auf den Anwendungsnamen, wenn Sie weitere Details anzeigen möchten.

   Siehe Details zu Anwendungen im Softwarekatalog anzeigen.

Details zu Anwendungen im Softwarekatalog anzeigen

Sie können Details zu erkannten, nicht erkannten, nicht katalogisierten oder lokal katalogisierten Suites und Anwendungen anzeigen.

Zum Anzeigen von nicht katalogisierten Anwendungen muss die Datenaufbewahrung für nicht katalogisierte Anwendungen aktiviert sein. Sie können keine Details zu nicht katalogisierten Anwendungen anzeigen,

wenn die Datenaufbewahrung deaktiviert ist. Siehe Allgemeine Einstellungen auf Verwaltungs- oder organisationsspezifischer Ebene konfigurieren.

TIPP: Weitere Informationen zur Lizenz-Compliance finden Sie auf der Seite *Lizenz-Compliance*. Siehe Anzeigen von Informationen zur Lizenz-Compliance für Anwendungen im Softwarekatalog.

1. Rufen Sie die Liste *Softwarekatalog* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Inventar** und anschließend auf **Softwarekatalog**.
2. Klicken Sie auf den Namen einer Anwendung mit aktivierter Nutzungserfassung, um die Seite *Softwarekatalogdetails* anzuzeigen.

   Auf dieser Seite werden folgende Informationen angegeben:

Element	Beschreibung
Übersicht	
Nicht zulässig	Zeigt an, ob die Anwendung oder Suite als „Nicht zulässig“ gekennzeichnet ist. Das Kennzeichnen von Anwendungen als „Nicht zulässig“ verhindert, dass diese auf agentenverwalteten Geräten ausgeführt werden.
Erfasst	Zeigt an, ob die Erfassung für die Suite oder Anwendung aktiviert ist. Ist die Erfassung für die Anwendung aktiviert, werden die Nutzungsdaten von agentenverwalteten Geräten erfasst, bei denen auch die Erfassung aktiviert ist. Siehe Erfassung von Geräten und Anwendungen aktivieren und konfigurieren.
Installiert	Die Anzahl verwalteter Geräte, auf denen die Suite oder Anwendung installiert ist
Lizenzen	Die Zahl der Lizenz-Assets, die mit der Suite oder Anwendung verknüpft sind
Abgelaufene Lizenzen	Die Zahl der abgelaufenen Lizenz-Assets, die mit der Suite oder Anwendung verknüpft sind
Aus Lizenz-Compliance ausschließen	Gibt an, ob die Suite oder Anwendung auf der Seite *Lizenz-Compliance* angezeigt wird.
Von Berichten ausschließen	Gibt an, ob die Suite oder Anwendung in ausgewählten Berichten angezeigt wird.
Eigenschaften	
Herausgeber	Der Herausgeber der Suite oder Anwendung. Diese Information wird vereinheitlicht, um eine korrekte Berichterstellung zu gewährleisten. Zum Beispiel

Element	Beschreibung
	werden „Microsoft Corp.“ und „Microsoft Inc.“ als „Microsoft Corporation“ gemeldet.
Plattform	Das Betriebssystem, für das die Suite oder Anwendung vorgesehen ist. Beispiel: Windows.
Softwaretyp	Zeigt an, ob die Suite oder Anwendung eine Einzelanwendung ist, wie z. B. Microsoft Word, oder ein Anwendungspaket, wie z. B. Microsoft Office.
Herausgeber-Lizenztyp	Der vorgeschlagene Lizenztyp für die Suite oder Anwendung
Kategorie	Die vom Softwarekatalogteam festgelegte Kategorie der Suite oder Anwendung Für lokal katalogisierte Anwendungen wird die Kategorie bei der Übermittlung der Katalogisierungsanforderung festgelegt.
Anwendungs-ID oder Suite-ID	Ein Code, der die Suite bzw. die Anwendung identifiziert
Allgemeine Verfügbarkeit	Das Datum, zu dem die Suite oder Anwendung erstmals für Kunden veröffentlicht wurde
End of Life	Das Datum, zu dem der Support für die Suite oder die Anwendung beendet wurde
MSRP ($)	Der empfohlene Einzelhandelspreis des Herstellers für die Suite oder Anwendung
Erfassung aktiviert	Das Datum und die Uhrzeit, als die Erfassung für die Suite oder Anwendung aktiviert wurde
Installierte Versionen/Anwendungen	
Dateiname	Bei Anwendungen der Name der ausführbaren Datei
Produktname	Bei Suites der Name der Suite
Version	Die Versionsnummer, die der Suite oder Anwendung zugeordnet ist
Kategorie	Die vom Softwarekatalogteam festgelegte Kategorie der Suite oder Anwendung Für lokal katalogisierte Anwendungen wird die Kategorie bei der Übermittlung der Katalogisierungsanforderung festgelegt.
Sprache	Die Sprache, für die die Suite oder Anwendung entwickelt wurde, zum Beispiel Englisch. Anwendungen, die nicht für eine bestimmte Sprache

Element	Beschreibung
	entwickelt wurden, werden als „sprachneutral“ bezeichnet.
Installiert	Die Anzahl verwalteter Geräte, auf denen die Suite Anwendung installiert ist. Klicken Sie auf eine Zahl, um Geräteinformationen anzuzeigen.
App-V	Die Anwendungsvirtualisierung (Application Virtualization, App-V) von Microsoft, die Anwendungen verwaltet, ohne sie auf Geräten zu installieren.
Zugehörige Dateien	Eine oder mehrere Dateien, die mit der ausgewählten Version verknüpft sind und dem Softwarekatalog angehangen wurden. Soll eine Datei angehängt werden, klicken Sie auf + und wählen Sie den Speicherort der Datei aus. Sie können angehängte Dateien nach Bedarf bearbeiten oder löschen. • Um eine Datei mit einer Softwareversion zu verknüpfen, navigieren Sie mit einem Dateibrowser zu der Datei. • Verwenden Sie für größere Dateien Samba-Freigabe. • Liefern Sie eine Anmerkung zu der Datei mit. Beispiel: Script Host 5.8 - x86 oder Script Host 5.8 - x64 • Um die Datei in die Replikationsfreigabe zu kopieren, stellen Sie sicher, dass das Kontrollkästchen **Zugehörige Datei replizieren** aktiviert wurde.
Repliziert	Zeigt an, ob die Dateien in die Replikationsfreigabe kopiert wurden.
Anmerkungen	Eine Anmerkung über die angehängte Datei, sofern eine geliefert wurde.
Lizenzen	Nur verfügbar, wenn ein Lizenz-Asset für die Suite oder Anwendung hinzugefügt wurde
Name	Name der Lizenz, beispielsweise **Office Professional Bestellnr. 1234**. Dies ist der Name, über den Sie nach dem Asset suchen. Wenn Sie einer Anwendung mehrere Lizenzen zuweisen möchten, empfiehlt es sich, die Bestellnummer oder das Kaufdatum einzugeben.
Anzahl	Die Anzahl der Installationen oder Arbeitsplätze, die gemäß der Lizenz zulässig sind. Beispiel: 50.

Element	Beschreibung
Modus	Der Modus des Lizenz-Assets. Der Modus wird in der Lizenz-Compliance-Tabelle auf dem *Dashboard* der **Administratorkonsole** angezeigt. Werte, die auf der Seite *Asset-Details* ignoriert wurden, werden mit einer Nutzung von 100 Prozent angezeigt.
Schlüssel, Kosten pro Einheit und Ablaufdatum	Weitere Informationen zur Lizenz. Sie können die Standardinformationen ändern und bearbeiten, die für jeden Lizenz-Asset-Typ erfasst werden können.
Hersteller	Der Name des Hersteller-Assets, das Sie mit der Suite oder Anwendung verknüpfen möchten. Die Dropdown-Liste *Hersteller* ist leer, es sei denn, Sie haben ein Hersteller-Asset hinzugefügt. Um nach einem Hersteller zu suchen, tippen Sie seinen Namen in die Liste.
Bestellnummer	Die mit der Lizenz verknüpfte Bestellnummer.
Gekauft	Das Datum, an dem Sie die Lizenz erhalten haben. Klicken Sie in das Feld und wählen Sie dann im Kalender ein Datum aus.
Erfassung der Nutzung	
Zuletzt verwendet (vor x Tagen)	Die Anzahl verwalteter Geräte, auf denen die Suite oder Anwendung in den vergangenen 24 Stunden gestartet wurde
1 - 7	Die Anzahl verwalteter Geräte, auf denen die Suite oder Anwendung in den vergangenen 7 Tagen gestartet wurde
8 - 30	Die Anzahl verwalteter Geräte, auf denen die Suite oder Anwendung in den vergangenen 8 bis 30 Tagen gestartet wurde
31 - 90	Die Anzahl verwalteter Geräte, auf denen die Suite oder Anwendung in den vergangenen 31 bis 90 Tagen gestartet wurde
Nicht verwendet	Die Anzahl verwalteter Geräte, auf denen die Suite oder Anwendung in den vergangenen 90 Tagen nicht gestartet wurde.

Hinzufügen von Anwendungen zum Softwarekatalog

Quest überprüft regelmäßig sein umfassendes Data Warehouse und fügt bei Bedarf automatisch neue Anwendungen zum Softwarekatalog hinzu. Falls eine Anwendung nicht im Katalog angezeigt wird, können Sie eine Katalogisierungsanforderung an das Quest Katalogteam senden, damit die Anwendung aufgenommen wird.

Eine Katalogisierungsanforderung ist ein Formular, mit dem Sie anfordern können, dass eine nicht im Softwarekatalog enthaltene (nicht katalogisierte) Anwendung in den öffentlichen Softwarekatalog aufgenommen wird. Wenn Quest eine Katalogisierungsanforderung erhält, wird überprüft, ob die Anwendung in den öffentlichen Softwarekatalog aufgenommen werden soll. Außerdem werden Anwendungen, für die eine Katalogisierungsanforderung übermittelt wird, automatisch zur lokalen Version des Softwarekatalogs auf der Appliance hinzugefügt.

Alternativ können Sie organisationsinterne Anwendungen, die Sie nicht zum öffentlichen Softwarekatalog hinzufügen möchten, zur lokalen Version Ihres Softwarekatalogs hinzufügen. Siehe Katalogisierungsanforderungen senden.

Beim Senden von Katalogisierungsanforderungen werden die Anwendungen automatisch zum lokalen Softwarekatalog hinzugefügt.

Wenn Sie eine Katalogisierungsanforderung für eine Anwendung senden, wird die Anwendung automatisch sofort zur lokalen Version des Softwarekatalogs Ihrer Appliance hinzugefügt.

Die Anwendung wird damit zu einer lokal katalogisierten Anwendung, deren Nutzung erfasst werden kann, und Sie können sie als "Nicht zulässig" kennzeichnen und mit Lizenz-Assets verknüpfen.

Wenn die Organisationskomponente in Ihrer Appliance aktiviert ist, können Sie Katalogisierungsanforderungen von jeder Organisation aus senden. Der Titel wird dann sofort zu Ihrem lokalen Appliance-Softwarekatalog hinzugefügt. Er steht für alle Ihre Organisationen zur Verfügung.

WICHTIG: Katalogisierungsanforderungen können nur gesendet werden, wenn die Datenaufbewahrung für nicht katalogisierte Anwendungen für die Organisation aktiviert ist. Siehe Allgemeine Einstellungen auf Verwaltungs- oder organisationsspezifischer Ebene konfigurieren.

So werden lokal katalogisierte Anwendungen zu katalogisierten Anwendungen

Lokal katalogisierte Anwendungen werden zu katalogisierten Anwendungen, wenn sie der öffentlichen Version des Softwarekatalogs hinzugefügt werden.

Lokal katalogisierte Anwendungen werden in folgenden Fällen der öffentlichen Version des Softwarekatalogs hinzugefügt:

- Sie senden eine Katalogisierungsanforderung an das Quest KACE Katalogteam und die Anwendung wird in den Softwarekatalog aufgenommen.
- Ein anderer Kunde sendet eine Katalogisierungsanforderung an das Quest KACE Katalogteam und die Anwendung wird in den Softwarekatalog aufgenommen.
- Das Softwarekatalogteam fügt die Anwendung proaktiv zum Softwarekatalog hinzu.

Wenn der Softwarekatalog mit der Anwendung auf Ihrer Appliance aktualisiert wird, kann sich der Name der Anwendung ändern. Wenn die Eigenschaften der katalogisierten Anwendung, beispielsweise der Name der ausführbaren Datei, die Dateigröße und -version sowie andere Informationen, mit den Eigenschaften Ihrer lokalen

katalogisierten Anwendung übereinstimmen, wird die lokale Information durch die Kataloginformationen ersetzt. Falls der Name der Anwendung übereinstimmt, die Dateigröße oder eine andere Information aber stark abweicht, wird die neue Anwendung hinzugefügt, ohne die lokalen Kataloginformationen zu ersetzen.

Die Informationen im öffentlichen Softwarekatalog haben demnach stets Vorrang vor lokalen Kataloginformationen. Lokale Kataloganwendungen, die einer Anwendung im öffentlichen Softwarekatalog entsprechen, werden durch Einträge aus dem öffentlichen Softwarekatalog ersetzt. Dies wirkt sich jedoch nicht auf Informationen aus, die Sie für die Anwendung hinzugefügt haben, wie z. B. Lizenzinformationen, und es ändert auch nichts an den Einstellungen, etwa für das Erfassen der Nutzung oder die Kennzeichnung als Nicht zulässig.

Informationen zur Auflösung von benutzerdefinierten Namen beim Hinzufügen von lokal katalogisierten Anwendungen zum Softwarekatalog

Anwendungsnamen können standardisiert werden, wenn benutzerdefinierte Anwendungen dem öffentlichen Softwarekatalog hinzugefügt werden.

Wenn Sie benutzerdefinierte Namen für lokale Anwendungen verwenden, werden die benutzerdefinierten Namen durch die Standardnamen ersetzt, wenn die Anwendung zum öffentlichen Softwarekatalog hinzugefügt wird. Wenn beispielsweise eine Anwendung mit dem Namen **Updater** nicht im öffentlichen Katalog enthalten ist, können Sie einen lokalen Eintrag für die Anwendung erstellen. Sie können die Anwendung z. B. **MyUpdater** nennen und sie wird als **MyUpdater** im lokalen Katalog angezeigt. Wenn die Anwendung jedoch anschließend zum öffentlichen Katalog hinzugefügt wird und der offizielle Name **RealTime Updater** lautet, wird Ihre Benennung **MyUpdater** bei der Aktualisierung des öffentlichen Katalogs durch **RealTime Updater** ersetzt. Diese Namensänderung hat keine Auswirkungen auf Einstellungen für das Erfassen der Nutzung, Lizenzeinstellungen oder Verlaufseinstellungen. Wenn Sie jedoch benutzerdefinierte Ansichten oder Suchvorgänge basierend auf dem alten Anwendungsnamen eingerichtet haben, müssen Sie die Ansichten und Suchvorgänge aktualisieren, wenn Sie diese weiterhin verwenden möchten.

Katalogisierungsanforderungen senden

Sie können nach Bedarf Katalogisierungsanforderungen für nicht katalogisierte Anwendungen senden. Die Anforderungen werden kontinuierlich bearbeitet und vom Quest KACE Softwarekatalogteam nach eigenem Ermessen angenommen oder abgelehnt.

Die Datenaufbewahrung für nicht katalogisierte Software ist aktiviert. Sie können keine Katalogisierungsanforderungen senden, wenn die Datenaufbewahrung deaktiviert ist. Siehe Allgemeine Einstellungen auf Verwaltungs- oder organisationsspezifischer Ebene konfigurieren.

Manche Anwendungen, wie ausführbare Hilfsdateien für bereits katalogisierte Anwendungen, können nicht katalogisiert werden. Falls Sie mehrere Versionen einer nicht katalogisierten Anwendung haben, müssen Sie außerdem je Version eine separate Katalogisierungsanforderung senden. Sie können nicht mehrere ausführbare Dateien in einer einzigen Katalogisierungsanforderung zusammenfassen.

TIPP: Sie können dabei helfen, den Prozess für die Katalogisierungsanforderung zu verbessern, indem Sie Inventardaten Ihrer Appliance an Quest weitergeben. Das Softwarekatalogteam verwendet diese Daten, um neue Anwendungen zu identifizieren und Anwendungsnamen und -versionen zu standardisieren. Siehe Konfigurieren der Datenfreigabeeinstellungen.

1. Rufen Sie die Liste *Softwarekatalog* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.

b. Klicken Sie in der linken Navigationsleiste auf **Inventar** und anschließend auf **Softwarekatalog**.

2. Klicken Sie über der Liste auf der linken Seite auf die Registerkarte **Nicht katalogisiert**.
3. Klicken Sie auf einen Anwendungsnamen, um die *Softwaredetailseite* anzuzeigen.
4. Klicken Sie auf **Zu Katalog hinzufügen**, um das Formular *Zu Katalog hinzufügen* anzuzeigen.
5. Geben Sie die folgenden Informationen an:

Option	Beschreibung
Softwaretitel	Der Name, der zur Identifizierung der Anwendung verwendet werden soll. Siehe Informationen zur Auflösung von benutzerdefinierten Namen beim Hinzufügen von lokal katalogisierten Anwendungen zum Softwarekatalog.
Kategorie	Die Kategorie der Anwendung Kategorien können nützlich sein, um Anwendungen zu ordnen und zu verwalten.

6. Wählen Sie Freigabeoptionen aus und geben Sie Kontaktinformationen an:

Option	Beschreibung
Freigabe	Die Katalogisierungsoptionen: • **Add software title to this appliance and share with the Quest KACE catalog (Softwaretitel zu dieser Appliance hinzufügen und an Katalog von Quest KACE weitergeben)**: Anforderung an Quest senden und den Titel zur lokalen Version des Softwarekatalogs hinzufügen. • **Add software title to this appliance only (Softwaretitel nur zu dieser Appliance hinzufügen)**: Titel zur lokalen Version des Softwarekatalogs hinzufügen, aber nicht an den Quest KACE Softwarekatalog senden.
Kontaktinformationen	Geben Sie Ihre Kontaktinformationen ein. Das Softwarekatalogteam verwendet diese Informationen, um Sie bei Fragen zu der Anforderung zu kontaktieren.

7. Klicken Sie auf **Speichern**.

Die Katalogisierungsanforderung wird an Quest gesendet. Die Schaltfläche **Aus lokalem Softwarekatalog entfernen** wird auf der Seite *Detail zum Softwarekatalog* angezeigt. Wenn Katalogisierungsanforderungen zum öffentlichen Softwarekatalog hinzugefügt werden und der Katalog auf der Appliance aktualisiert wird, wird die Schaltfläche **Aus lokalem Softwarekatalog entfernen** auf der Seite *Softwarekatalogdetails* nicht mehr angezeigt. Die Nachverfolgung von Katalogisierungsanforderungen ist derzeit nicht verfügbar.

HINWEIS: Informationen über Titel, die zum öffentlichen Katalog hinzugefügt werden, können sich von den ursprünglich gesendeten Informationen unterscheiden. Dies liegt daran, dass die Titel bei der Aufnahme in den öffentlichen Katalog standardisiert werden.

Katalogisierungsanforderungen stornieren und lokale Katalogisierungen entfernen

Unter bestimmten Voraussetzungen können Sie Katalogisierungsanforderungen stornieren und Anwendungen aus dem lokalen Softwarekatalog entfernen.

- Den Anwendungen sind keine Lizenz-Assets zugeordnet. Sie müssen Anwendungen von Lizenz-Assets entfernen, bevor Sie Anwendungen aus dem Katalog entfernen können.
- Die Anwendungen wurden noch nicht vom Softwarekatalogteam angenommen und noch nicht zum öffentlichen Katalog hinzugefügt. Wenn Sie zum Beispiel eine Anforderung senden und sie am selben Tag stornieren, ist die Wahrscheinlichkeit gering, dass das Softwarekatalogteam sie bereits angenommen hat, sodass die Anforderung ggf. noch storniert werden kann. Wenn Sie jedoch eine Anforderung senden und sie erst nach ein paar Tagen oder Wochen stornieren, ist es möglich, dass das Softwarekatalogteam die Anforderung bereits angenommen und sie in den öffentlichen Softwarekatalog aufgenommen hat. In diesem Fall kann die Katalogisierungsanforderung nicht mehr storniert werden.

Sie können nur lokal katalogisierte Anwendungen entfernen. Katalogisierte Anwendungen können nicht aus dem Katalog entfernt werden.

1. Rufen Sie die Liste *Softwarekatalog* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Inventar** und anschließend auf **Softwarekatalog**.
2. Klicken Sie auf einen Anwendungsnamen, um die *Softwarekatalog-Detailseite* anzuzeigen.
3. Wenn die Anwendung einem Lizenz-Asset zugeordnet ist:
   a. Klicken Sie auf der Seite *Detail zum Softwarekatalog* im Abschnitt *Lizenzen* auf den Namen des Lizenz-Assets, um die Seite *Lizenz-Asset-Details* anzuzeigen.
   b. Wählen Sie im Feld *Gültig für katalogisierte Software* den Namen der Anwendung und klicken Sie anschließend auf **Entfernen**.
   c. Klicken Sie auf **Speichern**.
4. Kehren Sie zur *Softwarekatalog-Detailseite* zurück.
5. Klicken Sie auf **Aus lokalem Softwarekatalog entfernen**.

Der Titel wird aus der lokalen Version des Softwarekatalogs entfernt und die Schaltfläche **Zu Katalog hinzufügen** wird auf der Seite *Softwarekatalogdetails* angezeigt.

Verwalten von Lizenz-Assets für Anwendungen im Softwarekatalog

Lizenz-Assets können entweder mit Elementen im Softwarekatalog oder mit Elementen auf der Seite *Software* verknüpft werden. Sie können jedoch nicht gleichzeitig mit Elementen des Softwarekatalogs und der Seite *Software* verknüpft werden.

Wenn Sie bereits über Lizenz-Assets verfügen, können Sie diese von Elementen auf der Seite *Software* zu Elementen auf der Seite *Softwarekatalog* migrieren. Dies ermöglicht es Ihnen, von den Funktionen des Softwarekatalogs zu profitieren, einschließlich der Lizenz-Compliance. Siehe Lizenz-Assets zu Anwendungen im Softwarekatalog migrieren.

Hinzufügen von Lizenz-Assets für das Softwarekataloginventar

Sie können Lizenz-Assets für Anwendungen im Softwarekataloginventar hinzufügen. Durch das Hinzufügen von Lizenz-Assets können Sie Lizenz-Compliance-Informationen in der Liste *Lizenz-Compliance* und im Dashboard-Widget *Lizenz-Compliance* anzeigen.

Anwendungen im Softwarekatalog müssen als *Erkannt*, *Nicht erkannt* oder *Lokal katalogisiert* klassifiziert werden. Lizenz-Assets für als *Nicht katalogisiert* klassifizierte Anwendungen können nicht hinzugefügt werden.

Wenn Sie Lizenz-Assets mit Anwendungen verknüpfen, können Sie auch auf der Seite *Softwarekatalogdetails* Lizenzinformationen anzeigen. Wenn auf der Appliance die Organisationskomponente aktiviert ist, können Sie die Lizenzinformationen für jede Organisation separat verwalten.

TIPP: Um Lizenz-Assets für mehrere Anwendungen auf einmal hinzuzufügen, können Sie die Informationen aus Tabellen oder CSV-Dateien importieren. Siehe Beispiel: Lizenzdaten aus vorbereiteten Tabellen importieren.

1. Rufen Sie die Liste *Softwarekatalog* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Inventar** und anschließend auf **Softwarekatalog**.
2. Klicken Sie auf den Namen einer Anwendung, um die *Softwarekatalog-Detailseite* anzuzeigen.
3. Klicken Sie am unteren Seitenrand auf **Neue Lizenz hinzufügen**, um die *Lizenz-Asset-Detailseite* anzuzeigen.
4. Geben Sie auf der Seite *Lizenz-Asset-Details* auf der Registerkarte *Allgemein* die folgenden Informationen an:

Option	Beschreibung
Untertyp	Der mit der Lizenz zu verknüpfende Asset-Untertyp. Siehe Informationen zu Asset-Untertypen, benutzerdefinierten Feldern und Gerätedetail-Voreinstellungen.
Asset-Status	Der Lizenzstatus, falls zutreffend. Sie können einen Standard-Asset-Status oder einen benutzerdefinierten festlegen (falls vorhanden).

Option	Beschreibung
	Eine Standardinstallation des Appliance umfasst die folgenden Asset-Status: • **Aktiv**: Alle Assets, die bereitgestellt, aktiv oder in Gebrauch sind. • **Entsorgt**: Ein Asset, das nicht mehr verfügbar ist. • **Abgelaufen** Ein Software-Lizenz oder ein Vertrags-Asset, das abgelaufen ist. • **Auf Lager**: Ein vor kurzem empfangenes Asset. • **Fehlt** Alle Assets, die nicht gefunden werden können. • **Reparieren** Ein Asset, das repariert wird. • **Reserviert** Ein Asset, das für eine bestimmte Person oder einen Zweck reserviert ist. • **außer Kraft gesetzt**: Alle Assets, die das Ende ihrer Lebensdauer erreicht haben oder nicht mehr in Gebrauch sind. • **Gestohlen**: Ein Asset, das als gestohlen gemeldet wurde. Weitere Informationen hierzu finden Sie unter Asset-Lebenszyklus-Einstellungen anzeigen und konfigurieren.
Standort	Der Name des Standorts, in dem sich die Organisation befindet. Siehe Standorte verwalten.
Name	Name der Lizenz, beispielsweise **Office Professional Bestellnr. 1234**. Dies ist der Name, über den Sie nach dem Asset suchen. Wenn Sie mehrere Lizenzen mit einer Anwendung verknüpfen möchten, geben Sie die Bestellnummer oder das Kaufdatum in die nachstehenden Felder ein, um die Lizenzen voneinander zu unterscheiden.
Lizenzanzahl	Die Anzahl der Installationen oder Arbeitsplätze, die gemäß der Lizenz zulässig sind. Beispiel: 50.
Gültig für katalogisierte Software	Anwendungen im Softwarekataloginventar, für das die Lizenz gilt. Gegebenenfalls können Sie Lizenz-Assets mehreren Anwendungen im Softwarekatalog zuordnen. Es ist jedoch nicht erforderlich, Lizenz-Assets mit mehreren Versionen der gleichen Anwendung zu verknüpfen, da die Appliance dies automatisch durchführt, um Upgrades und Downgrades zu unterstützen. Sie können einfach beim Hinzufügen der Lizenzinformationen die aktuelle Version dem Lizenz-Asset zuordnen. Wenn Sie Anwendungen von anderen Herausgebern, z. B. von Microsoft Office oder Adobe Acrobat, dem gleichen Lizenz-Asset

Option	Beschreibung
	zuweisen, wird jeder Anwendung die im Lizenz-Asset angegebene Gesamtzahl der Lizenzplätze zugewiesen. Wenn das Lizenz-Asset z. B. über 100 Lizenzplätze verfügt, werden sowohl Microsoft Office als auch Adobe Acrobat 100 Lizenzplätze zugewiesen.
Gültig für Software	Lassen Sie dieses Feld leer. Eine Lizenz kann jedoch nicht gleichzeitig mit im Inventar der Seite *Softwarekatalog* und der Seite *Software* enthaltenen Anwendungen verknüpft werden. Weitere Informationen zum Erstellen von Lizenz-Assets finden Sie unter Hinzufügen von Lizenz-Assets für das Inventar der Seite "Software".
Lizenzmodus	Der Modus des Lizenz-Assets. Für Anwendungen, die Lizenzen erfordern, und zum Anzeigen von Lizenznutzungsinformationen auf der Seite *Lizenz-Compliance* wählen Sie entweder *Unternehmen* oder *Lizenz für Einheit* aus. **HINWEIS:** Die meisten Modi, einschließlich *Nicht angegeben*, *Client-Lizenz*, *Abonnement*, *Shareware*, *Freeware*, *OpenSource*, *Keine Lizenzierung* und *Standortlizenz*, werden nicht für die Lizenz-Compliance verwendet. Der Lizenzmodus wird in den folgenden Abschnitten der **Administratorkonsole** verwendet: • Liste *Lizenz-Compliance*. Siehe Anzeigen von Informationen zur Lizenz-Compliance für Anwendungen im Softwarekatalog. • In der auf dem *Dashboard* angezeigten Lizenz-Compliance-Tabelle. Werte, die auf der Seite *Asset-Details* ignoriert wurden, werden mit einer Nutzung von 100 Prozent angezeigt. Siehe Informationen zu Dashboard-Widgets.

5. Klicken Sie auf **Weiter**.
6. Geben Sie auf der Seite *Lizenz-Asset-Details* auf der Registerkarte *Einkauf* die folgenden Informationen an:

Option	Beschreibung
Vertrag	Das mit der Lizenz verbundene Vertrags-Asset.
Gültig für katalogisierte Software	Anwendungen im Softwarekataloginventar, für das die Lizenz gilt. Gegebenenfalls können Sie Lizenz-Assets mehreren Anwendungen im Softwarekatalog zuordnen. Es ist jedoch nicht erforderlich, Lizenz-Assets mit mehreren Versionen der gleichen Anwendung zu verknüpfen, da die Appliance dies automatisch durchführt, um Upgrades und Downgrades zu unterstützen. Sie können einfach

Option	Beschreibung
	beim Hinzufügen der Lizenzinformationen die aktuelle Version dem Lizenz-Asset zuordnen. Wenn Sie Anwendungen von anderen Herausgebern, z. B. von Microsoft Office oder Adobe Acrobat, dem gleichen Lizenz-Asset zuweisen, wird jeder Anwendung die im Lizenz-Asset angegebene Gesamtzahl der Lizenzplätze zugewiesen. Wenn das Lizenz-Asset z. B. über 100 Lizenzplätze verfügt, werden sowohl Microsoft Office als auch Adobe Acrobat 100 Lizenzplätze zugewiesen.
Produktschlüssel	Den mit der Lizenz verbundenen Produktschlüssel. Sie können die Standardinformationen ändern und bearbeiten, die für jeden Lizenz-Asset-Typ erfasst werden können.
Kosten pro Einheit	Die mit der Lizenz verbundenen Einheitskosten. Sie können die Standardinformationen ändern und bearbeiten, die für jeden Lizenz-Asset-Typ erfasst werden können.
Hersteller	Der Name des Hersteller-Assets, das Sie mit der Anwendung verknüpfen möchten. Die Dropdown-Liste *Hersteller* ist leer, wenn Sie kein Hersteller-Asset hinzugefügt haben. Um nach einem Hersteller zu suchen, tippen Sie seinen Namen in die Liste. **HINWEIS:** Die Zuweisung mehrerer Hersteller zu einem einzigen Softwarelizenz-Asset wird nicht empfohlen, da dies zu fehlerhaften Lizenz-Compliance-Informationen führen kann.
Bestellnummer	Die mit der Lizenz verknüpfte Bestellnummer.
Kaufdatum	Das Datum des Kaufs. Klicken Sie in das Feld und wählen Sie dann im Kalender ein Datum aus.
Kauf	Wählen Sie einen oder mehrere mit dieser Lizenz verknüpfte Einkaufsdatensätze aus. Siehe Kaufdatensätze verwalten.

7. Klicken Sie auf **Weiter**.
8. Geben Sie auf der Seite *Lizenz-Asset-Details* auf der Registerkarte *Wartung* die folgenden Informationen an:

Option	Beschreibung
Schließt Upgrade-Rechte ein	Gibt an, ob die Lizenz Upgrade-Rechte einschließt. Upgrade-Rechte beziehen sich auf die Möglichkeit, auf eine neuere Version der lizenzierten Software aufzurüsten, wenn eine solche Version verfügbar wird. Weitere Informationen hierzu finden Sie unter

Option	Beschreibung
	Informationen zu Lizenz-Upgrades. Wählen Sie eine der folgenden Optionen aus: • **Ja**: Upgrade-Rechte werden durch Vergleich der bestehenden Lizenzen für die ausgewählte Software und die Anzahl verfügbarer Lizenzen für neuere Versionen der gleichen Software berechnet. • **Ja - aus Liste auswählen**: Wählen Sie eine oder mehrere Softwareversionen, für die Sie Upgrade-Rechte gewähren möchten. Klicken Sie unter *Software-Liste aktualisieren* auf **Katalogisierte Software zum Hinzufügen auswählen**. Die daraufhin angezeigte Liste wird mit höheren Versionen der ausgewählten Software ausgefüllt, auf die die Lizenz aktualisiert werden kann. Wenn Sie auf einen Eintrag in der Liste klicken, erscheint Ihre Auswahl im Feld *Liste der Upgrade-Software*. Sie können nach Bedarf eine oder mehrere Versionen hinzufügen. Um ein Element aus der Liste zu löschen, wählen Sie es im Feld *Liste der Upgrade-Software* aus und klicken Sie auf **Entfernen**. • **Nein**: Wenn Sie keine Upgrade-Rechte für die ausgewählte Software gewähren möchten, aktivieren Sie diese Option.
Service inklusive	Gibt an, ob die Lizenz die Benutzer zum Upgrade der installierten Version der Anwendung berechtigt. Siehe Informationen zur Lizenz-Compliance für Anwendungen im Softwarekatalog.
Ablaufdatum	Das Ablaufdatum des Wartungszeitraums, wenn die Lizenz Wartung beinhaltet. Die Lizenz-Compliance-Funktion der Appliance nutzt Softwarekataloginformationen, z. B. das Herausgabedatum von Anwendungen. Wenn während des Wartungszeitraums neue Anwendungsversionen herausgegeben werden, sind diese automatisch durch dieses Lizenz-Asset abgedeckt.
Schließt Downgrade-Rechte ein	Gibt an, ob die Lizenz Downgrade-Rechte einschließt. Downgrade-Rechte beziehen sich auf die Möglichkeit, Lizenzen für neuere Softwareversionen auf ältere Versionen der gleichen Software anzuwenden. Weitere Informationen hierzu finden Sie unter Informationen zu Lizenz-Downgrades. Wählen Sie eine der folgenden Optionen aus: • **Ja**: Downgrade-Rechte werden durch Vergleich der bestehenden Lizenzen für die ausgewählte Software und die Anzahl

Option	Beschreibung
	verfügbarer Lizenzen für ältere Versionen der gleichen Software berechnet. • **Ja - aus Liste auswählen**: Wählen Sie eine oder mehrere Softwareversionen, für die Sie Downgrade-Rechte gewähren möchten. Klicken Sie unter *Software-Liste zurückstufen* auf **Katalogisierte Software zum Hinzufügen auswählen**. Die daraufhin angezeigte Liste wird mit niedrigeren Versionen der ausgewählten Software ausgefüllt, auf die die Lizenz herabgestuft werden kann. Wenn Sie auf einen Eintrag in der Liste klicken, erscheint Ihre Auswahl im Feld *Liste der Downgrade-Software*. Sie können nach Bedarf eine oder mehrere Versionen hinzufügen. Um ein Element aus der Liste zu löschen, wählen Sie es im Feld *Liste der Downgrade-Software* aus und klicken Sie auf **Entfernen**. • **Nein**: Wenn Sie keine Downgrade-Rechte für die ausgewählte Software gewähren möchten, aktivieren Sie diese Option.

9. Klicken Sie auf **Weiter**.
10. Geben Sie auf der Seite *Lizenz-Asset-Details* auf der Registerkarte *Zugehörig* die folgenden Informationen an:

Option	Beschreibung
Abteilung	Die Unternehmensgruppe oder Abteilung, der diese Anwendung gehört.
Kostenstelle	Die mit der Abteilung, der diese Anwendung gehört, verknüpfte Kostenstelle.
Genehmigt für Gerät	Die Geräte, die die Lizenz verwenden dürfen. Diese Information wird für Lizenz-Compliance-Berichte verwendet. Wenn die Anwendung zum Beispiel auf Geräten installiert ist, die nicht in der Liste genehmigter Geräte enthalten sind, werden diese Geräte im Bericht *Nicht genehmigte Softwareinstallation* aufgeführt. Die Lizenz-Compliance wird von der Appliance jedoch nicht erzwungen. Sie verhindert beispielsweise nicht, dass Anwendungen auf verwalteten Geräten installiert werden, wenn eine Lizenz abgelaufen ist oder anderweitig gegen die Compliance-Vorgaben verstoßen wird.
Barcodes	Fügen Sie bei Bedarf Barcodes hinzu, die mit dieser Lizenz verknüpft sind, bzw. bearbeiten Sie diese.

Option	Beschreibung
	Weitere Informationen hierzu finden Sie unter Barcodes zu Assets hinzufügen.

11. Klicken Sie auf **Weiter**.
12. Geben Sie auf der Seite *Lizenz-Asset-Details* auf der Registerkarte *Benutzerdefiniert* zusätzliche benutzerdefinierte Daten an. Sie können den Lizenz-Asset-Typ ändern und so viele weitere Felder aufnehmen, wie für Ihre geschäftlichen Ziele notwendig sind. Weitere Informationen hierzu finden Sie unter Asset-Typen hinzufügen oder anpassen.
13. Klicken Sie auf **Weiter**.
14. Geben Sie auf der Seite *Lizenz-Asset-Details* auf der Registerkarte *Hinweise* die folgenden Informationen an:

Option	Beschreibung
Anmerkungen	Geben Sie nach Bedarf beliebige weitere Informationen ein.
Lizenztext	Ergänzende Informationen zur Lizenz, z. B. eine Lizenznummer.

15. Klicken Sie auf **Speichern**.

    Das neue Lizenz-Asset wird auf der Seite *Lizenzen* angezeigt. Der Wert von *Lizenzanzahl* ändert sich erst, wenn Sie das Asset aktualisieren. Dagegen ändert sich der Wert in der Spalte *Installiert*, sobald sich verwaltete Geräte, auf denen die Software installiert ist, bei der Appliance anmelden. Auf diese Weise können Sie die Anzahl der erworbenen und installierten Lizenzen verfolgen.

Führen Sie die folgenden optionalen Aufgaben aus:

- Aktivieren Sie die Nutzungserfassung für das Softwarekataloginventar. Wenn die Nutzungserfassung aktiviert ist, wird auf der Seite *Lizenz-Compliance* angezeigt, ob in den vergangenen 90 Tagen Anwendungen verwendet bzw. nicht verwendet worden sind. Siehe Informationen zur Erfassung der Softwarenutzung.
- Stellen Sie die Warnungsschwellenwerte für die Lizenznutzung ein. Diese Schwellenwerte werden vom Dashboard-Widget "Lizenz-Compliance" zur Erkennung von Lizenz-Compliance-Problemen genutzt.

Lizenz-Assets zu Anwendungen im Softwarekatalog migrieren

Wenn Sie bereits über Lizenz-Assets verfügen, können Sie diese migrieren oder von Anwendungen auf der Seite *Software* auf Anwendungen auf der Seite *Softwarekatalog* übertragen. Dies ermöglicht es Ihnen, von den erweiterten Funktionen des Softwarekatalogs zu profitieren.

Ändern Sie zum Migrieren von Lizenzen deren Zuweisung von einer Anwendung auf der Liste *Software* zu einer Anwendung auf der Liste *Softwarekatalog*.

Lizenz-Assets können entweder mit Anwendungen im *Softwarekatalog* oder mit Anwendungen auf der Liste *Software* verknüpft werden. Sie können jedoch nicht gleichzeitig mit beiden Arten von Anwendungen verknüpft werden.

1. Rufen Sie die Liste *Assets* auf:
    a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.

   b. Klicken Sie in der linken Navigationsleiste auf **Asset Management** und anschließend auf **Assets**.
2. Klicken Sie auf den Namen einer Lizenz, die einer Anwendung auf der Liste *Software* zugeordnet ist, um die Seite *Lizenz-Asset-Detail* anzuzeigen.

   Im oberen Bereich wird der Hinweis angezeigt, dass die Lizenz übertragen werden muss, damit sie auf ein Softwarekatalogelement angewendet werden kann.
3. Klicken Sie im oberen Bereich auf **Jetzt übertragen**.
4. Wählen Sie im Abschnitt *Gültig für katalogisierte Software* die Anwendung, die Sie mit der Lizenz verknüpfen möchten.
5. Klicken Sie unten auf der Seite auf **Speichern**.

Verknüpfen verwalteter Installationen mit katalogisierter Software

Sie können eine oder mehrere verwaltete Installationen zu Softwarekatalogelementen hinzufügen, um die Bereitstellung dieser Anwendungen auf Endbenutzergeräten zu verwalten.

1. Rufen Sie die Liste *Softwarekatalog* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Inventar** und anschließend auf **Softwarekatalog**.
2. Klicken Sie auf den Namen einer Anwendung, um die *Softwarekatalog-Detailseite* anzuzeigen.
3. Klicken Sie am unteren Seitenrand auf **Neue verwaltete Installation hinzufügen**, um die *Verwaltete Installationen-Detailseite* anzuzeigen.
4. Erstellen Sie ggf. eine neue verwaltete Installation. Weitere Informationen finden Sie nach Bedarf in den folgenden Abschnitten:
   - Verwaltete Installationen für Windows Geräte erstellen
   - Verwaltete Installationen für Mac OS X Geräte erstellen
   - Verwaltete Installationen für RPM-Dateien erstellen

Verwenden der Erfassung der Softwarenutzung

Mit der KACE Appliance können Sie Informationen zur Erfassung der Softwarenutzung verwalten.

Informationen zur Erfassung der Softwarenutzung

Durch die Erfassung der Softwarenutzung können Sie Informationen dazu sammeln, wie Anwendungen auf den verwalteten Windows und Mac Geräten installiert und verwendet werden.

Informationen werden auch für Windows Store-Anwendungen wie Bing Travel erfasst. Für Anwendungen, die auf anderen Betriebssystemen wie beispielsweise Linux installiert sind, ist die Erfassung der Nutzung nicht möglich. Im Softwarekatalog kann die Erfassung für erkannte und nicht erkannte Anwendungen sowie für lokal katalogisierte Anwendungen aktiviert werden. Die Erfassung der Nutzung ist nicht möglich, wenn es sich um Betriebssystemsoftware handelt, die Anwendungen auf nicht unterstützten Betriebssystemen wie Linux installiert sind oder die Anwendungen im Softwarekatalog als Nicht katalogisiert aufgeführt werden.

Informationen zur klassischen Erfassung

Die klassische Erfassung ist ein Erfassungssystem, das auf der Appliance vor der Version 5.5 verfügbar war. Wenn Sie ein Upgrade von Version 5.4 oder niedriger auf Version 5.5 durchgeführt und die Erfassung der Nutzung vor dem Upgrade aktiviert haben, können Sie auch in der Version 5.5 auf die klassische Erfassung zugreifen.

In der Version 6.0 wurde die klassische Erfassung jedoch durch das Softwarekatalog-Erfassungssystem ersetzt, das ausführlichere Informationen bietet. Ab Version 6.0 steht die klassische Erfassung nicht mehr zur Verfügung.

Informationen zu Erfassungsinformationen

Wenn Sie die Erfassung für Anwendungen aktivieren, werden Informationen für Geräte erfasst, auf denen die Anwendungen installiert sind – vorausgesetzt, die Erfassung wurde auch für die Geräte aktiviert.

Folgende Informationen werden erfasst:

- Versionsinformationen
- Informationen zu Suites
- Anzahl der Installationen
- Nutzungs- und Ausführungsinformationen

Siehe Softwarekatalog-Erfassungsinformationen anzeigen.

Darüber hinaus können Sie die Häufigkeit der Nutzungserfassung sowie die Aufbewahrungsdauer der entsprechenden Daten konfigurieren. Siehe Optionen für die Erfassung von Anwendungen im Softwarekatalog konfigurieren.

Informationen zu den Skripten, mit denen Erfassungsinformationen gesammelt werden

Der Dienst für die Erfassung der Softwarenutzung wird mit dem KACE Agent gebündelt und auf verwalteten Geräten installiert. Wenn die Erfassung aktiviert ist, werden Skripte zum Sammeln von Erfassungsinformationen ausgeführt.

Diese Erfassungsskripte variieren je nach Betriebssystem:

- **Windows**: Auf Windows-Geräten ist die Erfassung ein ereignisgesteuerter Prozess, der Windows Assets mit WMI-Ereignissen (Windows Verwaltungsinstrumentation) überwacht.
- **Mac**: Auf Mac Geräten identifiziert das Erfassungsskript Prozessereignisse asynchron mit NSWorkspace Notification Center.

Die Informationen, einschließlich des Namens der Anwendungsdatei, der Version und der Dateigröße, werden mit den Informationen im Softwarekatalog verglichen, um die Anwendung zu identifizieren.

Wie Suites erfasst werden

Wenn die Erfassung für eine Suite, beispielsweise Microsoft Office, aktiviert ist, ermittelt das System, ob Anwendungen der Suite auf verwalteten Geräten ausgeführt werden, auf denen die Erfassung aktiviert ist. Nutzungsinformationen werden für die gesamte Suite sowie für jede einzelne Anwendung gemeldet.

Verwaltete Geräte, auf denen eine Anwendung der Suite installiert ist (ermittelt anhand eines Eintrags unter *Software*), werden als Geräte gezählt, auf denen die Suite installiert ist. Auf Geräten muss nicht jede Anwendung der Suite installiert sein, damit sie als Geräte zählen, auf denen die Suite installiert ist.

Wenn die Erfassung für eine Suite aktiviert wurde, ist sie gleichzeitig für die einzelnen Anwendungen der Suite aktiv. Sie können die Erfassung nicht für einzelne Anwendungen in Suites aktivieren bzw. deaktivieren.

Erfassung von Geräten und Anwendungen aktivieren und konfigurieren

Wenn Sie Erfassungsinformationen für Anwendungen im Softwarekatalog abrufen möchten, müssen Sie zunächst die Erfassung für Anwendungen und für die Geräte aktivieren, auf denen die entsprechenden Anwendungen installiert sind.

Zu erfassende Geräte und Anwendungen auswählen

Bei aktivierter Erfassung von Geräten können entsprechende Informationen gesammelt werden, wobei die Server- oder Netzwerklast nicht nennenswert ansteigt.

Aus diesem Grund empfiehlt Quest, die Erfassung für alle verwalteten Windows und Mac Geräte zu aktivieren. Sie sollten die Anwendungen, die Sie erfassen möchten, jedoch überlegt auswählen. Durch die Speicherung von Erfassungsinformationen für eine Vielzahl von Anwendungen kann der Speicherplatzbedarf erheblich ansteigen und die Systemleistung beeinträchtigen.

Erfassung auf Geräten aktivieren

Wenn Sie die Erfassung der Softwarenutzung auf verwalteten Geräten aktivieren möchten, müssen Sie den Geräten ein für die Erfassung aktiviertes Label zuweisen.

Führen Sie eine der folgenden Aktionen aus, um Geräten ein für die Erfassung aktiviertes Label zuzuweisen:

- Wenden Sie das integrierte Label *MeteredDevices* auf Ihre Geräte an. Bei diesem Label ist die Erfassung der Nutzung aktiviert. Siehe Einrichten und Verwenden von Labels für die Verwaltung von Elementgruppen.
- Erstellen Sie ein manuelles Label für die Erfassung und weisen Sie es Geräten zu. Siehe Erfassung auf Geräten mit manuellen Labels aktivieren.
- Erstellen Sie ein Smart Label für die Erfassung (wird Geräten automatisch zugewiesen). Siehe Erfassung auf Geräten mit Smart Labels deaktivieren.

TIPP: Zur Aktivierung der Erfassung auf verwalteten Geräten können Sie manuelle Label oder Smart Label verwenden, die Verwendung von Labels ist aber in jedem Fall erforderlich. Die Erfassung kann nur auf Ebene der Labels aktiviert werden, nicht in den Einstellungen der einzelnen Geräte.

Erfassung auf Geräten mit manuellen Labels aktivieren

Sie können die Erfassung für ein manuelles Label aktivieren und dieses dann Geräten zuweisen, um die Erfassung auf Geräten zu aktivieren.

1. Rufen Sie die Liste *Smart Labels* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste im Abschnitt **Startseite** auf **Label-Verwaltung**.
   c. Klicken Sie im Bereich für die Label-Verwaltung auf **Labels**.
2. Wählen Sie **Aktion auswählen > Neues manuelles Label**, um die *Label-Detailseite* anzuzeigen.

   TIPP: Vermeiden Sie in Labelnamen die Verwendung des umgekehrten Schrägstrichs (\). Wenn Sie einen umgekehrten Schrägstrich in einem Labelnamen verwenden müssen, fügen Sie einen zweiten umgekehrten Schrägstrich hinzu (\\), damit er nicht als Befehl interpretiert wird.
3. Geben Sie die folgenden Informationen an:

Option	Beschreibung
Name	Der Name des Labels.
Beschreibung	Geben Sie nach Bedarf beliebige weitere Informationen ein.
Alternativer Speicherort	(Optional) Die alternative Download-Quelle für verwaltete Installationen, Dateisynchronisierungen und andere Bereitstellungen, die auf den diesem Label zugeordneten Elementen ausgeführt werden. Die Quelle, die Sie angeben, überschreibt die Zeichenfolge KACE_ALT_LOCATION. VORSICHT: **Weisen Sie Geräten nicht zwei Labels zu, die beide einen Wert in diesem Feld festlegen.**
Pfad	Geben Sie bei Angabe einer alternativen Downloadquelle den Pfad zu dieser Quelle an.
Anmeldung **Kennwort**	Wenn Sie eine alternative Download-Quelle angeben, geben Sie den Benutzernamen und das Kennwort für die Quelle an.
Labelnutzung beschränken auf	Der Typ des Labels. Aktivieren Sie das Kontrollkästchen *Geräteinventar*, um ein Label zu erstellen, das die Erfassung aktiviert. Sie können nach Bedarf zusätzliche Labeltypen auswählen, aber die Erfassung kann nur aktiviert werden, wenn der Labeltyp *Geräte* ausgewählt ist.
Erfassung der Softwarenutzung	Aktiviert die Nutzungserfassung auf Geräten, die dieses Label aufweisen. Es kann damit nur die Nutzungserfassung von Geräten aktiviert werden. Um auch die Nutzung von Software zu erfassen, müssen Sie auch die Nutzungserfassung für einzelne Anwendungen aktivieren.
Anwendungssteuerung zulassen	Aktivieren Sie die Anwendungssteuerung auf Geräten. Software, die als "Nicht zulässig" gekennzeichnet wurde, kann nicht auf den Geräten ausgeführt werden, auf die das Label angewendet wurde. Siehe Verwenden der Anwendungssteuerung.
Labelgruppe	(Optional) Die Labelgruppe, der das Label zugeordnet ist. Um das Label einer Labelgruppe zuzuordnen, klicken Sie auf **Bearbeiten** neben dem Feld *Labelgruppe* und wählen dann eine Labelgruppe aus. Dies ist nützlich, wenn Sie über eine große Zahl von Labels verfügen, die Sie in Unter-Labels gruppieren möchten. Sie können beispielsweise die Labels Ihrer lizenzierten Anwendungen in einer Labelgruppe namens *Lizenzen* zusammenfassen. Labels erben außerdem

Option	Beschreibung
	sämtliche Einschränkungen der Gruppen, denen sie angehören.

4. Klicken Sie auf **Speichern**.

   Die Seite *Labels* wird mit dem neuen Label in der Liste angezeigt. Das Symbol für die Erfassung der Nutzung wird in der entsprechenden Spalte neben dem Label angezeigt: .

5. Weisen Sie das Label manuell verwalteten Geräten zu:
   a. Klicken Sie auf **Inventar**.

      Die Seite *Geräte* wird angezeigt.

   b. Aktivieren Sie das Kontrollkästchen neben einem oder mehreren Geräten.
   c. Wählen Sie **Aktion auswählen** > **Label** > **Label zuweisen**.

      Eines der folgenden Symbole für die Erfassung der Nutzung wird neben dem Gerätenamen in der Liste *Geräte* angezeigt:

Symbol	Beschreibung
	Die Erfassung der Nutzung ist auf dem Gerät aktiviert, und der KACE Agent meldet nach Zeitplan die Nutzungsinformationen für Anwendungen im Softwarekatalog, deren Nutzungserfassung aktiviert ist. Siehe Erfassung von Geräten und Anwendungen aktivieren und konfigurieren. Abhängig vom Erfassungsintervall kann es bis zu 24 Stunden dauern, bis die Appliance-Erfassungsinformationen in der **Administratorkonsole** angezeigt werden. Informationen zum Ändern des Erfassungsintervalls finden Sie unter Erfassung von Anwendungen im Softwarekatalog aktivieren.
	Der Beginn der Erfassung ist geplant. Dieses Symbol wird angezeigt, wenn das Nutzungserfassungslabel einem Gerät zugewiesen wurde, dieses Gerät aber noch keine Nutzungserfassungsinformationen an die Appliance gemeldet hat. Wenn das Nutzungserfassungslabel Geräten mit Linux oder einem anderen nicht unterstützten Betriebssystem zugewiesen wurde, werden die Nutzungserfassungssymbole nicht angezeigt.

Erfassung auf Geräten mit Smart Labels aktivieren

Sie können die Erfassung mit Smart Labels unter der Voraussetzung aktivieren, dass das Smart Label ein Gerätelabel ist.

Smart Labels werden auf verwaltete Geräte angewendet bzw. entfernt, wenn die Geräte eine Verbindung mit der Appliance herstellen. Wenn Sie also ein Smart Label erstellen, das die Erfassung der Nutzung auf Geräten ermöglicht, kann es einige Zeit dauern, bis das Smart Label auf die Geräte angewendet wird und die Geräte mit der Meldung von Erfassungsinformationen beginnen. Die Erfassung der Nutzung wird für Geräte, die den Smart Label-Kriterien entsprechen, erst nach der Inventarisierung der Geräte und der Anwendung des Smart Labels aktiviert.

1. Rufen Sie die Liste *Smart Labels* auf:

a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.

b. Klicken Sie in der linken Navigationsleiste im Abschnitt **Startseite** auf **Label-Verwaltung**.

c. Klicken Sie im Bereich für die Label-Verwaltung auf **Smart Labels**.

2. Wählen Sie **Aktion auswählen** > **Neu** > **Smart Label für Gerät**, um den Smart Label-Bereich anzuzeigen.
3. Legen Sie die Suchkriterien anhand der verfügbaren Felder fest.
   - **Klicken Sie zum Hinzufügen einer Zeile auf Zeile hinzufügen.**
   - **Um einen Unterregelsatz hinzuzufügen, wählen Sie in der Dropdown-Liste für Operatoren rechts neben den Smart Label-Kriterien UND oder ODER aus und klicken anschließend auf Gruppe hinzufügen.**

4. Klicken Sie auf **Testen**, um Elemente anzuzeigen, die den angegebenen Kriterien entsprechen.
5. Passen Sie die Kriterien an, bis die Ergebnisse Ihren Erwartungen entsprechen.
6. Aktivieren Sie unter den Kriterien für Smart Labels das Kontrollkästchen *Erfassung aktiviert*.
7. Führen Sie im Menü *Label auswählen* einen der folgenden Schritte aus:
   - **Wählen Sie ein vorhandenes Label aus, um es mit diesem Smart Label zu verknüpfen. Geben Sie in das Feld *Label auswählen* einen Begriff ein, um nach vorhandenen Labels zu suchen.**

     HINWEIS: Wenn Sie statt eines Labels eine Labelgruppe auswählen, können Sie das Smart Label nicht auf einen Patching-Zeitplan anwenden. Patch-Zeitpläne können nur Smart Labels verwenden, die auf einem einzelnen Element basieren.

   - **Geben Sie einen neuen Namen für das Smart Label im Feld *Label auswählen* ein und drücken Sie Enter bzw. die Eingabetaste.**

     HINWEIS: Drücken Sie **Enter** bzw. die **Eingabetaste**, nachdem Sie einen neuen Smart Label-Namen eingegeben haben, um den Text aus dem Suchfeld in das Label-Feld zu verschieben.

8. Klicken Sie auf **Erstellen**.

   Bei der Inventarisierung verwalteter Geräte wird das Smart Label Geräten zugewiesen, die die angegebenen Kriterien erfüllen. Wurde das Label einem Gerät zugewiesen, wird in der Liste *Geräte* neben dem Namen des Geräts eines der folgenden Symbole für die Erfassung der Nutzung angezeigt:

Symbol	Beschreibung
	Die Erfassung der Nutzung ist auf dem Gerät aktiviert, und der KACE Agent meldet nach Zeitplan die Nutzungsinformationen für Anwendungen im Softwarekatalog, deren Nutzungserfassung aktiviert ist. Siehe Erfassung von Geräten und Anwendungen aktivieren und konfigurieren. Abhängig vom Erfassungsintervall kann es bis zu 24 Stunden dauern, bis die Appliance-Erfassungsinformationen in der **Administratorkonsole** angezeigt werden. Informationen zum Ändern des Erfassungsintervalls

Symbol	Beschreibung
	finden Sie unter Erfassung von Anwendungen im Softwarekatalog aktivieren.
	Der Beginn der Erfassung ist geplant. Dieses Symbol wird angezeigt, wenn das Nutzungserfassungslabel einem Gerät zugewiesen wurde, in der Appliance aber noch keine Nutzungserfassungsinformationen verfügbar sind. Wenn das Nutzungserfassungslabel Geräten mit Linux oder einem anderen nicht unterstützten Betriebssystem zugewiesen wurde, werden die Nutzungserfassungssymbole nicht angezeigt.

Erfassung von Anwendungen im Softwarekatalog aktivieren

Sie können die Erfassung für als "Erkannt" oder "Nicht erkannt" gekennzeichnete Anwendungen im Softwarekatalog sowie für lokal katalogisierte Anwendungen aktivieren. Wenn Sie die Erfassung für Anwendungen aktivieren, werden diese Anwendungen als erfasst identifiziert.

Sie müssen die Erfassung jedoch auch für die Geräte aktivieren, auf denen die Anwendungen installiert sind. Mit anderen Worten: Sie müssen die Erfassung sowohl für das Gerät als auch für die Anwendung aktivieren, um Erfassungsinformationen zu erhalten.

Wenn die Erfassung für eine Anwendung und für Geräte aktiviert ist, auf denen die Anwendung installiert ist, werden Erfassungsinformationen auf der Seite *Softwarekatalogdetails* für die Anwendung angezeigt. Die Erfassungsinformationen werden außerdem auf der Seite mit Details zu verwalteten Geräten angezeigt, auf denen die Anwendung installiert ist. Siehe Softwarekatalog-Erfassungsinformationen anzeigen.

VORSICHT: Die Erfassung ist nicht verfügbar für Betriebssystemsoftware, für Anwendungen, die unter nicht unterstützten Betriebssystemen (beispielsweise Linux) installiert wurden, oder für Anwendungen, die im Softwarekatalog als Nicht katalogisiert aufgeführt sind. Sie können die Erfassung für nicht erfasste Anwendungen jedoch aktivieren, wenn Sie die Anwendung zur lokalen Version des Softwarekatalogs hinzufügen.

1. Rufen Sie die Liste *Softwarekatalog* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Inventar** und anschließend auf **Softwarekatalog**.
2. Aktivieren Sie das Kontrollkästchen neben einer erkannten oder nicht erkannten Anwendung.
3. Wählen Sie **Aktion auswählen** > **Nutzungserfassung aktivieren**.

Ein Symbol für die Erfassung der Nutzung wird in der Spalte für die Erfassung der Nutzung neben den ausgewählten Anwendungen angezeigt: . Unter der Voraussetzung, dass die Erfassung für Geräte aktiviert ist, auf denen die Anwendung installiert ist, werden Erfassungsinformationen entsprechend dem Erfassungszeitplan gemeldet. Siehe:

- Erfassung auf Geräten aktivieren
- Optionen für die Erfassung von Anwendungen im Softwarekatalog konfigurieren

Optionen für die Erfassung von Anwendungen im Softwarekatalog konfigurieren

Sie können Erfassungsoptionen konfigurieren, z. B. die Häufigkeit der Nutzungserfassung sowie die Aufbewahrungsdauer der entsprechenden Daten in der Datenbank der Appliance.

Wenn die Organisationskomponente auf der Appliance aktiviert ist, können Sie die Einstellungen für jede Organisation separat konfigurieren.

1. Führen Sie einen der folgenden Schritte aus:
   - **Wenn die Organisationskomponente für die Appliance aktiviert ist, melden Sie sich bei der Systemverwaltungskonsole der Appliance an: `https://appliance_hostname/system`. Oder wählen Sie in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen den Eintrag System aus. Klicken Sie anschließend auf Organisationen. Klicken Sie auf den Namen einer Organisation, um Informationen dazu anzuzeigen.**

     Die Seite *Detail zu Organisation* wird angezeigt. Suchen Sie hier nach dem Abschnitt *Kommunikations- und Agenten-Einstellungen*.
   - **Wenn die Organisationskomponente nicht für die Appliance aktiviert ist, melden Sie sich bei der Administratorkonsole der Appliance an: `https://appliance_hostname/admin`. Wählen Sie anschließend Einstellungen > Provisionierung und klicken Sie im Fensterbereich** *Provisionierung* **auf Kommunikationseinstellungen.**

     Die Seite *Kommunikationseinstellungen* wird angezeigt.
2. Geben Sie im Abschnitt *Agenten- und Kommunikationseinstellungen* folgende Einstellungen an:

Option	Empfohlene Einstellung	Anmerkungen
Agentenprotokollierung	Aktiviert	Gibt an, ob die Appliance Skriptergebnisse speichert, die von Agenten auf verwalteten Geräten übermittelt wurden. Agenten-Protokolle können in der Datenbank bis zu 1GB Speicherplatz benötigen. Wenn Speicherplatz keine Rolle spielt, aktivieren Sie die *Agentenprotokollierung*, um alle Protokollinformationen für vom Agenten verwaltete Geräte zu speichern. Diese Protokolle können bei der Fehlerbehebung nützlich sein. Um Speicherplatz zu sparen und eine schnellere Kommunikation mit dem Agenten zu ermöglichen, deaktivieren Sie die *Agentenprotokollierung*.
Agenten-Inventar	12 Stunden	Die Häufigkeit, mit der Agenten auf verwalteten Geräten das Inventar melden. Diese Informationen werden im Abschnitt *Inventar* angezeigt.
Inventar ohne Agent	1 Tag	Die Häufigkeit, mit Geräte ohne Agent Inventar melden. Diese Informationen werden im Abschnitt *Inventar* angezeigt.
Kataloginventarisierung	24 Stunden	Die Häufigkeit, mit der verwaltete Geräte der Seite *Softwarekatalog* das Inventar melden sollen.

Option	Empfohlene Einstellung	Anmerkungen
Erfassung der Nutzung	4 Stunden	Die Häufigkeit, mit der verwaltete Geräte der Appliance Erfassungsinformationen melden sollen. Damit dies möglich ist, muss die Erfassung auf Geräten und in Anwendungen aktiviert sein.
Skriptaktualisierung	4 Stunden	Die Häufigkeit, mit der Agenten auf den verwalteten Geräten aktualisierte Skriptkopien anfordern sollen, die auf verwalteten Geräten verfügbar sind. Dieses Intervall hat keine Auswirkungen darauf, wie häufig ein Skript ausgeführt wird.

3. Klicken Sie auf **Speichern**.
4. Um die Datenaufbewahrungseinstellungen zu konfigurieren, rufen Sie die Seite *Allgemeine Einstellungen* auf der Verwaltungsebene auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Einstellungen** und anschließend auf **Allgemeine Einstellungen**.
5. Wählen Sie im Abschnitt *Datenaufbewahrung* die Optionen für die Datenaufbewahrung in der Appliance aus.

Option	Beschreibung
Erfassungsdaten beibehalten	Die Anzahl der Monate, für die Erfassungsdaten in der Datenbank der Appliance gespeichert werden. Erfassungsdaten, die älter als die ausgewählte Anzahl von Monaten sind, werden am ersten Tag jedes Monats aus der Datenbank gelöscht. Siehe Informationen zu Erfassungsinformationen.

6. Klicken Sie unten auf der Seite auf **Speichern** oder **Dienste speichern und neu starten**, je nachdem, ob die Organisationskomponente auf Ihrer Appliance aktiviert ist.
7. Wenn Sie mehrere Organisationen haben, wiederholen Sie die oben aufgeführten Schritte für jede Organisation.

Softwarekatalog-Erfassungsinformationen anzeigen

Sie können Erfassungsinformationen auf der Seite *Softwarekatalog-Detail* und auf der Seite *Gerätedetail* anzeigen.

HINWEIS: Die Erfassungsinformationen stehen jedoch nur für Geräte und Anwendungen mit aktivierter Erfassung zur Verfügung. Informationen hierzu finden Sie unter Erfassung von Geräten und Anwendungen aktivieren und konfigurieren.

Erfassungsinformationen auf der Seite "Softwarekatalogdetails" anzeigen

Auf der Seite *Softwarekatalogdetails* können Sie Erfassungsinformationen für Anwendungen im Softwarekatalog anzeigen.

Wie viele Erfassungsinformationen auf der Seite *Softwarekatalogdetails* verfügbar sind, hängt von den Einstellungen für die Aufbewahrung von erfassten Daten ab. Siehe Informationen zu Erfassungsinformationen.

1. Rufen Sie die Liste *Softwarekatalog* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Inventar** und anschließend auf **Softwarekatalog**.
2. **Optional**: Klicken Sie auf die Überschrift der Spalte für die Erfassung der Nutzung, um die Liste nach erfassten Anwendungen zu sortieren: .
3. Klicken Sie auf den Namen einer Anwendung mit aktivierter Nutzungserfassung, um die Softwarekatalog-Detailseite anzuzeigen.

   Auf dieser Seite werden folgende Informationen angegeben:

Spaltenname	Beschreibung
Installierte Versionen/Anwendungen	
Dateiname	Bei Anwendungen der Name der ausführbaren Datei
Produktname	Bei Suites der Name der Suite
Version	Die Versionsnummer der Anwendung
Sprache	Die Sprache, für die die Anwendung entwickelt wurde, zum Beispiel Englisch. Anwendungen, die nicht für eine bestimmte Sprache entwickelt wurden, werden als „sprachneutral“ bezeichnet.
Installiert	Die Anzahl verwalteter Geräte, auf denen die Anwendung installiert ist Klicken Sie auf eine Zahl, um Geräteinformationen anzuzeigen.
Erfassung der Nutzung	
Letzter Tag	Die Anzahl verwalteter Geräte, auf denen die Anwendung in den vergangenen 24 Stunden gestartet wurde
Vor 1 - 7 Tagen	Die Anzahl verwalteter Geräte, auf denen die Anwendung in den vergangenen 7 Tagen gestartet wurde
Vor 8 - 30 Tagen	Die Anzahl verwalteter Geräte, auf denen die Anwendung in den vergangenen 8 bis 30 Tagen gestartet wurde

Erfassungsinformationen auf der Seite "Gerätedetail" anzeigen

Auf der Seite *Gerätedetail* können Sie Erfassungsinformationen für Anwendungen im Softwarekatalog anzeigen.

1. Rufen Sie die Liste *Geräte* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Inventar** und anschließend auf **Dashboard**.
2. Klicken Sie auf den Namen eines verwalteten Geräts mit aktivierter Nutzungserfassung, um die *Gerätedetailseite* anzuzeigen.
3. Klicken Sie im Abschnitt *Software* auf **Software mit erfasster Nutzung**, um den Bereich zu erweitern.

   Informationen in diesem Abschnitt:

Spaltenname	Beschreibung
Anwendung	Der Name der erfassten Anwendung. Klicken Sie auf den Anwendungsnamen, um die Details für diese Anwendung aufzurufen.
Version	Die Version der installierten Anwendung. Hauptversionen werden getrennt als Titel im Softwarekatalog aufgeführt und getrennt erfasst. Beispielsweise werden Version **4.1** und Version **4.2** einer Anwendung als separate Einträge angezeigt. So können Sie sie getrennt verwalten und ihre Nutzung getrennt erfassen. Nebenversionen, beispielsweise **4.123**, **4.134** und **4.145**, werden unter demselben Eintrag angezeigt, beispielsweise **4.x**. Jede unter dem Eintrag **4.x** gruppierte Version wird auf der Seite mit den Details zur Anwendung aufgeführt.
Nutzungsstunden	Die Zeitdauer, in der die Anwendung im Laufe der letzten sieben Tage auf dem Gerät ausgeführt wurde, als Dezimalzahl. 0,75 zeigt beispielsweise an, dass die Anwendung 45 Minuten lang ausgeführt wurde.
Starts	Die Häufigkeit, mit der die Anwendung im Laufe der letzten sieben Tage auf dem Gerät ausgeführt wurde
Letzter Start	Datum und Zeit des aktuellsten Starts der Anwendung im Laufe der letzten 7Tage

HINWEIS: Wenn zwischen dem Zeitpunkt der Erfassung des Inventars eines Geräts und dem Zeitpunkt der Erstellung des Erfassungsberichts neue Anwendungen installiert werden, dann werden diese Anwendungen erst bei der nächsten Erfassung des Inventars gemeldet.

Erfassung von Anwendungen im Softwarekatalog sowie verwalteten Geräten deaktivieren

Mit der Deaktivierung der Erfassung für Anwendungen und Geräte wird die Speicherung der jeweiligen Erfassungsdaten beendet. Bereits gespeicherte Erfassungsdaten werden jedoch beibehalten.

Erfassung von Anwendungen im Softwarekatalog deaktivieren

Wenn die Erfassung für Anwendungen im Softwarekatalog aktiviert ist, können Sie sie bei Bedarf deaktivieren.

1. Rufen Sie die Liste *Softwarekatalog* auf:
    a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
    b. Klicken Sie in der linken Navigationsleiste auf **Inventar** und anschließend auf **Softwarekatalog**.
2. Aktivieren Sie das Kontrollkästchen neben einer Anwendung.
3. Wählen Sie **Aktion auswählen** > **Erfassung der Nutzung deaktivieren**.

Die Erfassung der Nutzung wird deaktiviert und das Symbol aus der entsprechenden Spalte neben den ausgewählten Anwendungen entfernt. Die Erfassungsdaten werden jedoch beibehalten.

Erfassung für Geräte deaktivieren

Wenn die Erfassung für Geräte aktiviert ist, können Sie sie bei Bedarf deaktivieren.

Erfassung auf Geräten mit manuellen Labels deaktivieren

Wenn die Erfassung für Geräte mit manuellen Labels aktiviert ist, können Sie sie in den Label-Details deaktivieren.

1. Rufen Sie die Liste *Labels* auf:
    a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
    b. Klicken Sie in der linken Navigationsleiste im Abschnitt **Startseite** auf **Label-Verwaltung**.
    c. Klicken Sie im Bereich für die Label-Verwaltung auf **Labels**.
2. Aktivieren Sie das Kontrollkästchen neben einem Nutzungserfassungslabel.
3. Wählen Sie **Aktion auswählen** > **Erfassung der Nutzung deaktivieren**.

Die Erfassung wird für alle Geräte deaktiviert, denen das Label zugewiesen wurde. Die Erfassungsdaten werden jedoch beibehalten.

Erfassung auf Geräten mit Smart Labels deaktivieren

Wenn die Erfassung für Geräte mit Smart Labels aktiviert ist, können Sie sie in den Smart Label-Details deaktivieren.

1. Rufen Sie die *Smart Label-Detailseite* auf:
    a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.

b. Klicken Sie in der linken Navigationsleiste im Abschnitt **Startseite** auf **Label-Verwaltung**.
c. Klicken Sie im Bereich für die Label-Verwaltung auf **Smart Labels**.
d. Klicken Sie auf den Namen eines Smart Labels.

2. Deaktivieren Sie das Kontrollkästchen *Nutzungserfassung aktivieren*.

Die Erfassung wird für alle Geräte deaktiviert, denen das Label zugewiesen wurde. Die Erfassungsdaten werden jedoch beibehalten.

Nutzungserfassung verwalten und Inventarerfassung planen

Die Erfassung der Nutzung ist nur für Anwendungen auf der Seite Softwarekatalog verfügbar. Für Anwendungen auf der Seite *Software* ist die Erfassung der Nutzung nicht verfügbar.

Informationen zur Aktivierung der Nutzungserfassung finden Sie unter Informationen zu Erfassungsinformationen.

Intervalle für die Erfassung der Nutzung und des Inventars planen

Die Intervalle für die Erfassung der Nutzung und des Inventars bestimmen die Häufigkeit, mit der Nutzungs- und Inventarinformationen auf verwalteten Geräten erfasst werden. Ist auf der Appliance die Organisationskomponente aktiviert, können Sie die Intervalle für die Erfassung der Nutzung und des Inventars für jede Organisation individuell planen.

1. Führen Sie einen der folgenden Schritte aus:

   - **Wenn die Organisationskomponente für die Appliance aktiviert ist, melden Sie sich bei der Systemverwaltungskonsole der Appliance an: `https://appliance_hostname/system`. Oder wählen Sie in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen den Eintrag System aus. Klicken Sie anschließend auf Organisationen. Klicken Sie auf den Namen einer Organisation, um Informationen dazu anzuzeigen.**

     Die Seite *Detail zu Organisation* wird angezeigt. Suchen Sie hier nach dem Abschnitt *Kommunikations- und Agenten-Einstellungen*.

   - **Wenn die Organisationskomponente nicht für die Appliance aktiviert ist, melden Sie sich bei der Administratorkonsole der Appliance an: `https://appliance_hostname/admin`. Wählen Sie anschließend Einstellungen > Provisionierung und klicken Sie im Fensterbereich *Provisionierung* auf Kommunikationseinstellungen.**

     Die Seite *Kommunikationseinstellungen* wird angezeigt.

2. Geben Sie im Abschnitt *Agenten- und Kommunikationseinstellungen* folgende Einstellungen an:

Option	Empfohlene Einstellung	Anmerkungen
Agentenprotokollierung	Aktiviert	Gibt an, ob die Appliance Skriptergebnisse speichert, die von Agenten auf verwalteten Geräten übermittelt wurden. Agenten-Protokolle können in der Datenbank bis zu 1GB Speicherplatz benötigen. Wenn Speicherplatz keine Rolle spielt, aktivieren Sie die *Agentenprotokollierung*, um alle Protokollinformationen für vom Agenten verwaltete Geräte zu speichern. Diese Protokolle können bei der Fehlerbehebung nützlich sein. Um Speicherplatz zu sparen und eine schnellere

Option	Empfohlene Einstellung	Anmerkungen
		Kommunikation mit dem Agenten zu ermöglichen, deaktivieren Sie die *Agentenprotokollierung*.
Agenten-Inventar	12 Stunden	Die Häufigkeit, mit der Agenten auf verwalteten Geräten das Inventar melden. Diese Informationen werden im Abschnitt *Inventar* angezeigt.
Inventar ohne Agent	1 Tag	Die Häufigkeit, mit Geräte ohne Agent Inventar melden. Diese Informationen werden im Abschnitt *Inventar* angezeigt.
Kataloginventarisierung	24 Stunden	Die Häufigkeit, mit der verwaltete Geräte der Seite *Softwarekatalog* das Inventar melden sollen.
Erfassung der Nutzung	4 Stunden	Die Häufigkeit, mit der verwaltete Geräte der Appliance Erfassungsinformationen melden sollen. Damit dies möglich ist, muss die Erfassung auf Geräten und in Anwendungen aktiviert sein.
Skriptaktualisierung	4 Stunden	Die Häufigkeit, mit der Agenten auf den verwalteten Geräten aktualisierte Skriptkopien anfordern sollen, die auf verwalteten Geräten verfügbar sind. Dieses Intervall hat keine Auswirkungen darauf, wie häufig ein Skript ausgeführt wird.

3. Klicken Sie auf **Speichern**.

Verwenden der Anwendungssteuerung

Mit der Anwendungssteuerung können Sie Anwendungen als "Nicht zulässig" kennzeichnen und sie blockieren oder verhindern, dass diese Anwendungen auf vom Agenten verwalteten Windows- und Mac-Geräten ausgeführt werden. Dies ist hilfreich, wenn Sie die Ausführung spezifischer Anwendungen in Ihrer Umgebung einschränken möchten.

Anwendungssteuerung bietet folgende Möglichkeiten:

- Verhindern, dass bestimmte Anwendungen auf vom Agenten verwalteten Windows und Mac Geräten ausgeführt werden. Diese Option ist für Linux Geräte und Geräte ohne Agent nicht verfügbar. Siehe Voraussetzungen für das Blockieren von Anwendungen.
- Erstellen von Berichten zu Anwendungen, die als Nicht zulässig gekennzeichnet sind. Siehe Berichte mit als "Nicht zulässig" gekennzeichneten Anwendungen erstellen.
- Suchen nach als "Nicht zulässig" gekennzeichneten Anwendungen mithilfe der *Erweiterten Suche*. Siehe Suchen nach Informationen und Filtern von Listen.

Als Nicht zulässig gekennzeichnete Anwendungen sind organisationsspezifisch. Wenn auf der Appliance die Organisationskomponente aktiviert ist, kennzeichnen Sie Anwendungen für jede Organisation separat als "Nicht zulässig".

Voraussetzungen für das Blockieren von Anwendungen

Zum Blockieren von Anwendungen müssen bestimmte Voraussetzungen der Anwendungssteuerung erfüllt werden.

Gehen Sie wie folgt vor, um Anwendungen zu blockieren deren Ausführung auf verwalteten Geräten zu verhindern:

- **Installieren Sie auf den Geräten den KACE Agent ab Version 6.0**. Anwendungssteuerung ist für Versionen des Agenten vor Version 6.0 sowie für Linux Geräte und Geräte ohne Agent nicht verfügbar. Siehe KACE Agent auf verwalteten Geräten aktualisieren.
- **Weisen Sie Geräten ein Label mit aktivierter Anwendungssteuerung zu**. Dadurch wird dem Agenten die Überwachung von Anwendungsstarts ermöglicht, einschließlich von Anwendungen, die als Nicht zulässig gekennzeichnet sind. Siehe Anwendungssteuerungslabel zu Geräten zuweisen.
- **Kennzeichnen Sie Anwendungen als "Nicht zulässig"**. Windows und Mac Anwendungen können nur dann als Nicht zulässig gekennzeichnet werden, wenn sie im Softwarekatalog als erkannte, nicht erkannte oder lokal katalogisierte Anwendungen aufgeführt sind. Nicht katalogisierte Anwendungen können erst dann als Nicht zulässig gekennzeichnet werden, wenn sie zum Softwarekatalog hinzugefügt wurden. Siehe Hinzufügen von Anwendungen zum Softwarekatalog. Linux Anwendungen können nicht als "Nicht zulässig" gekennzeichnet werden.
- **Geben Sie die Version der Anwendung an, die blockiert werden soll**. Wenn Sie beispielsweise alle Versionen von Adobe Acrobat blockieren möchten, müssen Sie sämtliche Versionen der Anwendung als "Nicht zulässig" kennzeichnen – zum Beispiel Acrobat 8.x, Acrobat 9.x usw. Wenn Sie jedoch eine Suite als Nicht zulässig kennzeichnen, werden alle Anwendungen in dieser Suite ebenfalls als Nicht zulässig gekennzeichnet. Wenn Sie eine Anwendung, die auf Windows und Mac Geräten ausgeführt werden kann, als "Nicht zulässig" kennzeichnen, wird diese Anwendung sowohl auf Windows als auch Mac Geräten blockiert.

Vorgehensweise zur Blockierung von Anwendungen

Wenn eine als nicht zulässig gekennzeichnete Anwendung auf einem verwalteten Gerät gestartet wird, dem ein für Anwendungssteuerung aktiviertes Label zugewiesen wurde, beendet der Agent die Anwendung und zeigt eine Meldung auf dem Gerät an.

Die Meldung gibt den Namen der Anwendung an und weist darauf hin, dass die Anwendung beendet wurde, weil sie in der Liste Nicht zulässig enthalten ist. Beendete Anwendungen werden in der lokalen Datenbank aufgeführt, die die Softwarenutzung aufzeichnet.

Informationen zum Blockieren von Anwendungseditionen, die ausführbare Dateien gemeinsam nutzen

Einige Anwendungen liegen in verschiedenen Editionen vor, wie etwa Pro und Standard, die dieselbe ausführbare Datei verwenden. Wenn solche Anwendungen blockiert werden, betrifft dies alle Editionen, die diese ausführbare Datei nutzen.

Anwendungen, die nicht blockiert werden können

Einige Anwendungen (wie etwa Plug-ins für andere Anwendungen) können nicht blockiert werden.

Die folgenden Anwendungen können zwar als "Nicht zulässig" gekennzeichnet werden, sie können jedoch nicht blockiert oder an der Ausführung auf verwalteten Geräten gehindert werden:

- Browser-Plug-ins oder externe DLL-Dateien
- Plug-Ins für Microsoft Visual Studio® (beispielsweise Infragistics)
- Java®-Anwendungen

Anwendungssteuerungslabel zu Geräten zuweisen

Zur Aktivierung der Anwendungssteuerung auf Geräten müssen Sie diesen das Label *ApplicationControlDevices* oder ein anderes Label mit aktivierter Anwendungssteuerung zuweisen.

Sobald das Label Geräten zugewiesen wurde, werden als "Nicht zulässig" gekennzeichnete Anwendungen blockiert bzw. an der Ausführung auf diesen Geräten gehindert.

1. Rufen Sie die Liste *Geräte* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Inventar** und anschließend auf **Dashboard**.
2. Aktivieren Sie die Kontrollkästchen neben einem oder mehreren Geräten.
3. Wählen Sie **Aktion auswählen** > **Labels zuweisen**.
4. Wählen Sie das Label **ApplicationControlDevices** aus.

Das Label wird neben den Gerätenamen auf der Seite *Geräte* angezeigt.

Anwendungen und Suites als "Nicht zulässig" kennzeichnen

Sie können einzelne Anwendungen und Anwendungs-Suites als "Nicht zulässig" kennzeichnen und so deren Ausführung auf vom Agenten verwalteten Geräten verhindern.

Wenn Sie eine Suite als Nicht zulässig kennzeichnen, werden die Anwendungen in dieser Suite ebenfalls als Nicht zulässig gekennzeichnet. Falls Sie nur einige Anwendungen in der Suite als Nicht zulässig kennzeichnen möchten, entfernen Sie die Kennzeichnung als Nicht zulässig von der Suite und markieren die einzelnen Anwendungen als Nicht zulässig.

1. Rufen Sie die Liste *Softwarekatalog* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Inventar** und anschließend auf **Softwarekatalog**.
2. Aktivieren Sie das Kontrollkästchen neben einer oder mehreren Anwendungen.
3. Wählen Sie **Aktion auswählen** > **Als 'Nicht zulässig' kennzeichnen**.

Die Anwendungen werden als "Nicht zulässig" gekennzeichnet und neben den Anwendungsnamen wird das entsprechende Symbol angezeigt: 🚫.

Anwendungen und Suites anzeigen, die als "Nicht zulässig" gekennzeichnet sind

Sie können als "Nicht zulässig" gekennzeichnete Anwendungen und Suites auf der Seite *Softwarekatalog* anzeigen.

1. Rufen Sie die Liste *Softwarekatalog* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Inventar** und anschließend auf **Softwarekatalog**.
2. Führen Sie einen der folgenden Schritte aus:
   - **Klicken Sie über der Liste auf der linken Seite auf die Registerkarte Erkannt oder Nicht erkannt und anschließend auf der Seite** *Softwarekatalog* **auf die Schaltfläche Nicht zulässig, um die Ergebnisse nach als "Nicht zulässig" gekennzeichneten Anwendungen zu sortieren:** 🚫**.**
   - **Klicken Sie rechts über der Liste auf die Registerkarte Erweiterte Suche und legen Sie die erforderlichen Kriterien zum Anzeigen von als "Nicht zulässig" gekennzeichneten Anwendungen fest:**

     `Softwarekatalog: Nicht zulässig | ist | Wahr`
3. Klicken Sie auf **Suchen**.

Berichte mit als "Nicht zulässig" gekennzeichneten Anwendungen erstellen

Sie können Berichte erstellen, die als "Nicht zulässig" gekennzeichnete Anwendungen sowie die Geräte enthalten, auf denen diese Anwendungen installiert sind.

1. Führen Sie eine der folgenden Aktionen aus, um die Liste *Berichte* aufzurufen:
   - **Wenn für Ihre Appliance die Organisationskomponente aktiviert ist, können Sie folgendermaßen auf einen Bericht auf Systemebene zugreifen:**

     Melden Sie sich bei der Systemadministratorkonsole der Appliance an: `https://`**appliance_hostname**`/system`. Oder wählen Sie in der Dropdown-Liste rechts oben auf der Seite den Eintrag **System** aus. Klicken Sie anschließend auf **Berichterstellung**.
     Berichte auf Systemebene enthalten konsolidierte Berichte, die Informationen von allen Organisationen zusammenfassen, sowie Standardberichte für verschiedene Appliance-Komponenten.
   - **Wenn die Organisationskomponente nicht für die Appliance aktiviert ist oder Sie auf einen Bericht auf Organisationsebene zugreifen möchten, melden Sie sich bei der Administratorkonsole der Appliance an: `https://`appliance_hostname`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option** *Organisationsmenü in Verwaltungskopfzeile anzeigen* **aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus. Klicken Sie anschließend auf Berichterstellung.**

     Berichte auf Organisationsebene enthalten Standardberichte für verschiedene Appliance-Komponenten. Wenn für Ihre Appliance die Organisationskomponente aktiviert ist, liefern diese Berichte Informationen speziell für die ausgewählte Organisation.

   Die Liste *Berichte* wird angezeigt.
2. Wählen Sie **Aktion auswählen > Neu (Assistent)**, um die *Berichtstitelseite* aufzurufen.
3. Legen Sie die folgenden Einstellungen fest:

Option	Beschreibung
Titel	Nicht zulässige Software
Kategorie	Software
Beschreibung	Software, die als Nicht zulässig gekennzeichnet ist
Zeilennummern anzeigen	(Optional) Aktivieren Sie das Kontrollkästchen, um eine Spalte mit Zeilennummern zum Bericht hinzuzufügen.
Thema	Softwarekatalog – Erkannte Software
Unterthema	Gerät

4. Klicken Sie auf **Weiter**, um die Seite *Anzuzeigende Felder* anzuzeigen.
5. Wählen Sie die gewünschten Berichtsfelder, z. B.:
   - **Name: Der Name der Anwendung**
   - **Installiert auf: Die Anzahl von Geräten, auf denen die Anwendung installiert ist**
   - **Kategorie: Die Kategorie der Anwendung**
   - **Gerät: Informationen zu den Geräten, auf denen die Anwendung installiert ist**
6. Klicken Sie auf **Weiter**, um die Seite *Spaltenreihenfolge* anzuzeigen.
7. Ziehen Sie die Spalten in die Reihenfolge, in der sie im Bericht erscheinen sollen, und klicken Sie auf **Weiter**, um die Seite *Sortieren und Untergliederung* anzuzeigen.
8. Wählen Sie die gewünschten Sortier- und Untergliederungsoptionen aus und klicken Sie auf **Weiter**, um die Seite *Filter* anzuzeigen.
9. Klicken Sie auf **Geben Sie Regeln zum Filtern der Daten an** und geben Sie die erforderlichen Kriterien für die Suche nach als "Nicht zulässig" gekennzeichneten Anwendungen an:

   ```
   Informationen zu erkannter Software: Nicht zulässig | = | 1
   ```

10. Klicken Sie in der Zeile auf **Speichern** und anschließend unten auf der Seite auf **Speichern**.

    Die Liste *Berichte* wird mit dem neuen Bericht angezeigt. Die rechts über der Tabelle angezeigte Liste *Anzeigen nach* wird automatisch auf die Kategorie des neuen Berichts eingestellt.
11. Klicken Sie auf ein Format in der Spalte *Bericht generieren*, um den Bericht auszuführen.

Der Bericht wird generiert. Bei HTML-Berichten wird die erste Datenspalte automatisch mit der Detailseite für dieses Element auf der **Administratorkonsole** verknüpft. Weitere Informationen zu Berichten finden Sie unter Erstellen von Berichten.

Kennzeichnung "Nicht zulässig" von Anwendungen entfernen

Wenn Sie Anwendungen als Nicht zulässig gekennzeichnet haben, können Sie diese Kennzeichnung bei Bedarf entfernen.

Die Kennzeichnung als Nicht zulässig ist organisationsspezifisch. Wenn auf der Appliance die Organisationskomponente aktiviert ist, können Sie die Kennzeichnung von Anwendungen als Nicht zulässig für jede Organisation individuell anwenden oder entfernen.

TIPP: Standardmäßig sind alle Anwendungen zulässig, sofern Sie sie nicht als Nicht zulässig kennzeichnen.

1. Rufen Sie die Liste *Softwarekatalog* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Inventar** und anschließend auf **Softwarekatalog**.
2. Aktivieren Sie das Kontrollkästchen neben einer oder mehreren Anwendungen.
3. Wählen Sie **Aktion auswählen** > **Als 'Zulässig' kennzeichnen**.

   Die Anwendung wird als Zulässig gekennzeichnet und das Symbol für Nicht zulässig wird entfernt.

Softwarekatalog aktualisieren oder neu installieren

Der Softwarekatalog wird kontinuierlich aktualisiert, wenn neue Softwareanwendungen verfügbar werden und Katalogisierungsanforderungen eingehen. Diese Aktualisierungen werden regelmäßig automatisch heruntergeladen und auf den KACE SMAs installiert. Sie können manuell nach Aktualisierungen für den Softwarekatalog suchen oder den Katalog neu installieren.

Wenn Sie eine Offline-Appliance ohne Internetverbindung besitzen, wenden Sie sich unter **Quest Support** an https://support.quest.com/contact-support, um Aktualisierungen für den Softwarekatalog zu erhalten.

HINWEIS: Wenn Aktualisierungen des Katalogs heruntergeladen werden, ermittelt die Appliance, ob lokal katalogisierte Anwendungen zum öffentlichen Softwarekatalog hinzugefügt worden sind. Falls Anwendungen hinzugefügt worden sind, werden die lokalen Katalogisierungen entfernt. Anderenfalls werden die lokalen Katalogisierungen beibehalten.

1. Navigieren Sie zur *Systemsteuerung* der Appliance:
   - **Wenn die Organisationskomponente nicht für die Appliance aktiviert ist, melden Sie sich bei der Administratorkonsole an: `https://`appliance_hostname`/admin`, und wählen Sie dann Einstellungen > Systemsteuerung aus.**
   - **Wenn die Organisationskomponente für die Appliance aktiviert ist, melden Sie sich bei der Systemverwaltungskonsole der Appliance an: `https://`appliance_hostname`/system`. Oder wählen Sie in der Dropdown-Liste rechts oben auf der Seite den Eintrag System aus, und klicken Sie dann auf Einstellungen > Systemsteuerung.**
2. Klicken Sie auf **Appliance-Aktualisierungen**, um die Seite *Appliance-Aktualisierungen* anzuzeigen.
3. Führen Sie einen der folgenden Schritte aus:
   - **Klicken Sie im Abschnitt** *Softwarekatalog* **auf die Option Auf Aktualisierungen prüfen.**

     Wenn der Softwarekatalog auf dem neuesten Stand ist, wird die Seite *Protokolle* mit den Versionsinformationen angezeigt. Wenn eine aktuelle Version verfügbar ist, werden Installationsinformationen angezeigt. Der vollständige Katalog muss neu installiert werden, falls einer der folgenden Punkte zutrifft: Auf der Appliance ist kein Grundlagenkatalog vorhanden, es ist kein Pfad für die Aktualisierung des vollständigen Katalogs verfügbar oder es stehen mehr als fünf Aktualisierungen zur Verfügung.
   - **Klicken Sie im Abschnitt** *Softwarekatalog* **auf Neu installieren.**

     Die Version des Softwarekatalogs, der auf der Appliance gespeichert ist, wird durch den neuesten Softwarekatalog von Quest KACE ersetzt. Der vollständige Softwarekatalog umfasst die neueste

Vollversion des Katalogs sowie alle Aktualisierungen oder Ergänzungen, die seit der Veröffentlichung der letzten Vollversion des Katalogs hinzugefügt worden sind.

- **Handelt es sich bei Ihrer Appliance um eine Offline-Appliance ohne Internetzugriff, wenden Sie sich unter https://support.quest.com/contact-support an den Quest Support.**

Verwalten des Prozess-, Startprogramm- und Dienstinventars

Sie können Prozesse, Startprogramme und Dienste im Appliance-Inventar verwalten.

Verwalten des Prozessinventars

Auf verwalteten Geräten erkannte Prozesse werden im Abschnitt *Inventar* gemeldet und können dort verwaltet werden.

Bei der Verwaltung von Prozessinventar haben Sie folgende Möglichkeiten:

- Sie können sich die Prozessnutzungsinformationen für die letzten 1, 2, 3, 6 oder 12 Monate anzeigen lassen.
- Prozessen Labels zuweisen oder von diesen entfernen
- Zuweisen von Kategorien und Bedrohungsstufen zu Prozessen
- Prozesse löschen

Für Prozessinventar kann keine Nutzungserfassung durchgeführt und Prozesse können nicht ausgeschlossen werden. Anwendungen können dagegen ausgeschlossen werden. Siehe Anwendungen und Suites als "Nicht zulässig" kennzeichnen.

Prozessdetails anzeigen und bearbeiten

Sie können Details zu Prozessen im Inventar anzeigen und bearbeiten.

1. Rufen Sie die *Prozessdetailseite* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Inventar** und anschließend auf **Prozesse**.
   c. Klicken Sie auf den Namen eines Prozesses.
2. Geben Sie die folgenden Informationen an:

Option	Beschreibung
Zuweisen zu Label	(Optional) Das dem Element zugeordnete Label.
Anmerkungen	Geben Sie nach Bedarf beliebige weitere Informationen ein.
Kategorie	Die Kategorie des Elements, z.B. Business, Treiber oder Sicherheit

Option	Beschreibung
Bedrohungsstufe	Die Bedrohungsstufe des Elements. Mögliche Bedrohungsstufen: a. Sicher b. Ziemlich sicher c. Unbekannt d. Könnte schädlich sein e. Schädlich

3. Klicken Sie auf **Speichern**.

Labels für Prozesse hinzufügen

Fügen Sie manuelle Labels hinzu, um Prozesse im Inventar als Gruppe zu verwalten.

1. Rufen Sie die Liste *Prozesse* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Inventar** und anschließend auf **Prozesse**.
2. Wählen Sie **Aktion auswählen > Label hinzufügen**.
3. Geben Sie im Fenster *Label hinzufügen* einen Namen für das Label ein.

   TIPP: Vermeiden Sie in Labelnamen die Verwendung des umgekehrten Schrägstrichs (\). Wenn Sie einen umgekehrten Schrägstrich in einem Labelnamen verwenden müssen, fügen Sie einen zweiten umgekehrten Schrägstrich hinzu (\\), damit er nicht als Befehl interpretiert wird.

4. Klicken Sie auf **Speichern**.

Prozessen Labels zuweisen oder Labels aus Prozessen entfernen

Labels können bei Bedarf Prozessen im Inventar zugewiesen oder entfernt werden.

1. Rufen Sie die Liste *Prozesse* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Inventar** und anschließend auf **Prozesse**.
2. Aktivieren Sie das Kontrollkästchen neben dem Prozess/den Prozessen.
3. Führen Sie einen der folgenden Schritte aus:
   - **Wählen Sie Aktion auswählen > Label zuweisen und anschließend das zuzuweisende Label aus.**
   - **Wählen Sie Aktion auswählen > Label entfernen und anschließend das zu entfernende Label aus.**

Prozesse kategorisieren

Sie können Prozesse im Inventar organisieren und verwalten, indem Sie sie manuell Kategorien zuweisen.

1. Rufen Sie die Liste *Prozesse* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Inventar** und anschließend auf **Prozesse**.
2. Aktivieren Sie das Kontrollkästchen neben dem Prozess/den Prozessen.
3. Wählen Sie **Aktion auswählen** > **Kategorie festlegen** und anschließend eine Kategorie aus.

Prozessen Bedrohungsstufen zuweisen

Sie können Prozessen, die unter Umständen eine Bedrohung für Geräte und Systeme darstellen, manuell eine Bedrohungsstufe zuweisen.

Mithilfe von Bedrohungsstufen können Sie die relative Sicherheit von Elementen und die Anzahl der Geräte anzeigen, auf denen diese Elemente installiert sind. Diese Informationen dienen nur Nachverfolgungszwecken. Die Appliance erzwingt basierend auf den Bedrohungsstufen keine Richtlinien.

1. Rufen Sie die Liste *Prozesse* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Inventar** und anschließend auf **Prozesse**.
2. Aktivieren Sie das Kontrollkästchen neben dem Prozess/den Prozessen.
3. Wählen Sie **Aktion auswählen** > **Bedrohungsstufe festlegen** und wählen Sie eine Bedrohungsstufe aus.

Prozesse löschen

Sie können Prozesse bei Bedarf manuell aus dem Inventar löschen.

Wenn die gelöschten Prozesse jedoch auf verwalteten Geräten gefunden werden, werden die Datensätze für die Prozesse mit neuen IDs neu erstellt, sobald die Geräte Inventarinformationen aktualisieren.

1. Rufen Sie die Liste *Prozesse* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Inventar** und anschließend auf **Prozesse**.
2. Führen Sie einen der folgenden Schritte aus:
   - **Aktivieren Sie das Kontrollkästchen neben mindestens einem Prozess und wählen Sie Aktion auswählen > Löschen.**
   - **Klicken Sie auf einen Prozessnamen und dann auf der Seite** *Prozessdetails* **auf Löschen.**
3. Klicken Sie zur Bestätigung auf **Ja**.

Verwalten des Startprogramm-Inventars

Auf verwalteten Geräten erkannte Startprogramme werden im Abschnitt *Inventar* gemeldet und können dort verwaltet werden.

Auf der Startprogramm-Inventarseite können Sie Informationen über die Startprogramme, die auf verwalteten Geräten erkannt wurden, anzeigen und bearbeiten.

Zu den Startinventardetails gehören der Name des Geräts, das die Startprogramme ausführt, die Systembeschreibung sowie der letzte Benutzer.

Startprogramme können nicht erfasst werden.

Startprogrammdetails anzeigen und bearbeiten

Sie können Details zu Startprogrammen im Inventar anzeigen und bearbeiten.

1. Rufen Sie die *Detailseite für das Startprogramm* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Inventar** und anschließend auf **Startprogramme**.
   c. Klicken Sie auf den Namen eines Startprogramms.

   Die Geräte, die das Programm ausführen, sind unten auf der Seite aufgeführt.
2. Geben Sie die folgenden Informationen an:

Option	Beschreibung
Zuweisen zu Label	(Optional) Das dem Element zugeordnete Label.
Anmerkungen	Geben Sie nach Bedarf beliebige weitere Informationen ein.
Kategorie	Die Kategorie des Elements, z.B. Business, Treiber oder Sicherheit
Bedrohungsstufe	Die Bedrohungsstufe des Elements. Mögliche Bedrohungsstufen: a. Sicher b. Ziemlich sicher c. Unbekannt d. Könnte schädlich sein e. Schädlich

3. Klicken Sie auf **Speichern**.

Labels Startprogrammen hinzufügen

Fügen Sie manuelle Labels hinzu, um Startprogramme im Inventar als Gruppe zu verwalten.

1. Rufen Sie die Liste *Startprogramme* auf:

a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.

b. Klicken Sie in der linken Navigationsleiste auf **Inventar** und anschließend auf **Startprogramme**.

2. Wählen Sie **Aktion auswählen** > **Label hinzufügen**.
3. Geben Sie im Fenster *Label hinzufügen* einen Namen für das Label ein.

TIPP: Vermeiden Sie in Labelnamen die Verwendung des umgekehrten Schrägstrichs (\). Wenn Sie einen umgekehrten Schrägstrich in einem Labelnamen verwenden müssen, fügen Sie einen zweiten umgekehrten Schrägstrich hinzu (\\), damit er nicht als Befehl interpretiert wird.

4. Klicken Sie auf **Speichern**.

Startprogrammen Labels zuweisen oder Labels aus Startprogrammen entfernen

Labels können bei Bedarf Startprogrammen im Inventar zugewiesen oder entfernt werden.

1. Rufen Sie die Liste *Startprogramme* auf:

a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.

b. Klicken Sie in der linken Navigationsleiste auf **Inventar** und anschließend auf **Startprogramme**.

2. Aktivieren Sie das Kontrollkästchen neben dem Programm/den Programmen.
3. Führen Sie einen der folgenden Schritte aus:

- **Wählen Sie Aktion auswählen > Label zuweisen und anschließend das zuzuweisende Label aus.**
- **Wählen Sie Aktion auswählen > Label entfernen und anschließend das zu entfernende Label aus.**

Startprogramme kategorisieren

Sie können Startprogramme im Inventar organisieren und verwalten, indem Sie sie manuell Kategorien zuweisen.

1. Rufen Sie die Liste *Startprogramme* auf:

a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.

b. Klicken Sie in der linken Navigationsleiste auf **Inventar** und anschließend auf **Startprogramme**.

2. Aktivieren Sie das Kontrollkästchen neben dem Programm/den Programmen.
3. Wählen Sie **Aktion auswählen** > **Kategorie festlegen** und anschließend eine Kategorie aus.

Bedrohungsstufen Startprogrammen zuweisen

Sie können Startprogrammen, die unter Umständen eine Bedrohung für Geräte und Systeme darstellen, manuell eine Bedrohungsstufe zuweisen.

Mithilfe von Bedrohungsstufen können Sie die relative Sicherheit von Elementen und die Anzahl der Geräte anzeigen, auf denen diese Elemente installiert sind. Diese Informationen dienen nur Nachverfolgungszwecken. Die Appliance erzwingt basierend auf den Bedrohungsstufen keine Richtlinien.

1. Rufen Sie die Liste *Startprogramme* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Inventar** und anschließend auf **Startprogramme**.
2. Aktivieren Sie das Kontrollkästchen neben dem Programm/den Programmen.
3. Wählen Sie **Aktion auswählen** > **Bedrohungsstufe festlegen** und wählen Sie eine Bedrohungsstufe aus.

Startprogramme löschen

Sie können Startprogramme bei Bedarf manuell aus dem Inventar löschen.

Wenn die gelöschten Startprogramme jedoch auf verwalteten Geräten gefunden werden, werden die Datensätze für diese Programme mit neuen IDs neu erstellt, sobald die Geräte Inventarinformationen aktualisieren.

1. Rufen Sie die Liste *Startprogramme* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Inventar** und anschließend auf **Startprogramme**.
2. Führen Sie einen der folgenden Schritte aus:
   - **Aktivieren Sie das Kontrollkästchen neben mindestens einem Programm und wählen Sie Aktion auswählen > Löschen.**
   - **Klicken Sie auf einen Programmnamen und dann auf der Seite** *Startprogrammdetails* **auf Löschen.**
3. Klicken Sie zur Bestätigung auf **Ja**.

Verwalten des Dienstinventars

Auf verwalteten Geräten erkannte Dienste werden im Abschnitt *Inventar* gemeldet und können dort verwaltet werden.

Auf der Seite "Dienstinventar" können Sie die Dienste, die auf verwalteten Geräten ausgeführt werden, nachverfolgen.

Die Dienstdetailseiten enthalten Informationen zu Diensten, z.B. den Namen des Geräts, auf dem diese Dienste ausgeführt werden, eine Systembeschreibung und Angaben zum letzten Benutzer.

Für Dienstinventar kann keine Nutzungserfassung erfolgen.

Dienstdetails anzeigen und bearbeiten

Sie können Details zu Diensten im Inventar anzeigen und bearbeiten.

1. Rufen Sie die *Dienstdetailseite* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen

Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.

b. Klicken Sie in der linken Navigationsleiste auf **Inventar** und anschließend auf **Dienste**.

c. Klicken Sie auf den Namen eines Dienstes.

Die Geräte, die den Dienst ausführen, sind unten auf der Seite aufgeführt.

2. Geben Sie die folgenden Informationen an:

Option	Beschreibung
Zuweisen zu Label	(Optional) Das dem Element zugeordnete Label.
Anmerkungen	Geben Sie nach Bedarf beliebige weitere Informationen ein.
Kategorie	Die Kategorie des Elements, z.B. Business, Treiber oder Sicherheit
Bedrohungsstufe	Die Bedrohungsstufe des Elements. Mögliche Bedrohungsstufen: a. Sicher b. Ziemlich sicher c. Unbekannt d. Könnte schädlich sein e. Schädlich

3. Klicken Sie auf **Speichern**.

Labels Diensten hinzufügen

Fügen Sie manuelle Labels hinzu, um Dienste im Inventar als Gruppe zu verwalten.

1. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
2. Wählen Sie **Inventar** > **Dienste** aus, um die Seite *Dienste* anzuzeigen.
3. Wählen Sie **Aktion auswählen** > **Label hinzufügen**.
4. Geben Sie im Fenster *Label hinzufügen* einen Namen für das Label ein.

   TIPP: Vermeiden Sie in Labelnamen die Verwendung des umgekehrten Schrägstrichs (\). Wenn Sie einen umgekehrten Schrägstrich in einem Labelnamen verwenden müssen, fügen Sie einen zweiten umgekehrten Schrägstrich hinzu (\\), damit er nicht als Befehl interpretiert wird.

5. Klicken Sie auf **Speichern**.

Diensten Labels zuweisen oder Labels aus Diensten entfernen

Labels können bei Bedarf Diensten im Inventar zugewiesen oder entfernt werden.

1. Rufen Sie die Liste *Dienste* auf:

   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen*

aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.

b. Klicken Sie in der linken Navigationsleiste auf **Inventar** und anschließend auf **Dienste**.

2. Aktivieren Sie das Kontrollkästchen neben dem Dienst/den Diensten.
3. Führen Sie einen der folgenden Schritte aus:
   - **Wählen Sie Aktion auswählen > Label zuweisen und anschließend die zuzuweisenden Labels aus.**
   - **Wählen Sie Aktion auswählen > Label entfernen und anschließend die zu entfernenden Labels aus.**

Dienste kategorisieren

Sie können Dienste im Inventar organisieren und verwalten, indem Sie sie manuell Kategorien zuweisen.

1. Rufen Sie die Liste *Dienste* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Inventar** und anschließend auf **Dienste**.
2. Aktivieren Sie das Kontrollkästchen neben dem Dienst/den Diensten.
3. Wählen Sie **Aktion auswählen** > **Kategorie festlegen** und anschließend eine Kategorie aus.

Bedrohungsstufen Diensten zuweisen

Sie können Diensten, die unter Umständen eine Bedrohung für Geräte und Systeme darstellen, manuell eine Bedrohungsstufe zuweisen.

Mithilfe von Bedrohungsstufen können Sie die relative Sicherheit von Elementen und die Anzahl der Geräte anzeigen, auf denen diese Elemente installiert sind. Diese Informationen dienen nur Nachverfolgungszwecken. Die Appliance erzwingt basierend auf den Bedrohungsstufen keine Richtlinien.

1. Rufen Sie die Liste *Dienste* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Inventar** und anschließend auf **Dienste**.
2. Aktivieren Sie das Kontrollkästchen neben dem Dienst/den Diensten.
3. Wählen Sie **Aktion auswählen** > **Bedrohungsstufe festlegen** und wählen Sie eine Bedrohungsstufe aus.

Dienste löschen

Sie können Dienste bei Bedarf manuell aus dem Inventar löschen.

Wenn die gelöschten Dienste jedoch auf verwalteten Geräten gefunden werden, werden die Datensätze für die Dienste mit neuen IDs neu erstellt, sobald die Geräte Inventarinformationen aktualisieren.

1. Rufen Sie die Liste *Dienste* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen*

aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.

b. Klicken Sie in der linken Navigationsleiste auf **Inventar** und anschließend auf **Dienste**.

2. Aktivieren Sie das Kontrollkästchen neben dem Dienst/den Diensten.
3. Führen Sie einen der folgenden Schritte aus:
   - **Aktivieren Sie das Kontrollkästchen neben mindestens einem Programm und wählen Sie Aktion auswählen > Löschen.**
   - **Klicken Sie auf einen Programmnamen und dann auf der Seite** *Startprogrammdetails* **auf Löschen.**
4. Klicken Sie zur Bestätigung auf **Ja**.

Erstellen benutzerdefinierter Inventarregeln

Mithilfe von Regeln für benutzerdefinierte Inventarisierung können ausführliche Informationen zu Inventarelementen erfasst werden.

Informationen zur Verwendung der Inventarkomponente finden Sie unter Verwalten von Anwendungen auf der Seite "Software".

Informationen zu benutzerdefinierten Inventarregeln

Mit Regeln für benutzerdefinierte Inventarisierung können Sie bei der Inventarerfassung benutzerdefinierte Informationen erfassen.

Regeln für benutzerdefinierte Inventarisierung sind hilfreich beim:

- Verwalten von Software, die unter Windows nicht im Bereich *Programme hinzufügen/entfernen* aufgeführt ist.
- Verwalten von Softwareversionen mit gleichen Einträgen im Bereich *Programme hinzufügen/entfernen* von Windows, insbesondere mit falschen oder unvollständigen Informationen für die *Anzeigeversion*.
- Erfassen benutzerdefinierter Details für Berichte.
- Erstellen von Bereitstellungsregeln, Skripten und Berichten auf der Grundlage einer Anwendung oder eines Werts, die bzw. der nicht durch den KACE Agent gemeldet wird.

Arten von benutzerdefinierten Inventarregeln

Mithilfe von Regeln für benutzerdefinierte Inventarisierung werden Registrierungsschlüssel und -einträge, Programme, Dateien, Skripte, Umgebungsvariablen, Systemeigenschaften und die Ausgabe von Befehlen getestet oder deren Werte abgerufen.

Es gibt zwei Arten von Regeln für benutzerdefinierte Inventarisierung:

- **Bedingungsregeln**: Mit diesen Regeln wird getestet, ob Bedingungen auf Geräten vorhanden sind. Wenn eine Regel vorhanden ist, meldet der KACE Agent das Element als ein installiertes Programm. Ist keine Regel vorhanden, wird das Element nicht als installiertes Programm angezeigt.
- **Werterückgabe-Regeln**: Mit diesen Regeln werden Daten von Geräten abgerufen. Ist der Wert vorhanden, meldet der KACE Agent das Element als installiertes Programm und legt ein entsprechendes *Feld für benutzerdefinierte Inventarisierung* fest.

Regeln für benutzerdefinierte Inventarisierung erstellen

Sie können benutzerdefinierte Anwendungen und Regeln für benutzerdefinierte Inventarisierung für diese Anwendungen erstellen, um Informationen über die Anwendungen von den von den verwalteten Geräten zu sammeln.

1. Rufen Sie die *Softwaredetailseite* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Inventar** und anschließend auf **Software**.
   c. Wählen Sie **Aktion auswählen** > **Neu**.
2. Machen Sie allgemeine Angaben: *Name*, *Version* und *Herausgeber*.

   Stellen Sie für die ordnungsgemäße nachgelagerte Berichterstellung sicher, dass diese Informationen im gesamten Softwareinventar einheitlich eingegeben werden.
3. Geben Sie die folgenden Informationen an:

Option	Beschreibung
Zuweisen zu Label	(Optional) Das Label, das dem Element zugewiesen wurde.
Anmerkungen	Geben Sie nach Bedarf beliebige weitere Informationen ein.
Unterstützte Betriebssysteme	Das Betriebssystem, auf dem die Anwendung ausgeführt wird. Die Bereitstellung der Anwendungen erfolgt nur auf Geräten mit den ausgewählten Betriebssystemen.
Regel für benutzerdefinierte Inventarisierung	(Optional) Die auf die Anwendung anzuwendenden Regeln für benutzerdefinierte Inventarisierung. Mithilfe von Regeln für benutzerdefinierte Inventarisierung können Sie Anwendungen und andere Elemente auf einem Gerät erkennen und Details für die Berichterstellung erfassen. So prüft die Appliance beispielsweise vor der Bereitstellung einer Anwendung zunächst, ob die Anwendung auf dem Gerät bereits vorhanden ist. Manchmal werden installierte Programme jedoch nicht unter *Software* oder in den Standardbereichen der Registrierung registriert. In diesen Fällen

Option	Beschreibung

	kann die Appliance die Software ohne zusätzliche Informationen vom Administrator möglicherweise nicht erkennen. Deshalb wiederholt die Appliance die Installation unter Umständen jedes Mal, wenn das Gerät eine Verbindung herstellt. Dies lässt sich mithilfe von Regeln für benutzerdefinierte Inventarisierung verhindern.
	Die folgende Regel überprüft, ob die auf einem Gerät installierte Version von Network Associates VirusScan neuer ist als eine angegebene Version, bevor diese bereitgestellt wird.
	`RegistryValueGreaterThan(HKEY_LOCAL_MACHINE\Software\Network Associates\TVD\`
	
	`Network Associates\TVD\Shared Components\VirusScanEngine\4.0.xx,szDatVersion,4.0.44)`

4. Klicken Sie neben *Datei hochladen und verknüpfen* auf **Datei auswählen**, um nach einer Datei zu suchen. Klicken Sie anschließend auf **Öffnen** oder **Auswählen**.

   Zur Verteilung von Anwendungen mithilfe verwalteter Installationen oder Dateisynchronisierungen müssen die jeweiligen Anwendungsdateien mit der Anwendung verknüpft werden.
5. Damit die Datei nicht in die Replikationsfreigabe kopiert wird, wählen Sie **Zugehörige Datei nicht replizieren** aus. Diese Einstellung ist bei großen Dateien sinnvoll, die die Benutzer nicht von Replikationsfreigaben installieren sollen (etwa bei Software-Suites).
6. **Optional**: Wählen Sie eine *Kategorie* und eine *Bedrohungsstufe* für die Software aus.
7. Klicken Sie auf **Speichern**.

Verwandte Themen

Informationen zu den Labels

Abrufen von Werten von einem Gerät (Benutzerdefiniertes Inventarfeld)

Verwenden von Bedrohungsstufen und Kategorien für Software

Regeln für benutzerdefinierte Inventarisierung implementieren

Der KACE Agent erhält die neuen Regeln für benutzerdefinierte Inventarisierung bei der ersten Geräteinventur nach dem Erstellen der Regeln. Während dieser ersten Inventur führt der Agent die neuen Regeln aus und meldet die Ergebnisse an die Appliance.

Der Agent führt alle Regeln sowie alle übrigen für diese Sitzung geplanten Prozesse aus. Daher dauert es nach der ersten Inventur unter Umständen einige Minuten, bis alle Regeln und Prozesse ausgeführt sind und die Ergebnisse zurückgegeben werden.

Die Ergebnisse werden nach der Rückmeldung durch den Agenten auf der Seite mit den Gerätedetails unter *Software* in *Installierte Programme* und *Feldern für benutzerdefinierte Inventarisierung* angezeigt.

HINWEIS: Die Anwendungen mit Werterückgabe-Regeln, durch die ein *Feld für benutzerdefinierte Inventarisierung* festgelegt wird, werden ebenfalls als installierte Programme angezeigt.

Sollten die Ergebnisse nicht Ihren Erwartungen entsprechen, vergewissern Sie sich, dass für das Gerät kürzlich eine Inventur durchgeführt wurde. Die Inventarzeit wird auf der Seite mit den Gerätedetails im Feld *Letztes Inventar* angezeigt.

Syntax für Regeln für benutzerdefinierte Inventarisierung

In Regeln für benutzerdefinierte Inventarisierung muss für Funktionsnamen und Argumente die korrekte Syntax verwendet werden.

Für Bedingungs- und Werterückgabe-Regeln gilt folgende Syntax:

```
functionName(argument,argument,...)
```

Detaillierte Informationen zu Funktionen und deren Argumenten finden Sie unter:

- Überprüfen von Bedingungen (Bedingungsregeln)
- Abrufen von Werten von einem Gerät (Benutzerdefiniertes Inventarfeld)
- Zuordnen von Dateinamen zu regulären Ausdrücken

Funktionen – Syntax

Geben Sie den **Funktionsnamen**, eine öffnende Klammer, die gewünschten Argumente und eine schließende Klammer ein. Zwischen dem Namen der Funktion und der öffnenden Klammer dürfen sich keine Leerzeichen befinden.

Argumente – Syntax

Geben Sie die **argument**-Syntax für alle Regeln mit Ausnahme von `command` und `regex` (regulärer Ausdruck) wie folgt ein:

- Trennen Sie die Argumente durch Kommas voneinander.
- Kommas sind an keiner anderen Stelle der Zeichenfolge zulässig (Ausnahmen finden Sie unter Kommas und Klammern als Werte in einer Regel).
- Fügen Sie keine einfachen oder doppelten Anführungszeichen hinzu.
- Leerzeichen vor und nach jedem Argument werden gelöscht.

Beispielsweise sind die folgenden Syntaxzeilen identisch:

```
RegistryValueEquals(HKEY_LOCAL_MACHINE\SOFTWARE\Mozilla\Mozilla Firefox, CurrentVersion, 78.0.2)
RegistryValueEquals(HKEY_LOCAL_MACHINE\SOFTWARE\Mozilla\Mozilla Firefox,CurrentVersion,78.0.2)
```

Kommas und Klammern als Werte in einer Regel

Wenn in einer Regel Kommas oder öffnende/schließende Klammern als Werte verwendet werden, müssen diese als {{comma}} (Komma). {{op}} (öffnende Klammer) und {{cp}} (schließende Klammer) angegeben werden.

- In Argumenten, in denen Kommas als Teil des Parameterwerts angegeben werden müssen, muss das Komma als "{{comma}}" angegeben werden. Hiervon ausgenommen ist nur das letzte Argument in der Funktion.

  Möchte der Benutzer also beispielsweise einen Test für den Registrierungswert mit dem Wertnamen "**test,value**" durchführen, muss er in diesem Fall die Escape-Sequenz für das Komma angeben, da es sich bei dem Namen des Registrierungswerts nicht um das letzte Argument in der Funktion für benutzerdefinierte Inventarisierung (Custom Inventory, CI) handelt.

  `RegistryValueEquals(HKEY_LOCAL_MACHINE\SOFTWARE\TestSoft,` **test{{comma}}value**`, HelloWorld)`

  Möchte der Benutzer einen Test für einen Registrierungswert mit enthaltenem Komma durchführen, muss keine Escape-Sequenz verwendet werden, da es sich bei dem Wert um das letzte Argument in der Funktion für benutzerdefinierte Inventarisierung handelt. Mit der folgenden Funktion für die benutzerdefinierte Inventarisierung wird getestet, ob der Registrierungswert "HKLM\SOFTWARE\TestSoft \test1" mit dem Wert **2,4** übereinstimmt.

  `RegistryValueEquals(HKEY_LOCAL_MACHINE\SOFTWARE\TestSoft,test1,`**2,4**`)`

  Enthält die Funktion für benutzerdefinierte Inventarisierung lediglich einen einzelnen Parameter, wird alles zwischen den Klammern als Wert für das Argument behandelt. In diesem Fall muss für Kommas keine

Escape-Sequenz verwendet werden und die Kommas werden als Teil des Arguments für die Funktion für benutzerdefinierte Inventarisierung betrachtet.

`ShellCommandTextReturn(`**wmic MEMORYCHIP get BankLabel,Capacity,description,manufacturer**`)`

- Für eine öffnende Klammer ohne Gegenstück muss die Escape-Sequenz **{{op}}** verwendet werden. Wenn der Parser die Argumente für die Funktion in Token umwandelt, wird die Anzahl öffnender und schließender Klammern gezählt, um das Ende der Funktion und des Arguments zu ermitteln. Eine öffnende Klammer ohne Gegenstück würde die Zählung durcheinander bringen und dazu führen, dass der Argumentwert nicht korrekt analysiert wird. Wird in einem Argumentwert eine öffnende Klammer benötigt, muss diese als **{{op}}** angegeben werden.

  Möchte der Benutzer also beispielsweise die Zeichenfolge "**Hello (World**" ausgeben, muss die Funktion für benutzerdefiniertes Inventar wie folgt aussehen:

  `ShellCommandTextReturn(echo` **Hello {{op}} World**`)`

- Für eine schließende Klammer ohne Gegenstück muss die Escape-Sequenz **{{cp}}** verwendet werden.

  Wenn der Parser die Argumente für die Funktion in Token umwandelt, wird die Anzahl öffnender und schließender Klammern gezählt, um das Ende der Funktion (die letzte schließende Klammer mit Gegenstück) zu ermitteln. Enthält jedoch der eigentlich Argumentwert eine schließende Klammer ohne Gegenstück, entsteht für den Parser der Eindruck, die Klammer sei das Ende der Funktion und der Argumentwert wird abgeschnitten.

  Wird in einem Argumentwert eine schließende Klammer benötigt, muss diese als **{{cp}}** angegeben werden.

  Möchte der Benutzer also beispielsweise die Zeichenfolge "**Hello) World**" ausgeben, muss die Funktion für benutzerdefiniertes Inventar wie folgt aussehen:

  `ShellCommandTextReturn(echo` **Hello {{cp}} World**`)`

Überprüfen von Bedingungen (Bedingungsregeln)

Sie können Regeln für benutzerdefinierte Inventarisierung erstellen, um zu ermitteln, ob eine Anwendung installiert ist (wahr/falsch).

Wenn bei Verwendung einer Bedingungsregel "Wahr" zurückgegeben wird, wird der Anzeigename (Titel) der benutzerdefinierten Anwendung im Bereich *Software: Installierte Programme* der Seite *Gerätedetail* im Abschnitt *Inventar* angezeigt.

In den folgenden Abschnitten werden die Regeln beschrieben, mit denen Bedingungen überprüft werden:

- Referenz für Bedingungsregeln
- Überprüfen, ob eine Bedingung vorhanden ist (Exists-Regeln)
- Auswerten von Geäteeinstellungen (Equals-Regeln)
- Vergleichen von Gerätewerten (GreaterThan- und LessThan-Regeln)
- Testen mehrerer Bedingungen

Trifft die Regel nicht zu ("Falsch"), wird die Anwendung nicht unter *Installierte Programme* in den Inventardetails des Geräts angezeigt.

TIPP: Eine Liste der Geräte, auf denen das Element installiert ist, wird auch unter *Inventar* > *Software* > *Benutzerdefiniertes_Element: Details* angezeigt.

Referenz für Bedingungsregeln

In der folgenden Tabelle wird beschrieben, welche Datentypen für den Vergleich verwendet werden können.

Für Vergleichsfunktionen unterstützte Datentypen

Bedingungsregel	Für Vergleichsfunktionen unterstützte Datentypen `Equals`, `GreaterThan`, `LessThan`
`EnvironmentVariable`	DATE, NUMBER, TEXT
`FileInfo`	DATE, NUMBER, TEXT
`FilenamesMatchingRegex`	NUMBER
`FileVersion`	TEXT
`PlistValue`	NUMBER, TEXT
`ProductVersion`	TEXT
`RegistryValue`	TEXT

In der folgenden Tabelle wird die Vorgehensweise zum Ausführen von Vergleichen erläutert.

Ausführen von Vergleichen

Datentyp	Überlegungen
DATE	• Vor der Auswertung werden Zielwerte als Datum mithilfe der gleichen Regeln wie in der DateTime-PHP-Klasse analysiert und anschließend für die Verwendung des folgenden Formats normalisiert: `MM/TT/JJJJ HH:MM:SS` • Der Zeitstempel in der Appliance-Datenbank verwendet das 24-Stunden-Format (0 – 24 Stunden). • Der Zeitstempel in der Appliance-Datenbank ist in koordinierter Weltzeit (UTC, Coordinated Universal Time) angegeben, sodass er für alle Geräte unabhängig von den entsprechenden Zeitzonen normalisiert wird. • Enthält der Zielwert nur ein Datum, wird ein Zeitstempel hinzugefügt, der auf Mitternacht für UTC basiert.
NUMBER	• Nur ganze Zahlen werden bewertet. • Falls ein Zielwert andere Zeichen (Buchstaben, Satzzeichen usw.) enthält, werden nur die Zahlen vor dem ersten Zeichen bewertet.

Datentyp	Überlegungen
	Beispiel: Lautet der Zielwert "52a1" wird nur "52" bewertet. • Es werden nur Zahlen bis zum maximalen positiven ganzzahligen 32-Bit-Wert (2.147.483.647) unterstützt.
TEXT	• Werte werden wortwörtlich ohne mögliche Formatierungsänderungen (wie es beispielsweise bei den Datentypen DATE und NUMBER der Fall sein kann) bewertet. • Textfolgen müssen in lexikografischer Reihenfolge bewertet werden. • Die bewerteten Zeichenfolgen dürfen Kommas enthalten. Es sind keine Escape-Zeichen erforderlich.

Die folgende Tabelle enthält eine Liste der verfügbaren Bedingungsregeln mit Links zu näheren Informationen dazu, wie die Argumente angegeben werden:

Referenz für Bedingungsregeln

Syntax	Windows	RHEL	OS X	Beschreibung
`DirectoryExists (path)`	X	X	X	Überprüft, ob im angegebenen Pfad auf dem Gerät ein Verzeichnis vorhanden ist.
`FileExists (path)`	X	X	X	Überprüft, ob im angegebenen Pfad auf dem Gerät eine Datei vorhanden ist. Geben Sie im Pfad den Namen der Datei und die Erweiterung an.
`FileVersionEqualS (path, version)`	X			Überprüft, ob die Eigenschaft **Version > Dateiversion** der im Pfad angegebenen Datei dem eingegebenen TEXT-Wert entspricht.
`FileVersionLessThan (path, version)`	X			Überprüft, ob die Eigenschaft **Version > Dateiversion** der als Pfad angegebenen

Syntax	Windows	RHEL	OS X	Beschreibung
				Datei niedriger als der eingegebene TEXT-Wert ist.
`FileVersionGreaterThan (path, version)`	X			Überprüft, ob die Eigenschaft **Version > Dateiversion** der angegebenen Datei höher als der eingegebene TEXT-Wert ist.
`ProductVersionEquals (path, version)`	X			Überprüft, ob die Eigenschaft **Version > Produktversion** der angegebenen ausführbaren Datei oder Installationsdatei dem eingegebenen TEXT-Wert entspricht.
`ProductVersionLessThan (path, version)`	X			Überprüft, ob die Eigenschaft **Version > Produktversion** der angegebenen ausführbaren Datei oder Installationsdatei niedriger als der eingegebene TEXT-Wert ist.
`ProductVersionGreaterThan (path, version)`	X			Überprüft, ob die Eigenschaft **Version > Produktversion** der angegebenen ausführbaren Datei oder Installationsdatei höher als der eingegebene TEXT-Wert ist.
`FileInfoGreaterThan (fullpath, attribute, type, value)`	X	X	X	Überprüft, ob der Wert für die Eigenschaft **Dateiinfo** der von Ihnen angegebenen ausführbaren Datei bzw.

Syntax	Windows	RHEL	OS X	Beschreibung
				Installationsdatei größer ist als der von Ihnen eingegebene Wert.
`FileInfoLessThan (fullpath, attribute, type, value)`	X	X	X	Überprüft, ob der Wert für die Eigenschaft **Dateiinfo** der von Ihnen angegebenen ausführbaren Datei bzw. Installationsdatei kleiner ist als der von Ihnen eingegebene Wert.
`FileInfoEquals (fullpath, attribute, type, value)`	X	X	X	Überprüft, ob die attribute-Eigenschaft der von Ihnen angegebenen ausführbaren Datei bzw. Installationsdatei dem von Ihnen eingegebenen Wert entspricht.
`RegistryKeyExists (registryPath)`	X			Überprüft, ob ein Registrierungsschlüssel vorhanden ist.
`RegistryValueEquals (registryPath, valueName, value)`	X			Überprüft, ob ein Registrierungsschlüssel genau dem von Ihnen eingegebenen Wert entspricht. Der Wert wird als TEXT verglichen.
`RegistryValueLessThan (registryPath, valueName, value)`	X			Überprüft, ob ein Registrierungseintrag niedriger ist als der von Ihnen eingegebene Wert. Der Wert ist ein TEXT-Wert.
`RegistryValueGreaterThan (registryPath, valueName, value)`	X			Überprüft, ob ein Registrierungseintrag höher ist als der von Ihnen eingegebene Wert.

Syntax	Windows	RHEL	OS X	Beschreibung
				Der Wert ist ein TEXT-Wert.
`EnvironmentalVariableExists (var)`	X	X	X	Überprüft, ob eine Umgebungsvariable mit dem von Ihnen angegebenen Namen vorhanden ist.
`EnvironmentalVariableGreaterThan (var, type, value)`	X	X	X	Überprüft, ob die Definition der Umgebungsvariablen höher ist als der von Ihnen eingegebene Wert. Alle drei Typen sind gültig: TEXT, DATE (im vollständigen Format `mm/tt/jjjj hh:mm:ss`) und NUMBER.
`EnvironmentalVariableLessThan (var, type, value)`	X	X	X	Überprüft, ob die Definition der Umgebungsvariablen niedriger ist als der von Ihnen eingegebene Wert. Alle drei Typen sind gültig: TEXT, DATE (im vollständigen Format `mm/tt/jjjj hh:mm:ss`) und NUMBER.
`EnvironmentalVariableEquals (var, type, value)`	X	X	X	Überprüft, ob die Definition der Umgebungsvariablen genau dem von Ihnen eingegebenen Wert entspricht. Alle drei Typen sind gültig: TEXT, DATE (im vollständigen Format `mm/tt/jjjj hh:mm:ss`) und NUMBER.
`PlistValueExists (fullpath, entry)`			X	Überprüft, ob ein benannter Wert in einer PLIST-Datei vorhanden ist.

Syntax	Windows	RHEL	OS X	Beschreibung
`PlistValueGreaterThan (fullpath, entry, type, value)`			X	Überprüft, ob der benannte Wert ein NUMBER- oder TEXT-Wert und höher als der angegebene Wert ist.
`PlistValueLessThan (fullpath, entry, type, value)`			X	Überprüft, ob der benannte Wert ein NUMBER- oder TEXT-Wert und niedriger als der angegebene Wert ist.
`PlistValueEquals (fullpath, entry, type, value)`			X	Überprüft, ob der benannte Wert ein NUMBER- oder TEXT-Wert ist und genau dem angegebenen Wert entspricht.

Informationen zu `Equals`, `GreaterThan` und `LessThan` für `FilenamesMatchingRegex` finden Sie unter Referenz zu Regeln mit regulären Ausdrücken.

Überprüfen, ob eine Bedingung vorhanden ist (Exists-Regeln)

Mit Regeln, deren Name mit **Exists** endet, wird überprüft, ob eine Datei, ein Verzeichnis, ein Registrierungsschlüssel oder ein anderes Element vorhanden ist. Wenn der KACE Agent das Element auf dem Gerät ermittelt, wird die Regel als "Wahr" ausgewertet und das Element als installiertes Programm angezeigt.

Verwenden Sie eine der folgenden Exists-Regeln:

- `DirectoryExists (path)`
- `FileExists (path)`
- `RegistryKeyExists (registryPath)`
- `EnvironmentalVariableExists (var)`
- `PlistValueExists (fullpath, entry)`
- `FilenameMatchingRegexExist (fullpath, regex)`

Beispiel: Überprüfen, ob ein Verzeichnis (Ordner) vorhanden ist

Mit dem folgenden Beispiel wird getestet, ob das Windows Verzeichnis auf dem Gerät vorhanden ist:

```
DirectoryExists(C:\WINDOWS\)
```

Beispiel: Überprüfen, ob eine Datei vorhanden ist

HINWEIS: Mit dem folgenden Beispiel wird überprüft, ob die ausführbare Notepad-Datei auf dem Gerät vorhanden ist:

```
FileExists(C:\WINDOWS\notepad.exe)
```

Auswerten von Geäteeinstellungen (Equals-Regeln)

Mit Regeln, deren Name mit **Equals** endet, werden die Werte auf dem Gerät mit den Werten verglichen, die Sie in der Regel angeben. Die Regeln sind zutreffend ("Wahr"), wenn die Werte genau übereinstimmen.

Mithilfe von Regeln, in denen Argumente mit festgelegten Datentypen verwendet werden, können nur Werte desselben Typs verglichen werden.

Verwenden Sie eine der folgenden Equals-Regeln:

- `FileVersionEquals (path, version)`
- `ProductVersionEquals (path, version)`
- `FileInfoEquals (fullpath, attribute, type, value)`
- `RegistryValueEquals (registryPath, valueName, value)`
- `EnvironmentalVariableEquals (var, type, value)`
- `PlistValueEquals (fullpath, entry, type, value)`
- `FilenameMatchingRegexEqual (fullpath, regex, value)`

Beispiel: Testen der Einstellung JAVA_HOME

So überprüfen Sie, ob die Einstellung für JAVA_HOME C:\Program Files\Java\jdk1.6.0_02 ist:

```
EnvironmentVariableEquals(JAVA_HOME, TEXT, C:\Program Files\Java\jdk1.6.0_02)
```

Beispiel: Testen der Einstellung des McAfee®-Registrierungseintrags

So überprüfen Sie, ob für die Einstellung das Datumsformat im Eintrag verwendet wird

```
RegistryValueEquals(HKEY_LOCAL_MACHINE\Software\McAfee\AVEngine, AVDatDate, 2014/03/01)
```

Beispiel: Erkennen von Windows XP Service Pack 1

Windows XP Service Pack 1 wird nur für Geräte, auf denen ursprünglich SP1 ausgeführt wurde und die dann auf SP1 heraufgestuft wurden, unter *Software* angezeigt. Im standardmäßigen Anwendungsinventar für dieses Element sind keine Geräte erfasst, auf denen bereits SP1 ausgeführt wird, da für diese Geräte ursprünglich ein Image auf SP1-Ebene erstellt wurde.

Erstellen Sie die folgende Regel für benutzerdefinierte Inventarisierung für eine benutzerdefinierte Anwendung, wenn Sie die Appliance zur Bereitstellung von Windows 7 Service Pack 1 einsetzen:

```
RegistryValueEquals(HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\
CurrentVersion,CSDVersion,Service Pack 2)
```

Sie können dann Geräte ausschließen, auf denen dieses Element installiert ist, um zu verhindern, dass die Appliance versucht, SP2 auf Geräten bereitzustellen, die sich bereits auf dieser Stufe befinden (d. h. Geräte mit SP1, für die ein Upgrade durchgeführt wurde, sowie Geräte, deren Images ursprünglich mit SP2 erfasst wurden).

Vergleichen von Gerätewerten (GreaterThan- und LessThan-Regeln)

Mit Funktionen, deren Namen auf **GreaterThan** und **LessThan** enden, werden nur die unter Table 24 aufgeführten Werte verglichen.

Verwenden Sie eine der folgenden Regeln vom Typ "GreaterThan" und "Less Than":

- `FileVersionGreaterThan (path, version)` und `FileVersionLessThan (path, version)`
- `ProductVersionGreaterThan (path, version)` und `ProductVersionLessThan (path, version)`
- `FileInfoGreaterThan (fullpath, attribute, type, value)` und `FileInfoLessThan (fullpath, attribute, type, value)`
- `RegistryValueGreaterThan (registryPath, valueName, value)` und `RegistryValueLessThan (registryPath, valueName, value)`
- `EnvironmentalVariableGreaterThan (var, type, value)` und `EnvironmentalVariableLessThan (var, type, value)`
- `PlistValueGreaterThan (fullpath, entry, type, value)` und `PlistValueLessThan (fullpath, entry, type, value)`
- `FilenameMatchingRegexGreaterThan (fullpath, regex, value)` und `FilenameMatchingRegexLessThan (fullpath, regex, value)`

Beispiel: Testen, ob die Produktversion höher ist

So überprüfen Sie, ob die Produktversion höher ist als eine bestimmte Nummer:

```
ProductVersionGreaterThan(C:\Program Files\Mozilla Firefox\firefox.exe, 78)
```

Geben Sie Folgendes ein, um zu überprüfen, ob die Produktversion gleich oder höher einer bestimmten Version ist:

```
ProductVersionEquals(C:\Program Files\Mozilla Firefox\firefox.exe, 78)
OR ProductVersionGreaterThan(C:\Program Files\Mozilla Firefox\firefox.exe,
 78)
```

Beispiel: Testen, ob eine Produktversion innerhalb eines bestimmten Bereichs liegt

Zum Testen, ob sich die Produktversion innerhalb eines bestimmten Bereichs befindet, kombinieren Sie Less Than- und Greater Than-Regeln:

```
ProductVersionGreaterThan(C:\Program Files\Mozilla Firefox\firefox.exe, 77)
 AND ProductVersionLessThan(C:\Program Files\Mozilla Firefox\firefox.exe, 79)
```

WICHTIG: Geben Sie Regeln nicht in separate Zeilen ein. Trennen Sie die Regeln nur durch ein Leerzeichen. Wenn sich Regeln in separaten Zeilen befinden, wird dadurch die Verbindungsregel außer Kraft gesetzt.

Testen mehrerer Bedingungen

Sie können Regeln mit den Operatoren UND oder ODER verknüpfen, um zu testen, ob mehrere Bedingungen zutreffen.

HINWEIS: Die Verwendung beider Operatoren (UND und ODER) in der gleichen Regel für benutzerdefinierte Inventarisierung wird nicht unterstützt. Richten Sie getrennte Anwendungen ein.

Durch die Verknüpfung von Bedingungsregeln werden folgende Ergebnisse erzielt:

- Operator UND: Alle Regeln müssen zutreffen ("Wahr" sein), damit die Ergebnisse ebenfalls zutreffend ("Wahr") sind und die Anwendung als installiertes Programm gemeldet wird.
- Operator ODER: Nur eine Regel muss zutreffen ("Wahr" sein), damit die Anwendung als installiertes Programm gemeldet wird.

WICHTIG: Geben Sie Regeln nicht in separate Zeilen ein. Trennen Sie die Regeln nur durch ein Leerzeichen. Wenn sich Regeln in separaten Zeilen befinden, wird dadurch die Verbindungsregel außer Kraft gesetzt.

Überprüfen, ob mehrere Bedingungen zutreffen (UND)

Verwenden Sie den Operator UND, um Bedingungsregeln im Feld für benutzerdefinierte Inventarisierung zu verknüpfen, wenn das Element nur dann als installiertes Programm gemeldet werden soll, wenn alle Regeln zutreffen ("Wahr" sind).

Verknüpfen Sie im *Feld für benutzerdefinierte Inventarisierung* Regeln mithilfe der folgenden Syntax:

```
Funktion
(Argumente ...
) AND Funktion
(Argumente
) AND ...
```

Trennen Sie die Bedingungsanweisung durch Leerzeichen vom Operator.

Beispiel: Überprüfen, ob ein Registrierungsschlüssel vorhanden ist, und Vergleichen von Werten

Zum Überprüfen, ob ein Registrierungsschlüssel und ein Registrierungseintragswert auf einem Windows Gerät vorhanden sind, kombinieren Sie die Regeln wie folgt mit dem Operator AND:

```
RegistryKeyExists(registryPath
) AND RegistryValueEquals(registryPath, valueName, value)
```

Überprüfen, ob eine Bedingung zutrifft (ODER)

Wenn Sie Regeln mit dem Operator `ODER` verknüpfen und eine der Regeln im *Feld für benutzerdefinierte Inventarisierung* zutrifft ("Wahr" ist), wird die Anwendung in der Liste *Installierte Programme* des Geräts angezeigt.

Verknüpfen Sie die Regeln im *Feld für benutzerdefinierte Inventarisierung* mithilfe der folgenden Syntax:

```
Funktion
(Argumente
) OR Funktion
(Argumente
) OR ...
```

Trennen Sie die Funktionsanweisungen und den Operator mithilfe eines Leerzeichens voneinander.

Beispiel: Überprüfen eines Registrierungswerts

So überprüfen Sie, ob ein Registrierungswert einen bestimmten Wert oder einen anderen Wert aufweist:

```
RegistryValueEquals(registryPath, valueName, value) OR
RegistryValueEquals(registryPath, valueName, value)
```

TIPP: Verwenden Sie zur Angabe eines Bereichs die Regeln `RegistryValueGreaterThan` und `RegistryValueLessThan` und verknüpfen Sie sie mit dem Operator `AND`.

Abrufen von Werten von einem Gerät (Benutzerdefiniertes Inventarfeld)

Mit Regeln, die auf **ValueReturn** enden, können Informationen vom Gerät abgerufen werden. Diese Regeln ermöglichen das Abrufen von Informationen, die der KACE Agent normalerweise nicht erfasst.

Die zurückgegebenen Werte werden mit dem Anzeigenamen der benutzerdefinierten Anwendung (Titel) festgelegt. Die wird auf der Seite *Gerätedetails* unter *Software* in den Feldern *Installierte Programme* und *Felder für benutzerdefinierte Inventarisierung* angezeigt.

Verwenden Sie die Werte des Felds für benutzerdefinierte Inventarisierung für die Verwaltung von Installationen sowie zur Verteilung von Software und Berichten, dem Filter *Anzeigen nach* und Smart Label-Suchkriterien oder anderer Prozesse, die mit einer automatisch erkannten Einstellung durchgeführt werden können.

In diesem Abschnitt werden die folgenden Themen behandelt:

- Referenz für Werterückgabe-Regeln
- Abrufen von Registrierungsschlüsselwerten
- Abrufen der Befehlsausgabe
- Abrufen von PLIST-Werten
- Abrufen mehrerer Werte

Referenz für Werterückgabe-Regeln

Die folgende Tabelle enthält alle verfügbaren Werterückgabe-Regeln, mit denen Sie ein *Feld für benutzerdefinierte Inventarisierung* festlegen können:

Syntax	Windows	RHEL	OS X	Beschreibung
`RegistryValueReturn (registryPath, valueName, type)`	X			Gibt den Wert eines Registrierungseintrags zurück und legt den von Ihnen angegebenen Datentyp fest.
`EnvironmentalVariableReturn (var, type)` Angeben von Umgebungs- oder Benutzervariablen	X	X	X	Gibt den Wert einer Umgebungsvariable zurück und legt den von Ihnen angegebenen Datentyp fest.
`FileInfoReturn (path, attribute, type)`	X	X	X	Gibt den Wert eines Dateiattributs zurück. Gültige Typen finden Sie unter Definieren von Regelargumenten.
`ShellCommandTextReturn (command)`	X	X	X	Gibt die Befehlsausgabe zurück und legt den Datentyp auf TEXT fest.
`ShellCommandDateReturn (command)`	X	X	X	Gibt die Befehlsausgabe zurück und legt den Datentyp auf DATE fest.
`ShellCommandNumberReturn (command)`	X	X	X	Gibt die Befehlsausgabe zurück und legt den Datentyp auf NUMBER fest.

Syntax	Windows	RHEL	OS X	Beschreibung
`PlistValueReturn (fullpath, entry, type)`			X	Gibt den Wert des Schlüssels PLIST zurück und legt den Datentyp auf TEXT, NUMBER oder DATE fest.

Abrufen von Dateiinformationswerten

Mit der Regel `FileInfoReturn` können Sie das *Feld für benutzerdefinierte Inventarisierung* auf jedes der Attribute für Windows Dateiinformationen festlegen.

Beispiel: Version von Mozilla Firefox abrufen

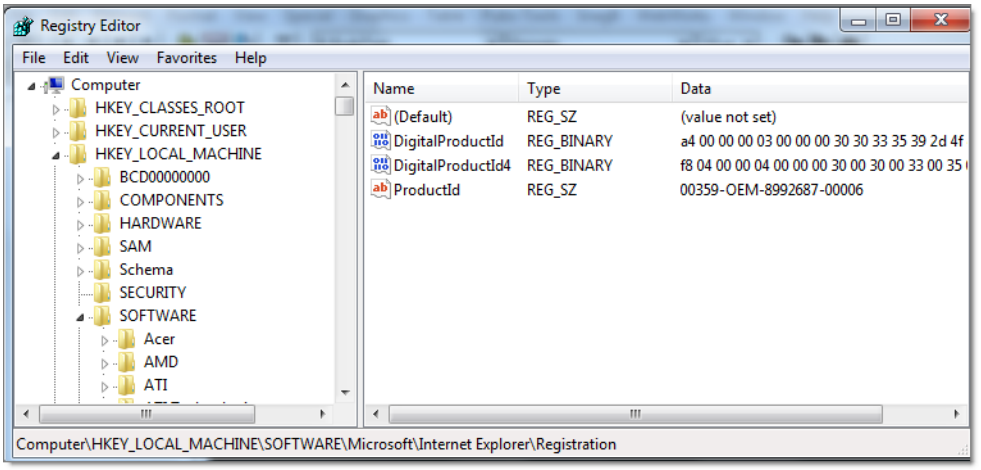
Mit dem folgenden Beispiel wird das *Feld für benutzerdefinierte Inventarisierung* für die Produktversion von Mozilla Firefox als NUMBER-Wert festgelegt.

Geben Sie im *Feld für benutzerdefinierte Inventarisierung* Folgendes ein:

```
FileInfoReturn(C:\Program Files\Mozilla Firefox\firefox.exe,CurrentVersion,TEXT)
```

Abrufen von Registrierungsschlüsselwerten

Sie können das *Feld für benutzerdefinierte Inventarisierung* auf einen Registrierungsschlüssel festlegen. Verwenden Sie hierzu die Regel `RegistryValueReturn`. Dabei ist `registryPath` (auf der linken Seite) der Pfad zu dem Eintrag und `valueName` (auf der rechten Seite) der Schlüssel, der zurückgegeben werden soll.



Beispiel: CurrentVersion-Schlüssel für Mozilla FireFox abrufen

So legen Sie den CurrentVersion-Registrierungsschlüssel als *Feld für benutzerdefinierte Inventarisierung* fest:

```
RegistryValueReturn (HKEY_LOCAL_MACHINE\SOFTWARE\Mozilla\Mozilla Firefox\CurrentVersion, TEXT
```

Abrufen der Befehlsausgabe

Mithilfe von Befehlsregeln können Sie die Ausgabe eines Befehls als *Feld für benutzerdefinierte Inventarisierung* festlegen. Der Befehl richtet sich nach dem Befehlsinterpreter und dem ausführbaren Pfad auf dem Gerät.

Beispielsweise können Sie auf Windows-Geräten zwar MS-DOS-Befehle erstellen aber keine UNIX-Befehle im Cygwin-Stil, es sei denn Cygwin ist im Standardpfad für alle Benutzer installiert und verfügbar.

Verwenden Sie eine der folgenden Regeln, um die Ausgabe des Befehls als *Feld für benutzerdefinierte Inventarisierung* festzulegen:

- `ShellCommandTextReturn (command)`
- `ShellCommandDateReturn (command)`
- `ShellCommandNumberReturn (command)`

Beispiel: Abrufen der Betriebszeit für Mac OS X

So legen Sie die Betriebszeit als *Feld für benutzerdefinierte Inventarisierung* fest:

```
ShellCommandTextReturn(/usr/bin/uptime | sed -e 's/.*load averages://' | awk '{print $1}')
```

Abrufen von PLIST-Werten

Mit Regeln vom Typ `PlistValueReturn` kann ein Eigenschaftenlistenschlüssel (PList-Schlüssel) als *Feld für benutzerdefinierte Inventarisierung* festgelegt werden.

Beispiel: Abrufen des Systemgebietsschemas

Zur Verteilung von Anwendungen mithilfe verwalteter Installationen unter Zugrundelegung der vom System bereitgestellten Sprache geben Sie die folgende Regel ein, um das Gebietsschema des Geräts abzurufen und anschließend ein entsprechendes Smart Label zu erstellen, das basierend auf dem vom KACE SMA Agenten im *Feld für benutzerdefinierte Inventarisierung* gemeldeten Sprachcode auf das Gerät angewendet wird:

```
PlistValueReturn(~/Library/Preferences/GlobalPreferences.plist, AppleLocale, TEXT)
```

Abrufen mehrerer Werte

Verknüpfen Sie `ValueReturn`-Regeln entweder mit dem Operator UND oder ODER. Die Regel zeigt die Anwendung als installiertes Programm an, sofern einer oder mehrere der Werte nicht leer sind.

Die verknüpften Werte werden, getrennt durch den Operator, alle im gleichen *Feld für benutzerdefinierte Inventarisierung* festgelegt und gelten daher für Suchkriterien, Filter, Berichte und andere Prozesse der Appliance technisch gesehen als TEXT-Werte.

Regeln vom Typ `ValueReturn` mit folgender Verknüpfung:

- Operator UND: Alle Werte werden im *Feld für benutzerdefinierte Inventarisierung* erfasst.
- Operator ODER: Alle Werte werden im *Feld für benutzerdefinierte Inventarisierung* erfasst.

Verknüpfen Sie im Feld für benutzerdefinierte Inventarisierung Regeln mithilfe der folgenden Syntax:

```
Funktion(Argumente ...) AND Funktion(Argumente) AND ...
```

Trennen Sie die Bedingungsanweisung durch Leerzeichen vom Operator. Verwenden Sie die Operatoren AND und OR nicht in derselben Regel.

Zuordnen von Dateinamen zu regulären Ausdrücken

Mit regulären Ausdrücken wird ein Zeichen oder die angegebene Zeichenfolge mit den Dateinamen im angegebenen Verzeichnis abgeglichen.

In diesem Abschnitt werden die regulären Ausdrücke beschrieben, die Dateinamen in Bedingungs- und Werterückgabe-Regeln unter Verwendung eines regulären Ausdrucks zuordnen.

HINWEIS: Der KACE Agent bietet nur Funktionen, die Dateinamen mithilfe regulärer Ausdrücke vergleichen.

Die regulären Ausdrücke

Die Syntax regulärer Ausdrücke kann für den Abgleich von Dateinamen verwendet werden.

TIPP: Weitere Informationen zum Erstellen von regulären Ausdrücken finden Sie unter http://msdn.microsoft.com/en-us/library/az24scfc.aspx.

Die folgende Tabelle enthält eine Übersicht über die Syntax regulärer Ausdrücke für den Abgleich von Dateinamen:

Zeichen	Beschreibung	Beispielausdruck	Zieldateien	Abgeglichene Dateien
(beliebige Zeichenfolge)	Mit normalen Zeichen (keine Sonderzeichen) wird eine Übereinstimmung mit jedem Dateinamen gefunden, der die Zeichenfolge enthält.	`abc`	abcFile.xls Example.jpg File.doc Myabc.txt MyFile.abc	abcFile.xls Myabc.txt MyFile.abc
.	Durch den Punkt wird ein einzelnes Zeichen zugeordnet. Wird der Punkt alleine eingegeben, wird eine Übereinstimmung mit allen Dateien gefunden.	`.`	abcFile.xls Example.jpg File.doc Myabc.txt MyFile.abc	abcFile.xls Example.jpg File.doc Myabc.txt MyFile.abc
\	Der umgekehrte Schrägstrich fungiert als Escape-Zeichen für Sonderzeichen oder dient zum Erstellen eines Rückverweises. Weitere Informationen hierzu finden Sie unter http://rexegg.com/regex-capture.html.	`.*\.txt$`	abcFile.xls Example.jpg File.doc Myabc.txt MyFile.abc	Myabc.txt
^	Mit dem Caret-Zeichen wird eine Übereinstimmung mit den Zeichen gefunden, die Sie am Anfang	`^k`	install.exe kinstaller.exe runkbot.bat	kinstaller.exe

Zeichen	Beschreibung	Beispielausdruck	Zieldateien	Abgeglichene Dateien
	des Dateinamens angeben.			
|	Mit dem Pipe-Zeichen wird eine Liste von zuzuordnenden Optionen getrennt.	`run|install`	install.exe kinstaller.exe runkbot.bat	install.exe kinstaller.exe runkbot.bat
$	Mit dem Dollar-Zeichen wird eine Übereinstimmung mit den Zeichen gefunden, die Sie am Ende des Dateinamens angeben.	`bat$`	install.exe kinstaller.exe runkbot.bat	runkbot.bat
?	Das Fragezeichen gibt an, dass das vorhergehende Zeichen in Übereinstimmungen optional ist.	`\.log10?$`	a.log1 afile.txt3 app.log appconf.log11 mylog.log10	a.log1 mylog.log10
*	Mit dem Sternchen wird null Mal oder mehrere Male eine Übereinstimmung mit dem vorherigen Zeichen gefunden.	`\.log1*$`	a.log1 afile.txt3 app.log appconf.log11 mylog.log10	a.log1 app.log appconf.log11
+	Mit dem Pluszeichen wird einmal oder mehrere Male eine Übereinstimmung mit dem vorherigen Zeichen gefunden.	`ap+.*\.log`	a.log1 afile.txt3 app.log appconf.log11 mylog.log10	app.log appconf.log11
[ ]	Klammern umschließen eine Zeichenklasse, und es wird eine Übereinstimmung mit jedem Zeichen innerhalb der Klammern gefunden. Spezielle Zeichenregeln für Zeichenklassen unterscheiden sich von normalen	`[123]`	a.log1 afile.txt3 app.log appconf.log11 mylog.log10	a.log1 afile.txt3 appconf.log11 mylog.log10

Zeichen	Beschreibung	Beispielausdruck	Zieldateien	Abgeglichene Dateien
	regulären Ausdrücken.			
()	Durch Zeichen umschließende Klammern wird ein Rückverweis erstellt, und es wird eine Übereinstimmung mit den vorherigen Zeichen und/oder den Zeichen in den Klammern gefunden. Weitere Informationen hierzu finden Sie unter http://rexegg.com/regex-capture.html.	`(p)\1`	a.log1 afile.txt3 app.log appconf.log11 mylog.log10	app.log appconf.log11
{n}	Durch geschweifte Klammern wird das vorherige Zeichen so oft wiederholt, wie angegeben ist, wobei **n** größer als 1 oder gleich 1 ist.	`{p}\.log$`	a.log1 afile.txt3 app.log appconf.log11 mylog.log10	app.log

Referenz zu Regeln mit regulären Ausdrücken

Die Syntax einer Regel mit einem regulären Ausdruck unterscheidet sich leicht von der anderer Dateiregeln. Das Argument `fullpath` ist eine Zeichenfolge, die dem absoluten Pfad des Dateispeicherorts entspricht, den Namen der Datei aber nicht enthält. Der Dateiname wird als separates Argument unter Verwendung eines regulären Ausdrucks angegeben.

Die folgende Tabelle enthält eine Liste der Regeln, bei denen reguläre Ausdrücke verwendet werden können.

Syntax	Windows	RHEL	OS X	Beschreibung
`FilenamesMatchingRegexExist (fullpath,regex)`	X	X	X	Gibt "Wahr" zurück, wenn Dateien im angegebenen Verzeichnis dem Dateinamen entsprechen, den Sie unter Verwendung eines regulären Ausdrucks eingegeben haben.

Syntax	Windows	RHEL	OS X	Beschreibung
`FilenamesMatchingRegexGreaterThan (fullpath,regex,value)`	X	X	X	"Wahr", wenn die Anzahl der übereinstimmenden Dateien größer ist als der Wert.
`FilenamesMatchingRegexLessThan (fullpath,regex,value)`	X	X	X	"Wahr", wenn die Anzahl der übereinstimmenden Dateien kleiner ist als der Wert.
`FilenamesMatchingRegexEqual (fullpath,regex,value)`	X	X	X	"Wahr", wenn die Anzahl der übereinstimmenden Dateien dem Wert entspricht.
`FilenamesMatchingRegexReturn (fullpath,regex,type)`	X	X	X	Legt das Feld für benutzerdefinierte Inventarisierung auf die übereinstimmenden Dateinamen fest (enthält den Pfad).

Definieren von Regelargumenten

In Regeln für benutzerdefinierte Inventarisierung kann mithilfe von Argumenten nach Pfaden, Dateien, Registrierungsschlüsseln, Registrierungseinträgen, Versionsinformationen, Umgebungsvariablen und anderen Attributen zu gesucht werden.

Informationen zur Syntax und zur Nutzung der Regeln finden Sie in den Tabellen unter Überprüfen von Bedingungen (Bedingungsregeln), Abrufen von Werten von einem Gerät (Benutzerdefiniertes Inventarfeld) und Zuordnen von Dateinamen zu regulären Ausdrücken.

Suchen eines Pfads oder einer Datei

Bei `path` und `fullpath` handelt es sich um Zeichenfolgen, die den absoluten Pfad eines Verzeichnisses oder einer Datei auf dem Gerät angeben. Beispiel:

```
C:\Program Files\Mozilla Firefox\firefox.exe
```

Der KACE Agent ermittelt das Verzeichnis oder die Datei und führt den speziellen Test durch.

Suchen eines Registrierungsschlüssels und eines -eintrags

Bei `registryPath` handelt es sich um eine Zeichenfolge, die den absoluten Pfad eines Registrierungsschlüssels in der Registrierung angibt. Beispiel:

```
HKEY_LOCAL_MACHINE/application/kace
```

Angeben einer Version

Bei `version` handelt es sich um eine ganze Zahl (Typ: TEXT), die der KACE Agent mit der Version des Elements vergleicht, das gerade auf dem Gerät getestet wird.

Beispielsweise gibt der Test `FileVersionGreaterThan` 'true' zurück, wenn der angegebene Wert höher ist als die Versionsnummer der Datei oder des Ordners. Andernfalls wird 'false' zurückgegeben.

Verknüpfen Sie zum Testen eines Bereichs eine Less Than- und eine Greater Than-Regel wie folgt:

```
FileVersionGreaterThan(C:\Program Files\Adobe\Acrobat\7.0\Acrobat\Acrobat.exe, 6.99)
AND FileVersionLessThan(C:\Program Files\Adobe\Acrobat\7.0\
Acrobat\Acrobat.exe, 8.00)
```

Angeben von Umgebungs- oder Benutzervariablen

Bei `var` handelt es sich um eine Zeichenfolge, die dem tatsächlichen Namen der Umgebungsvariablen auf dem Gerät entspricht.

Sie können beispielsweise folgendermaßen testen, ob die Variable für das Programmverzeichnis richtig festgelegt ist:

```
EnvironmentVariableEquals(ProgramFiles, TEXT,
C:\Program Files)
```

Angeben eines Dateiattributs

Bei `attribute` handelt es sich um eine Systemeigenschaft, eine Datei- oder eine Ordnereigenschaft oder eine vom KACE Agenten zugewiesene Eigenschaft auf dem Gerät. Die Appliance stellt betriebssystemabhängige Argumenttypen zur Verfügung.

Verwenden von Windows Dateiattributen

Mithilfe der Funktionen `FileInfoGreaterThan`, `FileInfoLessThan` und `FileInfoEquals` können Sie eine Dateieigenschaft unter Windows in folgender Syntax testen:

`Funktionsname` `(vollständiger_Pfad, Attribut, Typ, Wert)`

Die folgende Tabelle enthält die von Windows unterstützten Attribute:

Attribut	Typ	Beschreibung
AccessedDate	DATE	Uhrzeit und Datum des letzten Dateizugriffs.
Kommentare	TEXT	Zu Diagnosezwecken bereitgestellte weitere Informationen.
CompanyName	TEXT	Der Name des Unternehmens, das die Datei erstellt hat.
CreatedDate	DATE	Die Uhrzeit der Dateierstellung.
FileBuildPart	NUMBER	Die dritte Position der Dateiversion. Beispiel: In Version 1.2.3, 3=Build.
FileDescription	TEXT	Dateibeschreibung auf der Seite Details der Windows Dateieigenschaften
FileMajorPart	NUMBER	Die erste Position der Dateiversion. Beispiel: In Version 1.2.3, 1=Major.

Attribut	Typ	Beschreibung
FileMinorPart	NUMBER	Die zweite Position der Dateiversion. Beispiel: In Version 1.2.3, 2=Minor.
FileName	TEXT	Der aktuelle Name der Datei. Siehe auch FileExists.
FilePrivatePart	NUMBER	Die vierte Position der Dateiversion. Beispiel: In Version 1.2.3.4, 4=Private.
FileVersion	TEXT	Die auf der Seite Details der Dateieigenschaften angezeigte vollständige Dateiversion. Siehe auch "FileVersionEquals", "FileVersionGreaterThan" und "FileVersionLessThan".
InternalName	TEXT	Sofern vorhanden, der interne Name der Datei sowie der Komponentenname. Wenn die Datei nicht über einen internen Namen verfügt, ist dies der ursprüngliche Dateiname ohne Erweiterung.
Sprache	TEXT	Der Sprachcode. Der entsprechende Name wird auf der Seite Details der Dateieigenschaften angezeigt.
LegalCopyright	TEXT	Copyright-Hinweise für die Datei.
LegalTrademarks	TEXT	Marken und eingetragene Marken, die für die Datei gelten.
ModifiedDate	DATE	Datum und Uhrzeit der letzten Änderung.
OriginalFilename	TEXT	Stellt den vollständigen Namen der Datei zur Verfügung, wenn diese auf dem Gerät abgelegt oder installiert wurde.
PrivateBuild	TEXT	Informationen zur Dateiversion.
ProductBuildPart	NUMBER	Die dritte Position der Produktversion. Beispiel: In Version 1.2.3, 3=Build.

Attribut	Typ	Beschreibung
ProductMajorPart	NUMBER	Die erste Position der Produktversion. Beispiel: In Version 1.2.3, 1=Major.
ProductMinorPart	NUMBER	Die zweite Position der Produktversion. Beispiel: In Version 1.2.3, 2=Minor.
ProductName	TEXT	Zeichenfolge, die dem Produktnamen der Windows Eigenschaft entspricht.
ProductPrivatePart	NUMBER	Die vierte Position der Produktversion. Beispiel: In Version 1.2.3.4, 4=Private.
ProductVersion	TEXT	Die vollständige Produktversion. Siehe auch ProductVersionEquals, ProductVersionGreaterThan und ProductVersionLessThan.
SpecialBuild	TEXT	Weitere Informationen zum Build.

Testen von Dateiattributen für Linux und Mac

Auf Linux und Mac Geräten können Sie Dateiattribute mithilfe der folgenden Argumente testen:

Attribut	Typ	Beschreibung
access_time	DATE	Der Zeitpunkt des letzten Benutzer- oder Systemzugriffs auf die Datei
block_size	NUMBER	Die Blockgröße der Datei.
Blocks	NUMBER	Die Anzahl der von der Datei verwendeten Blöcke.
creation_time	DATE	Die Uhrzeit der Dateierstellung
device_number	NUMBER	Die Identifizierungsnummer des Geräts (Datenträger), das die Datei enthält
Gruppe	TEXT	Der Gruppenname des Besitzers der Datei
inode	NUMBER	Die Inode-Nummer der Datei
modification_time	DATE	Der Zeitpunkt der letzten gespeicherten Änderung

Attribut	Typ	Beschreibung
number_links	NUMBER	Die Anzahl der Hardlinks zu der Datei
Besitzer	TEXT	Der Benutzername der Person, die Besitzer der Datei ist.
Größe	NUMBER	Die Größe der Datei

Angeben des Datentyps

`type` gibt den Datentyp an, der getestet oder zurückgegeben wird.

Der KACE Agent unterstützt die folgenden Typen:

- `TEXT` ist eine Zeichenfolge. Nur gültig für die genaue Übereinstimmung in Bedingungsregeln wie Equals-Regeln. In ValueReturn-Regeln wird hiermit das *Feld für benutzerdefinierte Inventarisierung* auf eine Zeichenfolge festgelegt. Dadurch werden die Suchkriterien und die Filter auf entsprechende Operatoren beschränkt.
- `NUMBER` ist eine ganze Zahl. Gültig in allen Bedingungsregeln. Ermöglicht die Angabe einer ganzen Zahl zwecks Vergleich.
- `DATE` muss im Format `MM/TT/JJJJ HH:MM:SS` angegeben werden. Beispiel: `09/28/2006 05:03:51`. Die Angabe der Zeit ist erforderlich. Beispielsweise müssen Sie bei einem Vergleich wie Größer als die Zeit mindestens als 00:00:00 angeben.

Angeben der zu testenden Werte

`value` folgt in der Regel auf `type`, ausgenommen in einer Regel, in der der Datentyp bekannt ist wie beispielsweise in einer Versionsregel. Der Wert, den Sie angeben, muss dem Typ entsprechen. Siehe Angeben des Datentyps.

Angeben des Namens eines Registrierungseintrags (nur Windows)

`valueName` ist eine Zeichenfolge, die dem Namen des zu testenden Registrierungseintrags entspricht. Wird nur in Registrierungstests für Windows Geräte verwendet.

Angeben eines PLIST-Schlüssels (Nur Mac)

`entry` ist entweder NUMBER, TEXT oder DATE und entspricht einem Schlüssel in einer PLIST-Datei auf einem Mac OS X Gerät. Befindet sich der gewünschte Schlüssel in einem Array/Wörterbuch innerhalb der PLIST-Datei, kann durch Angabe des Namens-/Ganzzahlwerts für das Array/Wörterbuch darauf verwiesen werden. Hierzu wird ein begrenzender Doppelpunkt und dann der Namens-/Ganzzahlwert des Schlüssels (**Wörterbuch**:**Schlüssel**) im Eintragsargument angegeben.

Beispiele für Argumente:

- Auf den Schlüssel **Item 0** innerhalb des Arrays **PackageGroups** wird mit `PackageGroups:0` als Argument verwiesen.
- Auf den Schlüssel **contentType** innerhalb des Wörterbuchs **Item 102** wird mit `102:contentType` als Argument verwiesen.

Verwenden regulärer Ausdrücke

`regex` ist ein regulärer Ausdruck, der einem Dateinamen in einer Bedingungs- oder Werterückgabe-Regel entspricht. Weitere Informationen finden Sie unter Zuordnen von Dateinamen zu regulären Ausdrücken.

Definieren von Befehlen

Mit den Shell-Funktionen können Sie den `command`-Befehl angeben, der auf dem Gerät ausgeführt werden soll. Die Richtlinien für das Erstellen von Regelargumenten beziehen sich nicht auf Befehle. Leerzeichen nach den öffnenden Klammern und unmittelbar vor den schließenden Klammern werden aus dem Befehl gelöscht.

Benutzerdefinierte Inventarregeln testen

Zum Testen von Regeln für benutzerdefinierte Inventarisierung können Sie einen Befehl für eine benutzerdefinierte Inventur auf einem von einem KACE Agent verwalteten Gerät ausführen. So können Sie Regeln für benutzerdefinierte Inventarisierung debuggen, ohne den gesamten Inventarprozess ausführen zu müssen.

1. Öffnen Sie eine Eingabeaufforderung auf einem Gerät, auf dem der KACE Agent installiert ist.
2. Geben Sie den folgenden Befehl ein: `kdeploy -custominventory`

   Der Agent stellt eine Verbindung mit der Appliance her und führt die benutzerdefinierte Inventarisierung aus. Abfragen und zurückgegebene Werte werden angezeigt.

Bereitstellen von Paketen auf verwalteten Geräten

Sie können Pakete auf verwalteten Geräten bereitstellen, um Software per Remotezugriff über die Appliance zu installieren.

Verteilen von Software und Verwenden von Wake on LAN

Sie können Anwendungen, Aktualisierungen und Dateien von der Appliance aus an verwaltete Geräte verteilen. Außerdem können Sie Geräte mithilfe von Wake on LAN per Remotezugriff einschalten.

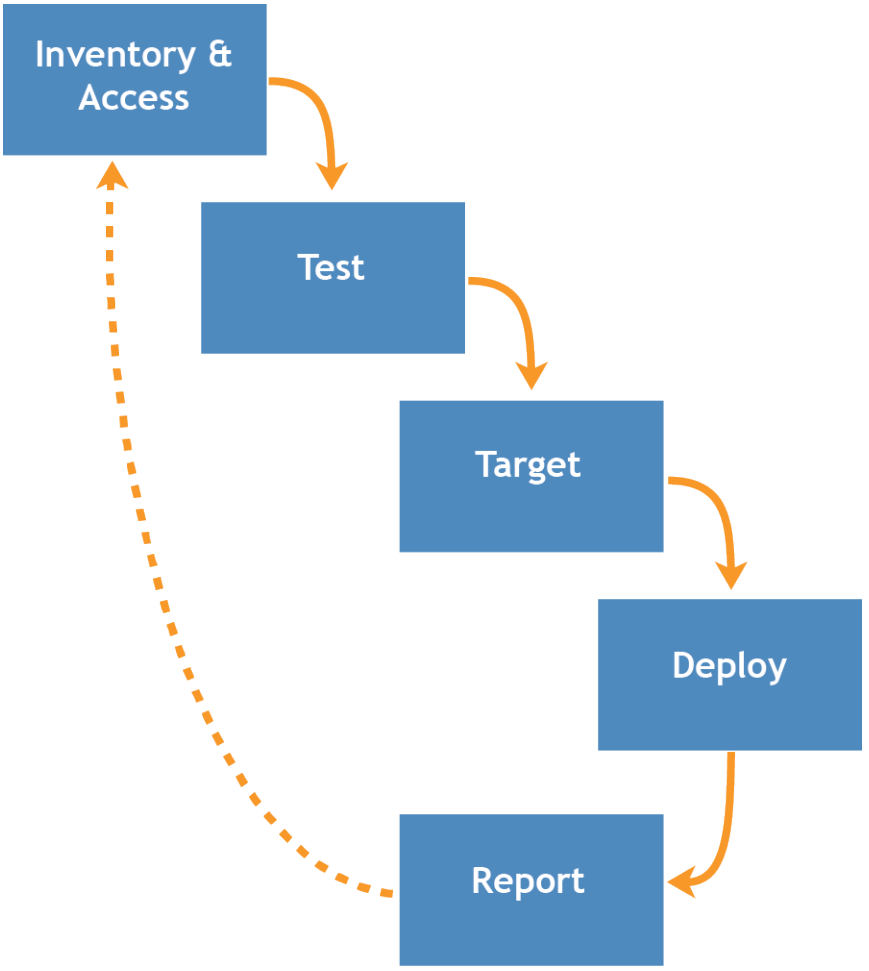
Informationen zur Softwareverteilung

Software kann von der Appliance an Windows-, Mac- und Linux-Geräte mit Agentenverwaltung verteilt werden.

> **TIPP:** Die Softwareverteilung ist nur für Elemente auf der Seite *Software* und für vom Agenten verwaltete Geräte verfügbar. Sie steht nicht für Elemente auf der Seite *Softwarekatalog*, für Microsoft Application Virtualization Software (App-V) oder für Geräte ohne Agenten-Software zur Verfügung.

Die Abbildung zeigt ein abstraktes Beispiel für einen allgemeinen Softwareverteilungsprozess. Sie können dieses Prozess nach Bedarf anpassen.

Softwareverteilungsverfahren



Informationen zum Testen der Softwareverteilung

Bevor Sie Software an eine Vielzahl von Geräten verteilen, sollten Sie die Bereitstellung auf einer kleinen, repräsentativen Gruppe von Geräten testen, um sicherzustellen, dass das Paket mit den Betriebssystemen und anderen Anwendungen der Zielgeräte kompatibel ist.

Wenn die Appliance Software an verwaltete Geräte verteilt, überprüft sie, ob ein Paket für ein bestimmtes Gerät oder Betriebssystem vorgesehen ist. Die Appliance kann jedoch nicht die Kompatibilität mit anderer Software auf dem Zielgerät überprüfen. Daher empfiehlt sich die Entwicklung eines Testprozesses für alle Bereitstellungen.

Sie könnten z. B. eine Testgruppe erstellen, indem Sie ein Label Geräten zuweisen, die zum Prüfen verwendet werden. Anschließend stellen Sie mithilfe des Labels die erforderliche Anwendung für die Testgruppe bereit, bevor Sie die Bereitstellung für eine größere Gruppe von Geräten durchführen. Mithilfe dieser Methode können Sie die Kompatibilität der Anwendung mit dem Betriebssystem und anderen Anwendungen in Ihrer Testgruppe prüfen. Weitere Informationen zum Erstellen von Labels für Geräte finden Sie unter Manuelle Labels hinzufügen oder bearbeiten.

In diesem Abschnitt werden in erster Linie die Test-, Ziel- und Bereitstellungsaspekte des Prozesses erläutert. Weitere Informationen zur Inventarverwaltung finden Sie unter Verwalten von Anwendungen auf der Seite "Software".

Nachverfolgen von Änderungen der Verteilungseinstellungen

Wenn Verlaufsabonnements zur Aufbewahrung von Informationen konfiguriert wurden, können Sie Details zu den an Einstellungen, Assets und Objekten vorgenommenen Änderungen anzeigen.

Diese Informationen beinhalten auch das Datum der Änderung und den Benutzer, der diese vorgenommen hat. Dies kann bei der Fehlerbehebung nützlich sein. Siehe Informationen zu den Verlaufseinstellungen.

Arten von Verteilungspaketen

Pakete können in Form von verwalteten Installationen, Dateisynchronisierungen, Benutzerkonsolenpaketen und MSI-Installationsprogrammen an verwaltete Geräte verteilt werden.

- **Verwaltete Installationen**: Installationspakete, die so konfiguriert sind, dass sie unbeaufsichtigt oder mit Benutzereingriffen ausgeführt werden. Verwaltete Installationen enthalten Installations-, Deinstallations- und Befehlszeilenparameter. Siehe Verwenden verwalteter Installationen.
- **Dateisynchronisierungen**: Eine Methode zum Verteilen von Dateien auf verwaltete Geräte. Im Gegensatz zu verwalteten Installationen werden bei Dateisynchronisierungen jedoch keine Dateien installiert, sondern lediglich verteilt. Siehe Dateisynchronisierungen erstellen und verwenden.
- **Benutzerkonsolenpakete**: Installationspakete, die Druckertreiber und andere über die Benutzerkonsole verteilte Anwendungen enthalten. Siehe Informationen zum Service Desk.
- **MSI-Installationsvorlage**: Ein Dienstprogramm, mit dem Sie Richtlinien erstellen und die grundlegenden Befehlszeilenparameter zum Ausführen von Windows MSI-basierten Installationsprogramme festlegen können. Siehe MSI-Installationsskripte hinzufügen.

Digitale Assets an Anwendungen anhängen und unterstützte Betriebssysteme auswählen

Um Anwendungen mithilfe von verwalteten Installationen oder **Benutzerkonsole**-Downloads an verwaltete Geräte zu verteilen, müssen Sie die entsprechenden digitalen Assets an Anwendungen anhängen. Digitale Assets sind die Dateien, die für die Bereitstellung erforderlich sind (z. B. Installationsprogramme). Darüber hinaus müssen Sie die unterstützten Betriebssysteme für die Anwendung auswählen. Sie können diese Aufgaben über die Detailseite *Software* durchführen.

Diese Regel gilt auch dann, wenn:

- Sie einen Befehl anstelle einer Installation oder einer digitalen Datei an Geräte senden wollen.
- Sie leiten die auf verwalteten Geräten installierten KACE Agenten um, um das digitale Asset (z. B. EXE- oder MSI-Dateien) von einer alternativen Download-Quelle zu beziehen.

Siehe Digitale Assets an Anwendungen anhängen und unterstützte Betriebssysteme auswählen.

Verteilen von Paketen aus der Appliance

Über die Appliance verteilte Pakete werden nur dann auf verwalteten Geräten bereitgestellt, wenn das Inventarelement für die Ausführung unter dem Betriebssystem des Geräts vorgesehen ist.

Wenn das Inventarelement beispielsweise nur für Windows 7 vorgesehen ist, wird es auf Geräten unter Windows 8 nicht bereitgestellt.

Außerdem werden Pakete nur auf Geräten bereitgestellt, die Labelanforderungen erfüllen. Wenn für das Paket beispielsweise festgelegt wurde, dass es in einem Label mit der Bezeichnung *Büro A* bereitgestellt werden soll, wird es auf Geräten, die nicht mit dem Label *Büro A* versehen sind, nicht bereitgestellt. Wenn die Appliance ein Anwendungsinventar-Element erstellt, werden im ausführlichen Inventardatensatz nur die Betriebssysteme erfasst, unter denen das Element installiert war.

Um eine verwaltete Installation bereitzustellen, müssen Sie eine Ausführungsoption und ein Bereitstellungsfenster auswählen. Siehe Verwenden verwalteter Installationen.

Verteilen von Paketen über alternative Download-Quellen und Replikationsfreigaben

Sie können Pakete über alternative Download-Quellen und Replikationsfreigaben verteilen.

Diese Verteilung kann in folgenden Situationen sinnvoll sein:

- Sie verfügen über Remote-Standorte mit eingeschränkter Bandbreite, die beim Zugriff auf die Appliance Schwierigkeiten haben können.
- Sie möchten die Speicherung großer Verteilungspakete auf der Appliance vermeiden.

Informationen zu alternativen Download-Quellen

Alternative Download-Quellen sind verwaltete Geräte, die die Dateien hosten können, die benötigt werden, um Software von der Appliance an andere verwaltete Geräte zu verteilen.

Eine alternative Download-Quelle kann jeder beliebige Netzwerkspeicherort sein, an dem sich alle erforderlichen Dateien zur Installation einer bestimmten Anwendung befinden. Sie können Pakete von alternativen Download-Quellen bereitstellen, beispielsweise von einer UNC-Adresse oder einer DFS-Quelle. Die CIFS- und SMB-Protokolle, Samba-Server und Dateiserver-Appliances werden unterstützt. Sie müssen den Speicherort angeben, wenn Sie eine verwaltete Installation erstellen.

Siehe Digitale Assets an Anwendungen anhängen und unterstützte Betriebssysteme auswählen.

Informationen zu Replikationsfreigaben

Replikationsfreigaben sind Geräte mit Kopien von zu verteilenden Dateien. Sie sind besonders hilfreich, wenn sich Ihre verwalteten Geräte an unterschiedlichen geografischen Standorten befinden.

Mit Replikationsfreigaben kann beispielsweise ein Gerät in New York Dateien von einem anderen Gerät im selben Büro herunterladen anstatt von einer Appliance in Los Angeles. Eine Replikationsfreigabe ist eine vollständige Replikation aller digitalen Assets und wird von der Appliance automatisch verwaltet. Sobald eine Replikationsfreigabe für ein Label angegeben wird, rufen Geräte in diesem Label Dateien von dieser Replikationsfreigabe ab.

Der KACE Agent sucht auf der Appliance immer nach Verteilungsdateien, wenn für ein auf ein Gerät angewendetem Label keine Replikationsfreigaben angegeben sind. Wenn die Appliance mehrere Replikationsfreigaben verwendet, trifft der Agent eine zufällige Auswahl.

Siehe Verwenden von Replikationsfreigaben.

Verteilen von Software auf Mac OS X Geräten

Die Appliance bietet verschiedene Methoden für die Verteilung von Anwendungen, Aktualisierungen und Dateien an Mac OS X Geräte.

Informationen zu Installationsprogrammen und ungepackte Pakete

Auf Mac OS X ist eine universelle Installationsdatei mit der üblichen Dateierweiterung .pkg vorhanden. Sie können eine PKG-Datei nicht direkt hochladen, da diese Dateien aus Low-Level-Verzeichnissen bestehen und in Webbrowsern keine vollständigen Verzeichnisse hochgeladen werden können.

Ungepackte Pakete (APP) erfordern keine Installationsprogramme. Sie können installiert werden, indem Sie sie in den *Anwendungsordner* auf dem Mac ziehen. APP-Pakete müssen jedoch archiviert werden, da sie ebenso wie die Installationsprogrammpakete aus Low-Level-Verzeichnissen bestehen.

Installationsprogramme können zusammen mit normalen Anwendungen archiviert werden. Die Appliance führt zuerst die Installationsprogramme aus und kopiert anschließend Anwendungen in den *Anwendungsordner*.

Unterstützte Paketbereitstellungen unter Mac OS X

Zu den unterstützten Paketbereitstellungen zählen PKG, APP, DMG, ZIP, TGZ und TAR.GZ.

Wenn Sie die Datei als Datenträger-Image packen, erfolgt die Bereitstellung sowie die Aufhebung der Bereitstellung durch die Appliance im unbeaufsichtigten Modus. Dieser Abschnitt enthält Beispiele für jede Bereitstellungsart. Für jedes Beispiel müssen Sie die Datei auf die Appliance hochgeladen haben, bevor Sie das Paket für die verwaltete Installation erstellen. Quest empfiehlt, die Anwendung auf einem Testgerät zu installieren. Nachdem der KACE Agent eine Verbindung mit der Appliance hergestellt hat, erstellt die Appliance ein Inventarelement und ein Paket für eine verwaltete Installation für die Anwendung.

Verwenden verwalteter Installationen

Verwaltete Installationen (Managed Installations, MIs) sind die primäre Art der Bereitstellung (oder Entfernung) von Anwendungen auf verwalteten Geräten. Jede verwaltete Installation beschreibt eine zu installierende oder zu entfernende Kombination aus Anwendungstitel und Version – einschließlich Installationsbefehlen, Installationsdateien und Zielgeräten (nach Label).

Verwaltete Installationen finden stets dann statt, wenn verwaltete Geräte Inventardaten in die Appliance hochladen. Auf diese Weise bestätigt die Appliance vor Durchführung der Installation, dass die Installation tatsächlich benötigt wird. Installationspakete können so konfiguriert werden, dass sie unbeaufsichtigt oder mit Benutzereingriffen ausgeführt werden. Verwaltete Installationen können Installations-, Deinstallations- und Befehlszeilenparameter enthalten.

Für verwaltete Installationen sind aktive Netzwerkverbindungen zur Appliance erforderlich. Wenn die Verbindung während einer Installation unterbrochen wird, wird der Prozess fortgesetzt, sobald der Agent die Verbindung erneut herstellt.

Die gängigsten Paketbereitstellungen für verwaltete Installationen unter Windows sind MSI-, EXE- und ZIP-Dateien.

Zu den unterstützten Paketbereitstellungen für Linux Geräte zählen RPM-, ZIP-, BIN-, TGZ- und TAR.GZ-Dateien.

Anwendungen zum Inventar hinzufügen

Vor der Erstellung einer verwalteten Installation müssen Sie die bereitzustellenden Dateien zunächst auf der Seite *Software* einer Anwendung zuweisen. Ist die Anwendung noch nicht auf der Seite *Software* verfügbar, können Sie sie hinzufügen.

Wenn Sie der Seite *Software* eine dort noch nicht vorhandene Anwendung hinzufügen möchten, haben Sie folgende Möglichkeiten:

- Installieren Sie die Anwendung auf einem verwalteten Gerät, und führen Sie anschließend vom Gerät aus eine Inventaraktualisierung durch. Siehe Erzwingen von Inventaraktualisierungen.
- Fügen Sie die Anwendung manuell zum Inventar hinzu. Siehe Anwendungen manuell dem Inventar der Seite "Software" hinzufügen.

VORSICHT: Wenn der Anzeigename des Anwendungsinventar-Elements nicht exakt mit dem Namen übereinstimmt, den die Anwendung in *Software* registriert hat, versucht die Appliance möglicherweise wiederholt, ein bereits vorhandenes Paket bereitzustellen. Fügen Sie zur Behebung dieses Problems die Anwendung der Inventarliste der Seite *Software* hinzu und verwenden Sie anschließend den registrierten Anwendungsnamen in der verwalteten Installation.

Informationen zu verwalteten Installationen

Sie können verwaltete Installationen für auf der Seite *Software* angezeigte Elemente erstellen.

Siehe:

- Verwaltete Installationen für Windows Geräte erstellen
- Verwaltete Installationen für Mac OS X Geräte erstellen
- Verwaltete Installationen für RPM-Dateien erstellen
- Verwaltete Installationen für TAR.GZ-Dateien erstellen
- Verwaltete Installationen für ZIP-Dateien erstellen

Wenn Sie Pakete mit speziellen Einstellungen (wie Parametern, Labels oder Bereitstellungsdefinitionen) erstellen möchten, können Sie mehrere Verteilungspakete für ein Inventarelement erstellen. Die verwaltete Installation kann jedoch nicht für mehrere Inventarelemente überprüft werden, da sie nur auf die Existenz eines einzigen Inventarelements überprüft.

Für jedes Beispiel müssen Sie die Datei auf die Appliance hochgeladen haben, bevor Sie das Paket für die verwaltete Installation erstellen. Quest empfiehlt, die Anwendung auf einem Testgerät zu installieren. Warten Sie dabei, bis der KACE Agent eine Verbindung mit der Appliance hergestellt hat, und erstellen Sie dann ein Inventarelement für die Anwendung und anschließend aus der Anwendung das Paket für die verwaltete Installation.

HINWEIS: Die Agenten-Bereitstellung wird im Abschnitt Provisionierung des KACE Agent beschrieben. Informationen zum Aktualisieren einer vorhandenen Version des Agenten finden Sie unter Agenten-Aktualisierungen manuell hochladen.

Informationen zu Installationsparametern

Sie können Installationsparameter zu den Paketdefinitionen hinzufügen, die für die Anwendungsverteilung und -installation auf verwalteten Geräten verwendet werden.

Paketdefinitionen können MSI-, EXE-, ZIP- und andere Dateitypen für die Bereitstellung von Anwendungen enthalten. Wenn ein Administrator die Datei durch Ausführen einer einzelnen Datei, einer BAT- oder einer VBScript-Datei auf einem lokalen Gerät installiert, kann das Paket von der Appliance über das Netzwerk installiert werden.

Die Paketdefinition kann zum Vereinfachen von Verteilung und Installation auch Parameter enthalten, die dem Installationsprogramm zur Laufzeit auf dem lokalen Gerät übergeben werden. Sie können beispielsweise Parameter als benutzerdefinierte Installationseinstellungen zum Umgehen des automatischen Neustarts verwenden.

Von Installationsprogrammdateien unterstützte Parameter identifizieren

Sie können die Parameter anzeigen, die von den Installationsprogrammdateien von der Windows Befehlszeile aus unterstützt werden.

1. Öffnen Sie eine Eingabeaufforderung.
2. Wechseln Sie in das Verzeichnis, das das Zielinstallationsprogramm enthält.

   Zum Beispiel: `c:\...\adobe.exe`
3. Geben Sie **Dateiname** `/?` ein.

   Zum Beispiel: `adobe.exe /?`

   Wenn dieses Paket Parameter unterstützt, werden diese angezeigt. Beispiel: `/quiet, /norestart`.
4. Verwenden Sie die erkannten Parameterdefinitionen, um Ihre Paketdefinition zu aktualisieren.

Weitere Informationen hierzu finden Sie in der Dokumentation des Herstellers der Anwendung.

Verwaltete Installationen für Windows Geräte erstellen

Mithilfe verwalteter Installationen können Sie Software auf Windows-Geräten mit Agentenverwaltung bereitstellen.

Wenn Sie verwaltete Installationen für die Windows-Plattform erstellen, können Sie angeben, ob Benutzern vor und nach der Installation eine Meldung angezeigt werden soll. Sie können auch angeben, ob das Paket bereitgestellt werden soll, wenn der Benutzer angemeldet ist, und ob die Bereitstellung auf ein bestimmtes Label beschränkt werden soll.

Ausführlichere Informationen zum Erstellen einer verwalteten Installation für eine MSI-, EXE- oder ZIP-Datei finden Sie unter Beispiele für gängige Bereitstellungen unter Windows.

Wenn Sie Anwendungen an verwaltete Geräte verteilen möchten, müssen Sie den Anwendungen die digitalen Assets, d. h. die für die Installation erforderlichen Dateien, zuordnen. Darüber hinaus müssen Sie die unterstützten Betriebssysteme für die Anwendungen auswählen. Siehe Digitale Assets an Anwendungen anhängen und unterstützte Betriebssysteme auswählen.

1. Rufen Sie die *Detailseite für verwaltete Installation* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Verteilung** und anschließend auf **Verwaltete Installationen**.
   c. Wählen Sie **Aktion auswählen** > **Neu**.
2. Geben Sie im Bereich *Konfigurieren* die folgenden Informationen ein:

Option	Beschreibung
Name	Ein Name, der die verwaltete Installation identifiziert. Dieser Name wird auf der Seite *Verwaltete Installationen* angezeigt.

Option	Beschreibung
Ausführung	Die Einstellung für die Paketbereitstellung. Zur Auswahl stehen folgende Optionen: • **Deaktiviert**: Das Paket nicht bereitstellen. • **Jederzeit**: Das Paket bei der nächsten Gelegenheit bereitstellen, z. B. wenn der KACE Agent Inventarinformationen an die Appliance meldet. • **Beim Start**: Das Paket beim nächsten Starten des Geräts bereitstellen. **HINWEIS:** Wenn auf einem Gerät eine Active Directory- oder Gruppenrichtlinienobjekt-Einstellung aktiv ist, mit der eine Meldung angezeigt wird, die der Benutzer vor dem Anmelden bestätigen muss, werden keine Pakete bereitgestellt und keine Skripte ausgeführt, bevor die Bestätigung erfolgt ist. • **Nach dem Anmelden**: Das Paket bereitstellen, nachdem der Benutzer sich angemeldet hat, jedoch bevor der Desktop lädt. • **Bei angemeldetem Benutzer**: Das Paket bereitstellen, während der Benutzer angemeldet ist. • **Bei abgemeldetem Benutzer**: Das Paket nur bereitstellen, wenn das Gerät läuft und der Benutzer abgemeldet ist.
Inventar	Geben Sie an, ob Sie den Softwaretitel von **Katalogisierter Software** oder sämtlicher **Software** hinzufügen wollen, indem Sie eine der Optionen wählen. • Um nach einem Titel zu suchen, beginnen Sie mit der Eingabe in das Feld *Software* oder *Katalogisierter Software* . **HINWEIS: Nur ungenutzte Softwarelizenzen zurückgewinnen.** Der Name der Software, die Sie deinstallieren möchten, wird standardmäßig in diesem Feld angezeigt. Weitere Informationen hierzu finden Sie unter Rückgewinnen ungenutzter Softwarelizenzen. • Wenn nur die Software mit einer oder mehreren verknüpften Dateien anzeigen wollen, wählen Sie **Nur Software mit einer zugehörigen Datei anzeigen**.
Zugehörige Datei	Software und katalogisierte Software können je nach Bedarf über eine oder mehrere Dateien als Anlage verfügen. Geben Sie an, ob Sie eine bestimmte

Option	Beschreibung
	Datei, die mit dem gewählten Softwaretitel verknüpft ist, wählen möchten. • **Zugehörige Datei auswählen**: Wählen Sie diese Option, wenn Sie eine Datei zuordnen möchten. Sie können eine Datei aus der Liste wählen. Wenn Sie den Dateiname kennen, geben Sie diesen in das Feld ein, und wählen sie unter den verfügbaren Einträge der Liste aus. • **Datei nicht verknüpfen**: Wählen Sie diese Option, wenn Sie eine Datei nicht zuordnen möchten.
Alternativer Speicherort	Geben Sie eine Download-Quelle für eine bestimmte verwaltete Installation an. **Pfad**: Geben Sie die Quelle ein, von der der KACE Agent digitale Installationsdateien abrufen kann. **Prüfsumme**: Geben Sie eine alternative Prüfsumme (MD5) ein, die mit der MD5-Prüfsumme in der Remote-Dateifreigabe übereinstimmt. Wenn keine Prüfsumme eingegeben wird, muss das digitale Asset in der Dateifreigabe mit dem digitalen Asset übereinstimmen, das mit dem Bereitstellungspaket in der Appliance verknüpft ist. Zudem muss der Zielpfad den vollständigen Dateinamen enthalten (z. B. `\\fileserver_one\software\adobe.exe`). Sie können die Prüfsumme mit einem beliebigen Tool erstellen, unter anderem mit dem Programm KDeploy.exe, das mit dem KACE Agenten installiert wird. **So erstellen Sie eine Prüfsumme mit KDeploy.exe:** a. Öffnen Sie auf einem Gerät, auf dem der KACE Agent installiert ist, ein Eingabeaufforderungs- oder Terminalfenster. b. Öffnen Sie das Installationsverzeichnis von Quest KACE. Beispiel: Windows 32-Bit-Geräte: `C:\Programme\Quest\KACE` Windows 64-Bit-Geräte: `C:\Programme (x86)\Quest\KACE\` Mac OS X Geräte: `/Library/Application Support/Quest/KACE/bin` c. Geben Sie den folgenden Befehl ein: KDeploy -hash=**Dateiname** Wobei **Dateiname** für den UNC-Pfad der Datei steht. Wenn der Pfad Leerzeichen enthält, geben Sie den gesamten Pfad in doppelten Anführungszeichen an. d. Drücken Sie **STRG+C** bzw. **Befehlstaste +C**, um die MD5-Prüfsumme zu kopieren. Anschließend können Sie sie in andere Dateien kopieren, z. B. in Notepad.

Option	Beschreibung
	Anmeldeinformationen: Die Details des Dienstkontos, die erforderlich sind, um eine Verbindung zum Gerät herzustellen und Befehle auszuführen Wählen Sie vorhandene Anmeldeinformationen in der Dropdown-Liste aus oder wählen Sie **Neue Anmeldeinformationen hinzufügen** aus, um nicht bereits aufgeführte Anmeldeinformationen hinzuzufügen. Siehe Hinzufügen und Bearbeiten von Benutzer-/Kennwort-Anmeldeinformationen. **HINWEIS:** Wenn das Zielgerät einem Replikationslabel angehört, ruft die Appliance keine Anwendung von der alternativen Download-Quelle ab. Sie können ein vorhandenes Label bearbeiten oder ein Label erstellen, um den alternativen Speicherort global anzugeben. Da dieses Label keiner verwalteten Installation zugewiesen ist, können Sie keine alternative Prüfsumme angeben, die mit der Prüfsumme in der Remote-Dateifreigabe übereinstimmt. Siehe Verteilen von Paketen über alternative Download-Quellen und Replikationsfreigaben und Manuelle Labels hinzufügen oder bearbeiten.
Standardinstallation	Verwenden Sie die Standardbefehle während der Installation. **Zusätzliche Parameter**: Geben Sie das Installationsverhalten wie folgt an: • Die maximale Feldlänge beträgt 256 Zeichen. Wenn ein Pfad diesen Grenzwert überschreitet, verweisen Sie in der Befehlszeile auf eine BAT-Datei, die den Pfad und den Befehl enthält. • Wenn ein Dateipfad Leerzeichen enthält, geben Sie den gesamten Pfad in doppelten Anführungszeichen an. Beispiel: "`\\kace_share\demo files\share these files\setup.bat`"
Standardinstallation überschreiben	Geben Sie die vollständigen Befehlszeilenparameter an. Verfügbare Laufzeitoptionen finden Sie in der Dokumentation zur MSI-Befehlszeile. • **Deinstallieren**: Deinstallieren Sie die Anwendung über die Befehlszeile. • **Nur Befehl ausführen (Datei nicht herunterladen)**: Es wird nur der Befehl in der Befehlszeile ausgeführt. • **msiexec.exe nicht voranstellen**: Verhindert, dass die Appliance `msiexec.exe` am Anfang der Datei hinzufügt.

Option	Beschreibung
Heruntergeladene Dateien löschen	Löscht die Dateien, wenn die Bereitstellung abgeschlossen ist.
ITNinja	Bereitstellungstipps von ITNinja. Diese Tipps sind nur verfügbar, wenn Sie Nutzungsdaten weitergeben. Siehe Konfigurieren der Datenfreigabeeinstellungen.

3. Legen Sie die Bereitstellungseinstellungen fest:

Option	Beschreibung
Alle Geräte	Stellen Sie die Funktion auf allen Geräten bereit. Deaktivieren Sie das Kontrollkästchen, um die Bereitstellung auf bestimmte Labels oder Geräte zu beschränken.
Labels	Beschränken Sie die Bereitstellung auf Geräte, die zu angegebenen Labels gehören. Klicken Sie zum Auswählen von Labels auf **Bearbeiten**, ziehen Sie die Labels ins Fenster *Bereitstellung beschränken auf* und klicken Sie dann auf **Speichern**. Wenn Sie ein Label auswählen, das über eine Replikationsfreigabe oder eine alternative Download-Quelle verfügt, werden digitale Assets aus dieser Replikationsfreigabe oder aus dieser alternativen Download-Quelle kopiert und nicht direkt von der Appliance heruntergeladen. **HINWEIS:** Die Appliance nutzt eine Replikationsfreigabe, bevor sie den Alternativen KACE Speicherort verwendet.
Geräte	Beschränken Sie die Bereitstellung auf bestimmte Geräte. Wählen Sie aus der Dropdown-Liste die Geräte aus, auf denen Sie die Anwendung bereitstellen möchten. Um die Liste zu filtern, geben Sie einige Zeichen ins Feld *Geräte* ein. Die Zahl neben dem Feld zeigt die Anzahl der verfügbaren Geräte an. **HINWEIS: Nur ungenutzte Softwarelizenzen zurückgewinnen.** Alle Geräte, von denen Sie die Software entfernen möchten, werden aufgeführt. Sie können die Liste der Geräte nach Bedarf bearbeiten. Um die Software von allen Geräten zu entfernen, wählen Sie einfach, wie oben beschrieben. Weitere Informationen hierzu finden Sie unter Rückgewinnen ungenutzter Softwarelizenzen.

4. Geben Sie die folgenden Benutzerbenachrichtigungseinstellungen an:

Option	Beschreibung
Benutzer vor der Ausführung benachrichtigen	Mit dieser Option wird auf verwalteten Geräten vor der Installation eine Meldung angezeigt. Wenn Sie diese Option auswählen, werden die folgenden Felder angezeigt: • **Meldung**: Die Meldung, die auf verwalteten Geräten vor Beginn der Installation angezeigt wird. • **Timeout**: Die Zeitdauer in Minuten, für die die Meldung angezeigt werden soll. • **Aktion**: Die Aktion, die am Ende der Zeitspanne für den **Timeout der ersten Meldung** ausgeführt wird. Die Optionen **Später installieren** und **Jetzt installieren** sind verfügbar. Wählen Sie **Jetzt installieren**, um die Anwendung sofort zu installieren, oder **Später installieren**, um die Installation bis zu einer Benutzerreaktion zu verschieben. „Später installieren“ ist nützlich, wenn Sie Benutzer vor einer Installation oder einem Neustart darüber benachrichtigen möchten.
Erste Meldung	Mit dieser Option wird auf verwalteten Geräten vor der Installation eine Meldung angezeigt. Wenn Sie diese Option auswählen, werden die folgenden Felder angezeigt: • **Meldung**: Die Meldung, die auf verwalteten Geräten vor Beginn der Installation angezeigt wird. • **Timeout**: Die Zeitdauer in Minuten, für die die Meldung angezeigt werden soll. • **Aktion**: Die Aktion, die am Ende der Zeitspanne für den **Timeout der ersten Meldung** ausgeführt wird. Die Optionen **Später installieren** und **Jetzt installieren** sind verfügbar. Wählen Sie **Jetzt installieren**, um die Anwendung sofort zu installieren, oder **Später installieren**, um die Installation bis zu einer Benutzerreaktion zu verschieben. „Später installieren“ ist nützlich, wenn Sie Benutzer vor einer Installation oder einem Neustart darüber benachrichtigen möchten.
Abschlussmeldung	Mit dieser Option wird auf verwalteten Geräten nach der Installation eine Meldung angezeigt. Wenn Sie

Option	Beschreibung
	diese Option auswählen, werden die folgenden Felder angezeigt: • **Meldung**: Die Meldung, die auf verwalteten Geräten nach Abschluss der Installation angezeigt wird. • **Timeout**: Die Zeitdauer in Minuten, für die die Meldung angezeigt werden soll.

5. Wählen Sie die Optionen für die Zeitplanung aus:

Option	Beschreibung
Bereitstellungsfenster Start Ende	Die Uhrzeit im 24-Stunden-Format für Beginn und Ende der Bereitstellung des Pakets. Die Uhrzeit im *Bereitstellungsfenster* wirkt sich auf alle Optionen unter *Aktion* aus. Zudem setzen die in der Appliance unter *Einstellungen* definierten Ausführungsintervalle die Angaben im Bereitstellungsfenster bestimmter Pakete außer Kraft oder treten in Wechselwirkung mit diesen Angaben.
Reihenfolge	Die Reihenfolge, in der die Anwendung installiert oder deinstalliert werden soll. Die Software mit dem niedrigsten Wert wird als Erstes bereitgestellt. Wenn die Installations- und die Deinstallationsaktion beide denselben Reihenfolgenwert haben, wird zuerst die Deinstallationsaktion ausgeführt. **HINWEIS:** Verwaltete Installationen werden immer der Reihenfolge nach bereitgestellt, unabhängig davon, ob die angegebenen Softwarepakete aus dem Softwarekatalog oder aus der Softwareliste stammen. Verwaltete Installationen mit einer niedrigeren Bereitstellungsreihenfolge verhindern immer, dass andere verwaltete Installationen ausgeführt werden, bis sie erfolgreich installiert wurden oder die angegebenen Wiederholungsversuche überschreiten.
Maximale Anzahl Versuche	Die maximale Anzahl der Versuche für die Installation des Pakets durch die Appliance (zwischen 0 und 99). Wenn Sie 0 angeben, versucht die Appliance unbegrenzt, das Paket zu installieren.

6. Klicken Sie auf **Speichern**.

Beispiele für gängige Bereitstellungen unter Windows

Die gängigsten Paketbereitstellungen für die verwaltete Installation sind MSI-, EXE- und ZIP-Dateien.

Beispiel für eine MSI-Standarddatei

Mithilfe von MSI-Dateien können Sie Software komfortabel und eigenständig auf Windows-Geräten bereitstellen. Wenn Ihre MSI-Datei keine spezielle Umwandlung oder Anpassung erfordert, ist die Bereitstellung unkompliziert.

Für MSI-Dateien muss die Option `/i` angegeben werden, wenn bei der Installation andere Optionen verwendet werden.

In der Parameterzeile der Appliance muss weder der Dateiname noch die `msiexec`-Syntax angegeben werden. Lediglich die Option `/*` muss angegeben werden:

`/qn /I` (richtig)

`msiexec /I /qn` (falsch)

HINWEIS: Um mit MSI-Dateien Parameter verwenden zu können, muss sich auf allen Zielgeräten dieselbe Version von Windows Installer befinden (über Microsoft zu beziehen). Bei älteren Versionen sind möglicherweise einige Optionen nicht aktiv. Die aktuelle Version von Windows Installer kann von der Appliance aus an die Geräte verteilt werden.

TIPP: Bei Verwendung von Windows Installer 3.0 oder einer höheren Version können Sie die unterstützten Parameter ermitteln, indem Sie im *Startmenü* die Option **Ausführen** auswählen. Geben Sie im Popup-Fenster msiexec ein. In einem Fenster wird eine Liste mit den unterstützten Parametern angezeigt.

Beispiel für eine EXE-Standarddatei

EXE-Dateien ähneln MSI-Dateien – mit einer Ausnahme.

EXE-Dateien unterscheiden sich von MSI-Dateien wie folgt: /I muss bei der Verwendung einer EXE-Datei in der Zeile *Ausführungsparameter* nicht angegeben werden.

Bei der Verwendung einer ausführbaren Datei ist es häufig hilfreich, Parameter für eine unbeaufsichtigte Installation anzugeben. Geben Sie hierzu im Feld *Ausführungsparameter* den Parameter /? an.

Verwaltete Installationen für ZIP-Dateien erstellen

Bei der Bereitstellung von Software mithilfe einer ZIP-Datei können Sie komfortabel ein Softwarepaket erstellen, falls zum Bereitstellen eines Titels mehrere Dateien erforderlich sind.

Ein Softwaretitel kann z. B. eine Datei namens `setup.exe` sowie Konfigurations- und Datendateien umfassen. Wenn sich auf einer CD-ROM mehrere Dateien befinden, die zum Installieren einer bestimmten Appliance benötigt werden, können Sie diese in einer ZIP-Datei zu einem Paket hinzufügen und zur Bereitstellung auf die Appliance hochladen.

HINWEIS: Der KACE Agent führt Bereitstellungspakete mit der Erweiterung MSI und EXE automatisch aus.

HINWEIS: Sie können außerdem ein ZIP-Archiv mit mehreren Dateien erstellen und die Appliance anweisen, das Archiv zu entpacken und eine bestimmte Datei auszuführen. Geben Sie den Namen der Datei, die ausgeführt werden soll, im Bereitstellungspaket in das Feld "Befehl (Ausführbare Datei)" ein (beispielsweise `runthis.exe`).

Wenn Sie Anwendungen an verwaltete Geräte verteilen möchten, müssen Sie den Anwendungen die digitalen Assets, d. h. die für die Installation erforderlichen Dateien, zuordnen. Darüber hinaus müssen Sie die unterstützten Betriebssysteme für die Anwendungen auswählen. Siehe Digitale Assets an Anwendungen anhängen und unterstützte Betriebssysteme auswählen.

1. Navigieren Sie zum Speicherort der erforderlichen Installationsdateien, wählen Sie alle Dateien aus und erstellen Sie mithilfe eines Dienstprogramms wie WinZIP® eine ZIP-Datei.
2. Melden Sie sich an der Administratorkonsole der Appliance an.
3. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
4. Erstellen Sie ein Inventarelement für die Zielbereitstellung.

Sie können diesen Vorgang manuell über die Seite *Inventar* > *Software* durchführen oder das Paket auf einem Gerät installieren, das regelmäßig eine Verbindung mit der Appliance herstellt. Siehe Informationen zur Seite "Software".

5. Verknüpfen Sie die ZIP-Datei mit dem Inventarelement und laden Sie diese auf die Appliance hoch:
   a. Klicken Sie in der linken Navigationsleiste auf **Verteilung** und anschließend auf **Verwaltete Installationen**.
   b. Wählen Sie **Aktion auswählen** > **Neu**.
   c. Wählen Sie in der Dropdown-Liste *Software* den Anwendungstitel aus, mit dem die ZIP-Datei verknüpft ist. Sollen alle Anwendungstitel angezeigt werden, deaktivieren Sie das Kontrollkästchen **Nur Datensätze mit einer verknüpften Datei anzeigen**.
6. Geben Sie in das Feld *Ausführungsparameter* den vollständigen Befehl mit Argumenten ein.

   Zum Beispiel: `setup.exe /qn`
7. Legen Sie nach Bedarf weitere Einstellungen fest.

   Siehe Verwaltete Installationen für Windows Geräte erstellen.
8. Klicken Sie auf **Speichern**.

Verwaltete Installationen für RPM-Dateien erstellen

Sie können verwaltete Installationen erstellen, um Software mithilfe von RPM-Dateien auf Linux Geräten bereitzustellen.

Wenn Sie Anwendungen an verwaltete Geräte verteilen möchten, müssen Sie den Anwendungen die digitalen Assets, d. h. die für die Installation erforderlichen Dateien, zuordnen. Darüber hinaus müssen Sie die unterstützten Betriebssysteme für die Anwendungen auswählen. Siehe Digitale Assets an Anwendungen anhängen und unterstützte Betriebssysteme auswählen.

1. Rufen Sie die *Detailseite für verwaltete Installation* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Verteilung** und anschließend auf **Verwaltete Installationen**.
   c. Wählen Sie **Aktion auswählen** > **Neu**.
2. Wählen Sie aus der Dropdown-Liste *Software* einen Softwaretitel aus. Um nach einem Titel zu suchen, tippen Sie in das Feld *Software*.

   Der KACE Agent versucht standardmäßig, die RPM-Datei mithilfe des folgenden Befehls zu installieren. Dieser Befehl reicht im Allgemeinen aus, um ein neues Paket zu installieren oder ein vorhandenes auf eine neue Version zu aktualisieren:

   `rpm -U` **Paketname.rpm**

   Wenn Sie eine ZIP-, TGZ- oder TAR.GZ-Datei auswählen, wird der Inhalt entpackt und das Stammverzeichnis nach allen RPM-Dateien durchsucht. Der Installationsbefehl wird für alle diese Dateien ausgeführt. Die Appliance findet alle RPM-Dateien auf der obersten Ebene eines Archivs automatisch, sodass Sie mehrere Pakete gleichzeitig installieren können. Sie können auch ein Archiv erstellen, das ein Shellskript enthält, und den Namen dieses Skripts in Form eines vollständigen Befehls angeben. Die Appliance führt diesen Befehl aus, wenn sie ihn findet, und zeichnet einen Fehler auf, wenn nicht.

   Wenn Sie im Feld *Ausführungsparameter* keine Parameter angeben, werden Standardparameter verwendet.

   In den Dateinamen, die Sie verwenden, können Sie Platzhalter angeben. Wenn der Dateiname Leerzeichen enthält, geben Sie den Dateinamen in einfachen oder doppelten Anführungszeichen an. Die

Dateien werden in ein Verzeichnis in `/tmp` extrahiert, das zum aktuellen Arbeitsverzeichnis des Befehls wird.

HINWEIS: Unter Red Hat Linux müssen Sie Ihrem Archiv keine anderen Dateien hinzufügen, wenn Sie nur das Skript ausführen möchten.

Wenn das aktuelle Arbeitsverzeichnis nicht in der Umgebungsvariablen PATH Ihres Stammkontos enthalten ist und Sie ein Shellskript oder eine andere ausführbare Datei, die Sie zu einem Archiv hinzugefügt haben, ausführen möchten, geben Sie im Feld *Vollständige Befehlszeile* den relativen Pfad zur ausführbaren Datei an. Der Befehl wird in einem Verzeichnis zusammen mit den extrahierten Dateien ausgeführt.

Beispiel: Um ein Shellskript mit dem Namen `installThis.sh` auszuführen, fügen Sie es zusammen mit einer RPM-Datei zum Paket hinzu und geben Sie den Befehl ./installThis.sh im Feld *Installationsbefehl* ein. Wenn Sie es in einem anderen Verzeichnis archivieren, geben Sie in das Feld *Installationsbefehl* Folgendes ein:

`./dir/Dateiname.sh`

Für beide Beispiele sowie für einige andere Funktionen der Appliance wird vorausgesetzt, dass `sh` im Pfad des Stamms angegeben ist. Bei Verwendung einer anderen Skriptsprache müssen Sie im Feld "Installationsbefehl" möglicherweise den vollständigen Pfad des gewünschten Befehlsprozessors angeben:

`/bin/sh ./`**Dateiname**`.sh`

Fügen Sie entsprechende Argumente für die unbeaufsichtigte Ausführung eines Batch-Skripts hinzu.

Wenn Sie das Kontrollkästchen zum Deinstallieren in den Details zur verwalteten Installation aktivieren, führt der KACE Agent den folgenden Befehl für die eigenständige RPM-Datei oder für alle RPM-Dateien im Archiv aus und entfernt dabei die Pakete automatisch:

`//usr/sbin/rpm -e` **Paketname**`.rpm`

Das Paket wird nur dann entfernt, wenn das Archiv oder Paket auf das Gerät heruntergeladen wurde. Wenn Sie das Kontrollkästchen *Deinstallieren unter Verwendung der vollständigen Befehlszeile* aktivieren, geben Sie im Feld *Installationsbefehl* eine vollständige Befehlszeile an, um sicherzustellen, dass der richtige Befehl zum Entfernen für das richtige Paket ausgeführt wird. Da in diesem Fall kein Paket heruntergeladen wird, geben Sie den Pfad in der Installationsdatenbank an, in der das empfangene Paket gespeichert wird.

3. Wenn das Paket weitere Optionen erfordert, geben Sie die folgenden Informationen an:

Option	Beschreibung
Name	Ein Name, der die verwaltete Installation identifiziert. Dieser Name wird auf der Seite *Verwaltete Installationen* angezeigt.
Ausführung	Wählen Sie den besten Zeitpunkt für die Bereitstellung des Pakets aus. Für die Linux Plattform stehen die Optionen **Anytime (next available) (Zu einem beliebigen (dem nächsten verfügbaren) Zeitpunkt)** und **Deaktiviert** zur Verfügung.
Inventar	Geben Sie an, ob Sie den Softwaretitel von **Katalogisierter Software** oder sämtlicher **Software** hinzufügen wollen, indem Sie eine der Optionen wählen. • Um nach einem bestimmten Titel zu suchen, beginnen Sie mit der Eingabe in das Feld *Software* oder *Katalogisierte Software*.

Option	Beschreibung
	HINWEIS: Nur ungenutzte Softwarelizenzen zurückgewinnen. Der Name der Software, die Sie deinstallieren möchten, wird standardmäßig in diesem Feld angezeigt. Weitere Informationen hierzu finden Sie unter Rückgewinnen ungenutzter Softwarelizenzen. • Wenn nur die Software mit einer oder mehreren verknüpften Dateien anzeigen wollen, wählen Sie **Nur Software mit einer zugehörigen Datei anzeigen**.
Zugehörige Datei	Software und katalogisierte Software können je nach Bedarf über eine oder mehrere Dateien als Anlage verfügen. Geben Sie an, ob Sie eine bestimmte Datei, die mit dem gewählten Softwaretitel verknüpft ist, wählen möchten. • **Zugehörige Datei auswählen**: Wählen Sie diese Option, wenn Sie eine Datei zuordnen möchten. Sie können eine Datei aus der Liste wählen. Wenn Sie den Dateiname kennen, geben Sie diesen in das Feld ein, und wählen sie unter den verfügbaren Einträge der Liste aus. • **Datei nicht verknüpfen**: Wählen Sie diese Option, wenn Sie eine Datei nicht zuordnen möchten.
Alternativer Speicherort	Geben Sie eine Download-Quelle für eine bestimmte verwaltete Installation an. **Pfad**: Geben Sie die Quelle ein, von der der KACE Agent digitale Installationsdateien abrufen kann. **Prüfsumme**: Geben Sie eine alternative Prüfsumme (MD5) ein, die mit der MD5-Prüfsumme in der Remote-Dateifreigabe übereinstimmt. Wenn keine Prüfsumme eingegeben wird, muss das digitale Asset in der Dateifreigabe mit dem digitalen Asset übereinstimmen, das mit dem Bereitstellungspaket in der Appliance verknüpft ist. Zudem muss der Zielpfad den vollständigen Dateinamen enthalten (z. B. `\\fileserver_one\software\adobe.exe`). Sie können die Prüfsumme mit einem beliebigen Tool erstellen, unter anderem mit dem Programm KDeploy.exe, das mit dem KACE Agenten installiert wird. **So erstellen Sie eine Prüfsumme mit KDeploy.exe:** a. Öffnen Sie auf einem Gerät, auf dem der KACE Agent installiert ist, ein Eingabeaufforderungs- oder Terminalfenster. b. Öffnen Sie das Installationsverzeichnis von Quest KACE. Beispiel:

Option	Beschreibung
	Windows 32-Bit-Geräte: `C:\Programme\Quest\KACE` Windows 64-Bit-Geräte: `C:\Programme (x86)\Quest\KACE\` Mac OS X Geräte: `/Library/Application Support/Quest/KACE/bin` c. Geben Sie den folgenden Befehl ein: KDeploy -hash=**Dateiname** Wobei **Dateiname** für den UNC-Pfad der Datei steht. Wenn der Pfad Leerzeichen enthält, geben Sie den gesamten Pfad in doppelten Anführungszeichen an. d. Drücken Sie **STRG+C** bzw. **Befehlstaste +C**, um die MD5-Prüfsumme zu kopieren. Anschließend können Sie sie in andere Dateien kopieren, z. B. in Notepad. **Anmeldeinformationen**: Die Details des Dienstkontos, die erforderlich sind, um eine Verbindung zum Gerät herzustellen und Befehle auszuführen Wählen Sie vorhandene Anmeldeinformationen in der Dropdown-Liste aus oder wählen Sie **Neue Anmeldeinformationen hinzufügen** aus, um nicht bereits aufgeführte Anmeldeinformationen hinzuzufügen. Siehe Hinzufügen und Bearbeiten von Benutzer-/Kennwort-Anmeldeinformationen. **HINWEIS:** Wenn das Zielgerät einem Replikationslabel angehört, ruft die Appliance keine Anwendung von der alternativen Download-Quelle ab. Sie können ein vorhandenes Label bearbeiten oder ein Label erstellen, um den alternativen Speicherort global anzugeben. Da dieses Label keiner verwalteten Installation zugewiesen ist, können Sie keine alternative Prüfsumme angeben, die mit der Prüfsumme in der Remote-Dateifreigabe übereinstimmt. Siehe Verteilen von Paketen über alternative Download-Quellen und Replikationsfreigaben und Manuelle Labels hinzufügen oder bearbeiten.
Installationsbefehl	Optionen für den Installationsbefehl
Standardinstallation	Wählen Sie diese Option aus, wenn Sie eine RPM-Datei verwenden und die Appliance den Standardinstallationsbefehl ausführen soll. Linux Geräte verwenden: rpm [-U | Ausführungsparameter] "**Paketname**.tgz" **Ausführungsparameter**: (Optional) Wenn Sie **Standard verwenden** auswählen, müssen Sie die zu verwendenden Parameter angeben. Wenn Sie eine RPM-Datei verwenden, sind keine Ausführungsparameter erforderlich.

Option	Beschreibung
	Geben Sie einen Wert zum Überschreiben an (Standard `-U` Standard). Wenn Sie beispielsweise für die **Ausführungsparameter** den Wert -ivh --replacepkgs festlegen, lautet der Befehl, der auf dem Gerät ausgeführt wird, wie folgt: `rpm -ivh -replacepkgs package.rpm`
Standardinstallation überschreiben	Wählen Sie diese Option aus, um die vollständige Befehlszeile hier anzugeben. Wenn Sie eine Archivdatei verwenden, wird dieser Befehl für alle gefundenen RPM-Dateien ausgeführt.
Deinstallation	Entfernen Sie das Paket über die Befehlszeile vom Gerät. Wenn Sie im Feld *Vollständige Befehlszeile* einen Befehl angegeben haben, wird dieser ausgeführt. Andernfalls versucht der KACE Agent, den Befehl auszuführen, der in der Regel zum Entfernen des Pakets erwartet wird.
Nur Befehl ausführen (Datei nicht herunterladen)	Es wird nur der Befehl ausgeführt. Damit wird das eigentliche digitale Asset nicht heruntergeladen.
Heruntergeladene Dateien löschen	Löscht die Dateien, wenn die Bereitstellung abgeschlossen ist.
ITNinja	Bereitstellungstipps von ITNinja. Diese Tipps sind nur verfügbar, wenn Sie Nutzungsdaten weitergeben. Siehe Konfigurieren der Datenfreigabeeinstellungen.

4. Legen Sie die Bereitstellungseinstellungen fest:

Option	Beschreibung
Alle Geräte	Stellen Sie die Funktion auf allen Geräten bereit. Deaktivieren Sie das Kontrollkästchen, um die Bereitstellung auf bestimmte Labels oder Geräte zu beschränken.
Labels	Beschränken Sie die Bereitstellung auf Geräte, die zu angegebenen Labels gehören. Klicken Sie zum Auswählen von Labels auf **Bearbeiten**, ziehen Sie die Labels ins Fenster *Bereitstellung beschränken auf* und klicken Sie dann auf **Speichern**. Wenn Sie ein Label auswählen, das über eine Replikationsfreigabe oder eine alternative Download-Quelle verfügt, werden digitale Assets aus dieser Replikationsfreigabe oder aus dieser alternativen Download-Quelle kopiert und nicht direkt von der Appliance heruntergeladen. **HINWEIS:** Die Appliance nutzt eine Replikationsfreigabe, bevor sie den Alternativen KACE Speicherort verwendet.

Option	Beschreibung
Geräte	Beschränken Sie die Bereitstellung auf bestimmte Geräte. Wählen Sie aus der Dropdown-Liste die Geräte aus, auf denen Sie die Anwendung bereitstellen möchten. Um die Liste zu filtern, geben Sie einige Zeichen ins Feld *Geräte* ein. Die Zahl neben dem Feld zeigt die Anzahl der verfügbaren Geräte an. **HINWEIS: Nur ungenutzte Softwarelizenzen zurückgewinnen.** Alle Geräte, von denen Sie die Software entfernen möchten, werden aufgeführt. Sie können die Liste der Geräte nach Bedarf bearbeiten. Um die Software von allen Geräten zu entfernen, wählen Sie einfach, wie oben beschrieben. Weitere Informationen hierzu finden Sie unter Rückgewinnen ungenutzter Softwarelizenzen.

5. Geben Sie die folgenden Benutzerbenachrichtigungseinstellungen an:

Option	Beschreibung
Benutzer vor der Ausführung benachrichtigen	Mit dieser Option wird auf verwalteten Geräten vor der Installation eine Meldung angezeigt. Wenn Sie diese Option auswählen, werden die folgenden Felder angezeigt: • **Meldung**: Die Meldung, die auf verwalteten Geräten vor Beginn der Installation angezeigt wird. • **Timeout**: Die Zeitdauer in Minuten, für die die Meldung angezeigt werden soll. • **Aktion**: Die Aktion, die am Ende der Zeitspanne für den **Timeout der ersten Meldung** ausgeführt wird. Die Optionen **Später installieren** und **Jetzt installieren** sind verfügbar. Wählen Sie **Jetzt installieren**, um die Anwendung sofort zu installieren, oder **Später installieren**, um die Installation bis zu einer Benutzerreaktion zu verschieben. „Später installieren“ ist nützlich, wenn Sie Benutzer vor einer Installation oder einem Neustart darüber benachrichtigen möchten.
Erste Meldung	Mit dieser Option wird auf verwalteten Geräten vor der Installation eine Meldung angezeigt. Wenn Sie

Option	Beschreibung
	diese Option auswählen, werden die folgenden Felder angezeigt: • **Meldung**: Die Meldung, die auf verwalteten Geräten vor Beginn der Installation angezeigt wird. • **Timeout**: Die Zeitdauer in Minuten, für die die Meldung angezeigt werden soll. • **Aktion**: Die Aktion, die am Ende der Zeitspanne für den **Timeout der ersten Meldung** ausgeführt wird. Die Optionen **Später installieren** und **Jetzt installieren** sind verfügbar. Wählen Sie **Jetzt installieren**, um die Anwendung sofort zu installieren, oder **Später installieren**, um die Installation bis zu einer Benutzerreaktion zu verschieben. „Später installieren“ ist nützlich, wenn Sie Benutzer vor einer Installation oder einem Neustart darüber benachrichtigen möchten.
Abschlussmeldung	Mit dieser Option wird auf verwalteten Geräten nach der Installation eine Meldung angezeigt. Wenn Sie diese Option auswählen, werden die folgenden Felder angezeigt: • **Meldung**: Die Meldung, die auf verwalteten Geräten nach Abschluss der Installation angezeigt wird. • **Timeout**: Die Zeitdauer in Minuten, für die die Meldung angezeigt werden soll.

6. Wählen Sie die Optionen für die Zeitplanung aus:

Option	Beschreibung
Bereitstellungsfenster Start Ende	Die Uhrzeit im 24-Stunden-Format für Beginn und Ende der Bereitstellung des Pakets. Die Uhrzeit im *Bereitstellungsfenster* wirkt sich auf alle Optionen unter *Aktion* aus. Zudem setzen die in der Appliance unter *Einstellungen* definierten Ausführungsintervalle die Angaben im Bereitstellungsfenster bestimmter Pakete außer Kraft oder treten in Wechselwirkung mit diesen Angaben.
Reihenfolge	Die Reihenfolge, in der die Anwendung installiert oder deinstalliert werden soll. Die Software mit dem niedrigsten Wert wird als Erstes bereitgestellt. Wenn die Installations- und die Deinstallationsaktion beide denselben Reihenfolgenwert haben, wird zuerst die Deinstallationsaktion ausgeführt.

Option	Beschreibung
	HINWEIS: Verwaltete Installationen werden immer der Reihenfolge nach bereitgestellt, unabhängig davon, ob die angegebenen Softwarepakete aus dem Softwarekatalog oder aus der Softwareliste stammen. Verwaltete Installationen mit einer niedrigeren Bereitstellungsreihenfolge verhindern immer, dass andere verwaltete Installationen ausgeführt werden, bis sie erfolgreich installiert wurden oder die angegebenen Wiederholungsversuche überschreiten.
Maximale Anzahl Versuche	Die maximale Anzahl der Versuche für die Installation des Pakets durch die Appliance (zwischen 0 und 99). Wenn Sie 0 angeben, versucht die Appliance unbegrenzt, das Paket zu installieren.

7. Klicken Sie auf **Speichern**.

Verwaltete Installationen für TAR.GZ-Dateien erstellen

Bei der Bereitstellung von Software mithilfe einer TAR.GZ-Datei können Sie komfortabel ein Softwarepaket erstellen, falls zum Bereitstellen eines bestimmten Softwaretitels mehrere Dateien erforderlich sind.

Einige Anwendungen benötigen mehrere Dateien für die Bereitstellung (beispielsweise RPM-, Konfigurations- und Datendateien). Diese Dateien können Sie in einer TAR.GZ-Datei zusammenfassen, an die Appliance hochladen und verwaltete Installationen mit den TAR.GZ-Dateien erstellen.

Wenn Sie Anwendungen an verwaltete Geräte verteilen möchten, müssen Sie den Anwendungen die digitalen Assets, d. h. die für die Installation erforderlichen Dateien, zuordnen. Darüber hinaus müssen Sie die unterstützten Betriebssysteme für die Anwendungen auswählen. Siehe Digitale Assets an Anwendungen anhängen und unterstützte Betriebssysteme auswählen.

1. Verwenden Sie die beiden folgenden Befehle, um eine TAR.GZ-Datei zu erstellen:
   a. `tar -cvf` **Dateiname**`.tar` **Paketname**`.rpm`
   b. `gzip` **Dateiname**`.tar`

   Damit wird die Datei **Dateiname**`.tar.gz` erstellt.
2. Melden Sie sich an der Administratorkonsole der Appliance an.
3. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
4. Erstellen Sie ein Inventarelement für die Zielbereitstellung.

   Sie können diesen Vorgang manuell über die Seite *Inventar* > *Software* durchführen oder das Paket auf einem verwalteten Gerät installieren, das regelmäßig eine Verbindung mit der Appliance herstellt. Siehe Informationen zur Seite "Software".
5. Verknüpfen Sie die TAR.GZ-Datei mit dem Inventarelement und laden Sie diese auf die Appliance hoch:
   a. Klicken Sie in der linken Navigationsleiste auf **Verteilung** und anschließend auf **Verwaltete Installationen**.
   b. Wählen Sie **Aktion auswählen** > **Neu**.
   c. Wählen Sie in der Dropdown-Liste *Software* den Anwendungstitel aus, mit dem die TAR.GZ-Datei verknüpft ist.

Während der Installation wird die Datei entpackt und der Installationsbefehl wird für jedes RPM-Paket ausgeführt.

Wenn keine *Ausführungsparameter* angegeben sind, wird `-U` verwendet.

Sie müssen keine vollständige Befehlszeile angeben. Die Appliance führt den Installationsbefehl selbständig aus. Das Linux Gerät versucht, die Installation mit folgendem Befehl auszuführen:

`rpm [-U | Ausführungsparameter] "`**Paketname**`.tgz"`

d. **Optional**: Wenn Sie mehrere Dateien haben, können Sie sie in einem ZIP-Archiv verpacken und die Appliance anweisen, das Archiv zu entpacken und eine bestimmte Datei auszuführen.

Geben Sie dazu den Namen der Datei, die ausgeführt werden soll, in das Feld "Befehl (Ausführbare Datei)" im Bereitstellungspaket ein (beispielsweise runthis.exe). Stellen Sie weitere Details zum Paket bereit. Siehe Verwenden verwalteter Installationen.

e. Klicken Sie auf **Speichern**.

Der KACE Agent führt Bereitstellungspakete mit der Erweiterung RPM automatisch aus.

Verwaltete Installationen für Mac OS X Geräte erstellen

Sie können verwaltete Installationen für Mac OS X Geräte nach Bedarf erstellen.

Wenn Sie Anwendungen an verwaltete Geräte verteilen möchten, müssen Sie der Anwendung die digitalen Assets, d. h. die für die Installation erforderlichen Dateien, zuordnen. Darüber hinaus müssen Sie die unterstützten Betriebssysteme für die Anwendung auswählen. Siehe Digitale Assets an Anwendungen anhängen und unterstützte Betriebssysteme auswählen.

1. Rufen Sie die *Detailseite für verwaltete Installation* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Verteilung** und anschließend auf **Verwaltete Installationen**.
   c. Wählen Sie **Aktion auswählen** > **Neu**.
2. Wählen Sie die Anwendung in der Dropdown-Liste *Software* aus.

   Der KACE Agent versucht standardmäßig, die PKG-Datei mithilfe des folgenden Befehls zu installieren:

   ```
   installer -pkg packagename.pkg -target / [Run Parameters]
   ```

   Wenn Sie eine DMG-, ZIP- oder TGZ-Datei ausgewählt haben, wird der Inhalt entpackt und das Stammverzeichnis nach allen PKG-Dateien durchsucht. Der Installationsbefehl wird für jede dieser PKG-Dateien ausgeführt und die Dateien werden in alphabetischer Reihenfolge verarbeitet.

   Danach sucht die Appliance nach allen ungepackten Anwendungen (APP) auf der obersten Ebene des Archivs und kopiert sie mit folgendem Befehl in den Ordner *Programme*:

   ```
   ditto -rscs Application.app /Applications/Application.app
   ```

   Zum Ausführen eines Skripts oder zum Ändern einer dieser Befehlszeilen können Sie den entsprechenden Skriptaufruf als **vollständige Befehlszeile** angeben. In den Dateinamen, die Sie verwenden, können Sie Platzhalter angeben. Schließen Sie den Dateinamen in einfache oder doppelte Anführungszeichen ein, falls er Leerzeichen enthält. Die Dateien werden in ein Verzeichnis unter `/tmp` extrahiert, das zum aktuellen Arbeitsverzeichnis des Befehls wird.

   TIPP: Wenn Sie das Skript nur unter Mac OS X ausführen möchten, müssen Sie Ihrem Archiv keine anderen Dateien hinzufügen.
3. Wenn das Paket weitere Optionen erfordert, geben Sie die folgenden Informationen an:

Option	Beschreibung
Name	Ein Name, der die verwaltete Installation identifiziert. Dieser Name wird auf der Seite *Verwaltete Installationen* angezeigt.
Ausführung	Die Einstellung für die Paketbereitstellung. Zur Auswahl stehen folgende Optionen: • **Deaktiviert**: Das Paket nicht bereitstellen. • **Jederzeit**: Das Paket bei der nächsten Gelegenheit bereitstellen, z. B. wenn der KACE Agent Inventarinformationen an die Appliance meldet. • **Beim Start**: Das Paket beim nächsten Starten des Geräts bereitstellen. **HINWEIS:** Wenn auf einem Gerät eine Active Directory- oder Gruppenrichtlinienobjekt-Einstellung aktiv ist, mit der eine Meldung angezeigt wird, die der Benutzer vor dem Anmelden bestätigen muss, werden keine Pakete bereitgestellt und keine Skripte ausgeführt, bevor die Bestätigung erfolgt ist. • **Nach dem Anmelden**: Das Paket bereitstellen, nachdem der Benutzer sich angemeldet hat, jedoch bevor der Desktop lädt. • **Bei angemeldetem Benutzer**: Das Paket bereitstellen, während der Benutzer angemeldet ist. • **Bei abgemeldetem Benutzer**: Das Paket nur bereitstellen, wenn das Gerät läuft und der Benutzer abgemeldet ist.
Inventar	Geben Sie an, ob Sie den Softwaretitel von **Katalogisierter Software** oder sämtlicher **Software** hinzufügen wollen, indem Sie eine der Optionen wählen. • Um nach einem bestimmten Titel zu suchen, beginnen Sie mit der Eingabe in das Feld *Software* oder *Katalogisierte Software*. **HINWEIS: Nur ungenutzte Softwarelizenzen zurückgewinnen.** Der Name der Software, die Sie deinstallieren möchten, wird standardmäßig in diesem Feld angezeigt. Weitere Informationen hierzu finden Sie unter Rückgewinnen ungenutzter Softwarelizenzen. • Wenn nur die Software mit einer oder mehreren verknüpften Dateien anzeigen

Option	Beschreibung
	wollen, wählen Sie **Nur Software mit einer zugehörigen Datei anzeigen**.
Zugehörige Datei	Software und katalogisierte Software können je nach Bedarf über eine oder mehrere Dateien als Anlage verfügen. Geben Sie an, ob Sie eine bestimmte Datei, die mit dem gewählten Softwaretitel verknüpft ist, wählen möchten. • **Zugehörige Datei auswählen**: Wählen Sie diese Option, wenn Sie eine Datei zuordnen möchten. Sie können eine Datei aus der Liste wählen. Wenn Sie den Dateiname kennen, geben Sie diesen in das Feld ein, und wählen sie unter den verfügbaren Einträge der Liste aus. • **Datei nicht verknüpfen**: Wählen Sie diese Option, wenn Sie eine Datei nicht zuordnen möchten.
Alternativer Speicherort	Geben Sie eine Download-Quelle für eine bestimmte verwaltete Installation an. **Pfad**: Geben Sie die Quelle ein, von der der KACE Agent digitale Installationsdateien abrufen kann. **Prüfsumme**: Geben Sie eine alternative Prüfsumme (MD5) ein, die mit der MD5-Prüfsumme in der Remote-Dateifreigabe übereinstimmt. Wenn keine Prüfsumme eingegeben wird, muss das digitale Asset in der Dateifreigabe mit dem digitalen Asset übereinstimmen, das mit dem Bereitstellungspaket in der Appliance verknüpft ist. Zudem muss der Zielpfad den vollständigen Dateinamen enthalten (z. B. `\\fileserver_one\software\adobe.exe`). Sie können die Prüfsumme mit einem beliebigen Tool erstellen, unter anderem mit dem Programm KDeploy.exe, das mit dem KACE Agenten installiert wird. **So erstellen Sie eine Prüfsumme mit KDeploy.exe:** a. Öffnen Sie auf einem Gerät, auf dem der KACE Agent installiert ist, ein Eingabeaufforderungs- oder Terminalfenster. b. Öffnen Sie das Installationsverzeichnis von Quest KACE. Beispiel: Windows 32-Bit-Geräte: `C:\Programme\Quest\KACE` Windows 64-Bit-Geräte: `C:\Programme (x86)\Quest\KACE\` Mac OS X Geräte: `/Library/Application Support/Quest/KACE/bin` c. Geben Sie den folgenden Befehl ein: KDeploy -hash=**Dateiname** Wobei **Dateiname** für den UNC-Pfad der Datei steht. Wenn der Pfad Leerzeichen enthält,

Option	Beschreibung
	geben Sie den gesamten Pfad in doppelten Anführungszeichen an. d. Drücken Sie **STRG+C** bzw. **Befehlstaste +C**, um die MD5-Prüfsumme zu kopieren. Anschließend können Sie sie in andere Dateien kopieren, z. B. in Notepad. **Anmeldeinformationen**: Die Details des Dienstkontos, die erforderlich sind, um eine Verbindung zum Gerät herzustellen und Befehle auszuführen Wählen Sie vorhandene Anmeldeinformationen in der Dropdown-Liste aus oder wählen Sie **Neue Anmeldeinformationen hinzufügen** aus, um nicht bereits aufgeführte Anmeldeinformationen hinzuzufügen. Siehe Hinzufügen und Bearbeiten von Benutzer-/Kennwort-Anmeldeinformationen. **HINWEIS:** Wenn das Zielgerät einem Replikationslabel angehört, ruft die Appliance keine Anwendung von der alternativen Download-Quelle ab. Sie können ein vorhandenes Label bearbeiten oder ein Label erstellen, um den alternativen Speicherort global anzugeben. Da dieses Label keiner verwalteten Installation zugewiesen ist, können Sie keine alternative Prüfsumme angeben, die mit der Prüfsumme in der Remote-Dateifreigabe übereinstimmt. Siehe Verteilen von Paketen über alternative Download-Quellen und Replikationsfreigaben und Manuelle Labels hinzufügen oder bearbeiten.

Standardinstallation	Sie müssen keinen Installationsbefehl angeben. Der Server führt den Installationsbefehl selbständig aus. Auf dem Mac OS X Gerät wird die Installation des Pakets mithilfe des folgenden Befehls versucht:
	`installer -pkg packagename.pkg -target / [Run Parameters]`
	oder
	`ditto -rsrc packagename.app /Applications/theapp`
	Wenn Sie eine Archivdatei angegeben haben, wird dieser Befehl für alle gefundenen PKG- bzw. APP-Dateien ausgeführt.

Standardinstallation überschreiben	Geben Sie die vollständigen Befehlszeilenparameter an. Verfügbare Laufzeitoptionen finden Sie in der Dokumentation zur MSI-Befehlszeile.

Option	Beschreibung
	HINWEIS: Bei Verwendung eines DMG-Pakets sollte sich die Befehlszeile auf den Dateipfad der gemounteten DMG-Datei beziehen. • **Deinstallieren**: Deinstallieren Sie die Anwendung über die Befehlszeile. • **Nur Befehl ausführen (Datei nicht herunterladen)**: Es wird nur der Befehl in der Befehlszeile ausgeführt. • **msiexec.exe nicht voranstellen**: Verhindert, dass die Appliance `msiexec.exe` am Anfang der Datei hinzufügt.
Heruntergeladene Dateien löschen	Löscht die Dateien, wenn die Bereitstellung abgeschlossen ist.
ITNinja	Bereitstellungstipps von ITNinja. Diese Tipps sind nur verfügbar, wenn Sie Nutzungsdaten weitergeben. Siehe Konfigurieren der Datenfreigabeeinstellungen.

HINWEIS: Die Benutzerbenachrichtigungsmeldungen stehen nicht auf Mac OS X Geräten zur Verfügung.

4. Legen Sie die Bereitstellungseinstellungen fest:

Option	Beschreibung
Alle Geräte	Stellen Sie die Funktion auf allen Geräten bereit. Deaktivieren Sie das Kontrollkästchen, um die Bereitstellung auf bestimmte Labels oder Geräte zu beschränken.
Labels	Beschränken Sie die Bereitstellung auf Geräte, die zu angegebenen Labels gehören. Klicken Sie zum Auswählen von Labels auf **Bearbeiten**, ziehen Sie die Labels ins Fenster *Bereitstellung beschränken auf* und klicken Sie dann auf **Speichern**. Wenn Sie ein Label auswählen, das über eine Replikationsfreigabe oder eine alternative Download-Quelle verfügt, werden digitale Assets aus dieser Replikationsfreigabe oder aus dieser alternativen Download-Quelle kopiert und nicht direkt von der Appliance heruntergeladen. **HINWEIS:** Die Appliance nutzt eine Replikationsfreigabe, bevor sie den Alternativen KACE Speicherort verwendet.
Geräte	Beschränken Sie die Bereitstellung auf bestimmte Geräte. Wählen Sie aus der Dropdown-Liste die Geräte aus, auf denen Sie die Anwendung bereitstellen möchten. Um die Liste zu filtern, geben Sie einige Zeichen ins Feld *Geräte* ein. Die Zahl

Option	Beschreibung
	neben dem Feld zeigt die Anzahl der verfügbaren Geräte an. **HINWEIS: Nur ungenutzte Softwarelizenzen zurückgewinnen.** Alle Geräte, von denen Sie die Software entfernen möchten, werden aufgeführt. Sie können die Liste der Geräte nach Bedarf bearbeiten. Um die Software von allen Geräten zu entfernen, wählen Sie einfach, wie oben beschrieben. Weitere Informationen hierzu finden Sie unter Rückgewinnen ungenutzter Softwarelizenzen.

5. Wählen Sie die Optionen für die Zeitplanung aus:

Option	Beschreibung
Bereitstellungsfenster Start Ende	Die Uhrzeit im 24-Stunden-Format für Beginn und Ende der Bereitstellung des Pakets. Die Uhrzeit im *Bereitstellungsfenster* wirkt sich auf alle Optionen unter *Aktion* aus. Zudem setzen die in der Appliance unter *Einstellungen* definierten Ausführungsintervalle die Angaben im Bereitstellungsfenster bestimmter Pakete außer Kraft oder treten in Wechselwirkung mit diesen Angaben.
Reihenfolge	Die Reihenfolge, in der die Anwendung installiert oder deinstalliert werden soll. Die Software mit dem niedrigsten Wert wird als Erstes bereitgestellt. Wenn die Installations- und die Deinstallationsaktion beide denselben Reihenfolgenwert haben, wird zuerst die Deinstallationsaktion ausgeführt. **HINWEIS:** Verwaltete Installationen werden immer der Reihenfolge nach bereitgestellt, unabhängig davon, ob die angegebenen Softwarepakete aus dem Softwarekatalog oder aus der Softwareliste stammen. Verwaltete Installationen mit einer niedrigeren Bereitstellungsreihenfolge verhindern immer, dass andere verwaltete Installationen ausgeführt werden, bis sie erfolgreich installiert wurden oder die angegebenen Wiederholungsversuche überschreiten.
Maximale Anzahl Versuche	Die maximale Anzahl der Versuche für die Installation des Pakets durch die Appliance (zwischen 0 und 99). Wenn Sie 0 angeben, versucht die Appliance unbegrenzt, das Paket zu installieren.

6. Klicken Sie auf **Speichern**.

Weitere Informationen finden Sie unter:

- Verteilen von Software und Verwenden von Wake on LAN
- Verwenden verwalteter Installationen

Dateisynchronisierungen erstellen und verwenden

Mithilfe von Dateisynchronisierungen können Sie beliebige Dateitypen auf Geräte mit Agentenverwaltung übertragen.

Mittels Dateisynchronisierungen können Sie Dateien an verwaltete Geräte verteilen. Im Gegensatz zu verwalteten Installationen werden bei Dateisynchronisierungen jedoch keine Dateien installiert, sondern lediglich verteilt. Mit Dateisynchronisierungen können Sie Dateien jedes Typs auf verwaltete Geräte kopieren.

Die Zeichenkette `KACE_ALT_Location` im Feld *Alternativer Speicherort* wird durch den zugewiesenen Wert des zugehörigen Labels ersetzt. Weisen Sie Geräten nicht mehrere Labels mit alternativem Speicherort zu.

1. Rufen Sie die Liste *Dateisynchronisierungen* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Verteilung** und anschließend auf **Dateisynchronisierungen**.
   c. Wählen Sie **Aktion auswählen** > **Neu**.

   Ist diese Option nicht verfügbar, enthält das Inventar keine Anwendungen mit den zugeordneten Dateien. Siehe Digitale Assets an Anwendungen anhängen und unterstützte Betriebssysteme auswählen.
2. Geben Sie im Bereich *Konfigurieren* die folgenden Informationen ein:

Option	Beschreibung
Aktiviert	Aktiviert die Dateisynchronisierung. Die Datei wird verteilt, sobald sich die KACE Agenten auf den ausgewählten Geräten bei der Appliance anmelden.
Name	Ein Name, der die Dateisynchronisierung identifiziert. Dieser Name wird auf der Seite *Dateisynchronisierungen* angezeigt.
Pfad	Der Verzeichnisort auf Zielgeräten, an dem Sie die Datei speichern möchten.
Pfad erstellen	Erstellen Sie das im Feld *Pfad* angegebene Verzeichnis, sofern es noch nicht vorhanden ist.
Anmeldeinformationen	Die Details des Dienstkontos, die erforderlich sind, um eine Verbindung zum Gerät herzustellen und Befehle auszuführen Wählen Sie vorhandene Anmeldeinformationen in der Dropdown-Liste aus oder wählen Sie **Neue Anmeldeinformationen hinzufügen** aus, um nicht bereits aufgeführte Anmeldeinformationen hinzuzufügen. Siehe Hinzufügen und Bearbeiten von Benutzer-/Kennwort-Anmeldeinformationen.
Datei	Die an die Zielgeräte zu verteilende Datei. Damit sie in der Liste aufgeführt werden, müssen im Inventar

Option	Beschreibung
	Dateien mit den Anwendungen verknüpft sein. Siehe Digitale Assets an Anwendungen anhängen und unterstützte Betriebssysteme auswählen.
Verteilung nicht dekomprimieren	Verhindert, dass die Appliance Dateien dekomprimiert.
Beibehalten	Bestätigen Sie, dass die Datei nicht bereits auf dem Zielgerät existiert, bevor Sie versuchen, sie zu verteilen.
Verknüpfung erstellen	Erstellen Sie eine Desktop-Verknüpfung zum Speicherort der Datei auf dem Gerät.
Name	Der Anzeigename der Desktop-Verknüpfung.
Temporäre Dateien löschen	Löscht die Dateien, wenn die Bereitstellung abgeschlossen ist.
ITNinja	Bereitstellungstipps von ITNinja. Diese Tipps sind nur verfügbar, wenn Sie Nutzungsdaten weitergeben. Siehe Konfigurieren der Datenfreigabeeinstellungen.

3. Legen Sie die Bereitstellungseinstellungen fest:

Option	Beschreibung
Alle Geräte	Stellen Sie die Funktion auf allen Geräten bereit. Deaktivieren Sie das Kontrollkästchen, um die Bereitstellung auf bestimmte Labels oder Geräte zu beschränken.
Labels	Beschränken Sie die Bereitstellung auf Geräte, die zu angegebenen Labels gehören. Klicken Sie zum Auswählen von Labels auf **Bearbeiten**, ziehen Sie die Labels ins Fenster *Bereitstellung beschränken auf* und klicken Sie dann auf **Speichern**. Wenn Sie ein Label auswählen, das über eine Replikationsfreigabe oder eine alternative Download-Quelle verfügt, werden digitale Assets aus dieser Replikationsfreigabe oder aus dieser alternativen Download-Quelle kopiert und nicht direkt von der Appliance heruntergeladen. **HINWEIS:** Die Appliance nutzt eine Replikationsfreigabe, bevor sie den Alternativen KACE Speicherort verwendet.
Geräte	Beschränken Sie die Bereitstellung auf bestimmte Geräte. Wählen Sie aus der Dropdown-Liste die Geräte aus, auf denen Sie die Anwendung bereitstellen möchten. Um die Liste zu filtern, geben Sie einige Zeichen ins Feld *Geräte* ein. Die Zahl

Option	Beschreibung
	neben dem Feld zeigt die Anzahl der verfügbaren Geräte an.
Erste Meldung	Mit dieser Option wird auf Geräten vor der Installation eine Meldung angezeigt.
Abschlussmeldung	Mit dieser Option wird auf verwalteten Geräten nach der Installation eine Meldung angezeigt.
Aussetzungsfenster	Der Zeitraum, in dem die Agenten auf den verwalteten Geräten keine Dateisynchronisierungen durchführen können.
Alternativer Speicherort	Geben Sie eine Download-Quelle für eine bestimmte verwaltete Installation an. **Pfad**: Geben Sie die Quelle ein, von der der KACE Agent digitale Installationsdateien abrufen kann. **Prüfsumme**: Geben Sie eine alternative Prüfsumme (MD5) ein, die mit der MD5-Prüfsumme in der Remote-Dateifreigabe übereinstimmt. Wenn keine Prüfsumme eingegeben wird, muss das digitale Asset in der Dateifreigabe mit dem digitalen Asset übereinstimmen, das mit dem Bereitstellungspaket in der Appliance verknüpft ist. Zudem muss der Zielpfad den vollständigen Dateinamen enthalten (z. B. `\\fileserver_one\software\adobe.exe`). Sie können die Prüfsumme mit einem beliebigen Tool erstellen, unter anderem mit dem Programm KDeploy.exe, das mit dem KACE Agenten installiert wird. **So erstellen Sie eine Prüfsumme mit KDeploy.exe:** a. Öffnen Sie auf einem Gerät, auf dem der KACE Agent installiert ist, ein Eingabeaufforderungs- oder Terminalfenster. b. Öffnen Sie das Installationsverzeichnis von Quest KACE. Beispiel: Windows 32-Bit-Geräte: `C:\Programme\Quest\KACE` Windows 64-Bit-Geräte: `C:\Programme (x86)\Quest\KACE\` Mac OS X Geräte: `/Library/Application Support/Quest/KACE/bin` c. Geben Sie den folgenden Befehl ein: KDeploy -hash=**Dateiname** Wobei **Dateiname** für den UNC-Pfad der Datei steht. Wenn der Pfad Leerzeichen enthält, geben Sie den gesamten Pfad in doppelten Anführungszeichen an. d. Drücken Sie **STRG+C** bzw. **Befehlstaste +C**, um die MD5-Prüfsumme zu kopieren. Anschließend können Sie sie in andere Dateien kopieren, z. B. in Notepad.

Option	Beschreibung
	Anmeldeinformationen: Die Details des Dienstkontos, die erforderlich sind, um eine Verbindung zum Gerät herzustellen und Befehle auszuführen Wählen Sie vorhandene Anmeldeinformationen in der Dropdown-Liste aus oder wählen Sie **Neue Anmeldeinformationen hinzufügen** aus, um nicht bereits aufgeführte Anmeldeinformationen hinzuzufügen. Siehe Hinzufügen und Bearbeiten von Benutzer-/Kennwort-Anmeldeinformationen. **HINWEIS:** Wenn das Zielgerät einem Replikationslabel angehört, ruft die Appliance keine Anwendung von der alternativen Download-Quelle ab. Sie können ein vorhandenes Label bearbeiten oder ein Label erstellen, um den alternativen Speicherort global anzugeben. Da dieses Label keiner verwalteten Installation zugewiesen ist, können Sie keine alternative Prüfsumme angeben, die mit der Prüfsumme in der Remote-Dateifreigabe übereinstimmt. Siehe Verteilen von Paketen über alternative Download-Quellen und Replikationsfreigaben und Manuelle Labels hinzufügen oder bearbeiten.

4. Klicken Sie auf **Speichern**.

TIPP: Um die zuvor bereitgestellten Dateien nach dem Schließen des Bereitstellungsfensters zu verteilen, rufen Sie die Seite *Dateisynchronisierungsdetails* für die Dateisynchronisierung auf. Klicken Sie anschließend unten auf der Seite auf **Dateien speichern und erneut senden**.

Verwenden von Wake on LAN

Mit Wake on LAN können Sie Geräte von einem Remote-Standort aus über die Appliance einschalten, unabhängig davon, ob der KACE Agent auf diesen Geräten installiert ist oder nicht.

HINWEIS: Um Wake on LAN zu verwenden, müssen Geräte mit einer Wake on LAN-fähigen Netzwerkkarte und einem Wake on LAN-fähigen BIOS ausgestattet sein.

Für Wake on LAN überträgt die Appliance UDP-Datenverkehr in Ihrem Netzwerk an Port 7. Die Appliance sendet 16 Pakete pro Wake on LAN-Anforderung, da sie die Broadcast-Adresse erraten muss, die zum Übertragen des "magischen Pakets" auf das Zielgerät benötigt wird. Der Datenverkehr wird von Geräten, die nicht von einem Remote-Standort aus eingeschaltet werden, ignoriert und sollte keine nennenswerten Auswirkungen auf das Netzwerk haben.

Sie können Geräte einschalten, die zum selben Subnetz wie die Appliance gehören oder sich in anderen Subnetzen befinden. Um ein Gerät einzuschalten, das mit einem anderen Subnetz verbunden ist, müssen Sie einen KACE Agent als ein Wake on LAN-Relay festlegen.

Wake on LAN-Anforderungen ausgeben

Sie können Geräte einzeln aktivieren oder ein Label angeben, dem mehrere Geräte angehören, und so mehrere Geräte gleichzeitig aktivieren.

Falls das zu aktivierende Gerät nicht im Inventar der Appliance erfasst ist, Sie jedoch dessen MAC-Adresse (Hardwareadresse) und die letzte verwendete IP-Adresse des Geräts kennen, können Sie die Informationen zum Aktivieren des Geräts manuell eingeben.

1. Rufen Sie die Liste *Wake-on-LAN-Zeitpläne* auf.
    a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
    b. Klicken Sie in der linken Navigationsleiste auf **Verteilung** und anschließend auf **Wake on LAN**.
2. Wählen Sie **Aktion auswählen** > **Neu** > **Einfach**.
3. Wählen Sie die Art des zu verwendenden Geräts aus:
    - **Um Geräte mit Labels zu aktivieren, wählen Sie in der Dropdown-Liste** *Labels* **ein Label aus.**
    - **Um einzelne Geräte zu aktivieren, wählen Sie die Geräte im Feld** *Verwaltete Geräte* **aus. Um die Liste zu durchsuchen, tippen Sie in das Feld.**
    - **Um erkannte Geräte zu aktivieren, wählen Sie die Geräte im Feld** *Erkannte Geräte* **aus. Um die Liste zu durchsuchen, tippen Sie in das Feld.**
4. Um Informationen zum Gerät manuell einzugeben, gehen Sie folgendermaßen vor:
    - **Geben Sie im Feld** *IP-Adresse* **die IP-Adresse eines Geräts an.**
    - **Geben Sie im Abschnitt** *Manuelle Eingabe* **die MAC-Adresse des entsprechenden Geräts an.**
5. Klicken Sie auf **Jetzt ausführen**.

Die Ergebnisse oben auf der Seite geben die Anzahl der Geräte an, die die Anforderung erhalten haben, sowie ggf. die Labels, denen diese Geräte angehören.

Wake on LAN-Anforderungen planen

Ein Zeitplan für eine Wake on LAN-Anforderung ist sinnvoll, wenn Sie Geräte regelmäßig aktivieren möchten. Dies ist hilfreich bei sich wiederholenden Aufgaben (wie etwa der monatlichen Wartung).

Wenn Sie Geräte einschalten möchten, die sich in einem anderen Subnetz befinden, müssen Sie eine Maschine finden, die zu dem Subnetz des Geräts gehört und auf dem eine KACE Agent-Instanz ausgeführt wird. Anschließend müssen Sie diese Maschine als Relay festlegen, indem Sie ihr ein Label zuweisen. Weitere Informationen zu Labels finden Sie unter Einrichten und Verwenden von Labels für die Verwaltung von Elementgruppen.

1. Rufen Sie die Liste *Wake-on-LAN-Zeitpläne* auf:
    a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
    b. Klicken Sie in der linken Navigationsleiste auf **Verteilung** und anschließend auf **Wake on LAN**.
2. Wählen Sie **Aktion auswählen** > **Neu** > **Erweitert**.
3. Wählen Sie die Art des zu verwendenden Geräts aus:
    - **Um Geräte zu wählen, die zu Labels gehören, klicken Sie im Abschnitt** *Konfigurieren* **unter** *Labels* **auf Verknüpfte Labels verwalten. Wählen Sie in dem nun angezeigten Dialogfeld** *Labels*

auswählen **ein oder mehrere Labels aus, die mit den einzuschaltenden Geräten verknüpft sind. Schließen Sie das Dialogfeld.**

- **Um Geräte über das Betriebssystem zu wählen, klicken Sie auf Verwaltung von Betriebssystemen. Wählen Sie im daraufhin angezeigten Dialogfeld Betriebssysteme die Betriebssystemversionen in der Navigationsstruktur aus.**

  Sie haben die Möglichkeit, Betriebssystemversionen nach Familie, Produkt, Architektur, Versions-ID oder Build-Version auszuwählen. Je nach Bedarf können Sie eine bestimmte Build-Version oder einen übergeordneten Knoten auswählen. Wenn Sie einen übergeordneten Knoten im Baum auswählen, werden die zugehörigen untergeordneten Knoten automatisch mit ausgewählt. Aufgrund dieses Verhaltens können Sie beliebige zukünftige Betriebssystemversionen auswählen, da Geräte in Ihrer verwalteten Umgebung hinzugefügt oder aktualisiert werden. Wenn Sie beispielsweise alle aktuellen und zukünftigen Versionen auswählen möchten, die mit der Windows 10 x64-Architektur verbunden sind, wählen Sie unter **Alle** > **Windows** > **Windows 10** die Option **x64** aus.

4. Um ein Gerät einzuschalten, das zu einem anderen Subnetz gehört, wählen Sie eine Relay-Maschine aus.
   a. Klicken Sie im Abschnitt *Konfigurieren* unter *Relay-Labels* auf **Verknüpfte Labels verwalten**.
   b. Wählen Sie im nun angezeigten Dialogfeld *Labels auswählen* das mit dem Relay-Gerät verknüpfte Label aus.
   c. Schließen Sie das Dialogfeld.
5. Auf der Seite *Wake on LAN-Einstellungen* geben Sie im Abschnitt *Zeitplan* folgende Zeitplanungseinstellungen an:

Option	Beschreibung
Kein(e)	Die Ausführung erfolgt im Zusammenhang mit einem Ereignis anstatt zu einem bestimmten Datum oder zu einem bestimmten Zeitpunkt.
jede Stunde	Der Vorgang wird im angegebenen Intervall durchgeführt.
Täglich/an einem bestimmten Tag um HH:MM	Die Erfassung wird täglich zu einem bestimmten Zeitpunkt oder an einem bestimmten Wochentag um eine bestimmte Uhrzeit ausgeführt.
Ausführen am n-ten jedes Monats/eines bestimmten Monats um HH:MM	Die Erfassung wird jeden Monat oder in einem bestimmten Monat an einem festgelegten Datum zu einer festgelegten Uhrzeit ausgeführt.
Ausführen am n-ten Wochentag **jedes Monats/ eines bestimmten Monats um HH:MM**	Die Erfassung wird jeden Monat oder in einem bestimmten Monat an einem festgelegten Wochentag zu einer festgelegten Uhrzeit ausgeführt.

Benutzerdefiniert	Führen Sie die Erfassung nach einem benutzerdefinierten Zeitplan aus.
	Verwenden Sie das Standard-5-Feld-Cron-Format (das erweiterte Cron-Format wird nicht unterstützt):
	`* * * * *`
	`| | | | +————————Wochentag (0-6) (Sonntag=0)`
	`| | | +————————Monat (1-12)`
	`| | +————————Monatstag (1-31)`
	`| +————————Stunde (0-23)`
	`+————————Minute (0-59)`

Option	Beschreibung
	Verwenden Sie bei der Angabe von Werten die folgenden Zeichen: • **Leerzeichen( )**: Die einzelnen Felder mit einem Leerzeichen trennen. • **Sternchen (*)**: Ein Sternchen repräsentiert den gesamten Wertebereich in einem Feld. Zum Beispiel repräsentiert ein Sternchen im Stundenfeld eine beliebige Stunde. • **Kommas (,)**: Mehrere Werte in einem Feld werden mit einem Komma getrennt. Zum Beispiel werden mit `0,6` im Feld „Wochentag“ Sonntag und Samstag angegeben. • **Bindestriche (-)**: Mit einem Bindestrich wird ein Wertebereich in einem Feld angegeben. Zum Beispiel entspricht `1-5` im Feld „Wochentag“ `1,2,3,4,5`, d. h. Montag bis Freitag. • **Schrägstriche (/)**: Die Angabe der Zeitabstände, mit denen eine Aktion wiederholt werden soll, erfolgt mit einem Schrägstrich. Zum Beispiel entspricht `*/3` im Feld Stunde `0,3,6,9,12,15,18,21`. Das Sternchen (`*`) gibt jede Stunde an, mit `/3` erfolgt aber eine Einschränkung auf durch drei teilbare Stunden. Beispiele: • `15 * * * * Jeden Tag 15 Minuten nach jeder vollen Stunde ausführen` • `0 22 * * * Jeden Tag um 22:00 Uhr ausführen` • `0 0 1 1,6 * Am 1. Januar und 1. Juni um 00:00 Uhr ausführen` • `30 8,12 * * 1-5 An Wochentagen um 08:30 Uhr und 12:30 Uhr ausführen` • `0 2 */2 * * Jeden zweiten Tag um 02:00 Uhr ausführen`
Aufgabenplan anzeigen	Klicken Sie, um den Aufgabenplan anzuzeigen. Im Dialogfeld *Aufgabenplan* wird eine Liste der geplanten Aufgaben angezeigt. Klicken Sie auf eine Aufgabe, um die Aufgabendetails anzuzeigen. Weitere Informationen hierzu finden Sie unter Aufgabenpläne anzeigen.

6. Klicken Sie auf **Speichern**.

Auf der Seite *Wake on LAN* wird die geplante Anforderung angezeigt.

Fehlerbehebung bei Wake on LAN

Unter bestimmten Bedingungen sind Wake on LAN-Anforderungen unter Umständen nicht erfolgreich.

Wake on LAN-Fehler können unter anderem in folgenden Fällen auftreten:

- Das Gerät ist nicht mit einer Wake on LAN-fähigen Netzwerkkarte ausgestattet oder wurde nicht ordnungsgemäß konfiguriert.
- Die Appliance verfügt über falsche Informationen zum Subnetz, an das das Gerät angeschlossen ist.
- UDP-Datenverkehr wird zwischen Subnetzen nicht weitergeleitet oder von einem Netzwerkgerät gefiltert.
- Broadcast-Datenverkehr wird zwischen Subnetzen nicht weitergeleitet oder von einem Netzwerkgerät gefiltert.
- Datenverkehr an Port 7 wird von einem Netzwerkgerät gefiltert.

Weitere Informationen hierzu finden Sie unter http://www.intel.com/content/www/us/en/support/network-and-i-o/ethernet-products/000005793.html.

Exportieren von verwalteten Installationen

Wenn Sie über mehrere Organisationen oder Appliances verfügen, können Sie verwaltete Installationen exportieren und nach Bedarf an andere Organisationen und Appliances übertragen.

Siehe Informationen zum Importieren und Exportieren von Anwendungsressourcen.

Senden von Warnungen an verwaltete Geräte

Sie können Warnungen in Form von Nachrichten an Benutzer senden. Diese werden dann als Popup-Meldungen auf Geräten mit Agentenverwaltung angezeigt.

Die Anzeige von Warnungen ist nützlich, wenn Sie dringende Informationen kommunizieren bzw. Benutzer über das bevorstehende Ausführen von Aktionen oder Skripten auf ihren Geräten informieren möchten.

Zudem können Sie E-Mail-Benachrichtigungen erstellen, die automatisch verschickt werden können, wenn die festgelegten Kriterien eingehalten werden. Siehe Zeitplanung für Benachrichtigungen.

HINWEIS: Das Anzeigen von Nachrichten auf verwalteten Geräten erfordert eine Verbindung zwischen dem Agenten und der Appliance. Informationen zu Verbindungen mit Agenten finden Sie unter Konfigurieren der Agenten-Einstellungen.

HINWEIS: Dieser Warnungstyp wird auf der Appliance generiert und an Geräte mit Agentenverwaltung gesendet. Überwachungswarnungen werden dagegen von Ihren Servergeräten an die Appliance übermittelt, sofern Sie auf den Geräten eine grundlegende Leistungsüberwachung aktiviert haben. Siehe Überwachen von Servern.

Zu sendende Warnungen erstellen

Bei Bedarf können Sie Warnungen für Geräte mit Agentenverwaltung erstellen und planen.

1. Rufen Sie die Seite *Warnungsdetail* auf:

a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://appliance_hostname/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.

b. Klicken Sie in der linken Navigationsleiste auf **Verteilung** und anschließend auf **Warnungen**.

c. Wählen Sie **Aktion auswählen > Neu**.

2. Geben Sie die folgenden Informationen an:

Option	Beschreibung
Meldung	Geben Sie den Inhalt der Benachrichtigung ein, die angezeigt werden soll. Die Meldung kann bis zu 500 Zeichen enthalten.
Alle Geräte	Zeigt die Meldung auf allen Geräten an, deren KACE Agenten mit der Appliance verbunden sind.
Dringend	Die Warnmeldung wird in der Mitte des Bildschirms angezeigt, ohne dass der Benutzer sie verschieben oder zurückstellen kann. Die Warnmeldung muss bearbeitet werden, bevor die Arbeit fortgesetzt werden kann.
Geräte	Die Benachrichtigung auf ausgewählten Geräten anzeigen Klicken Sie bei gedrückter **STRG**- oder **Befehls**-Taste, um mehrere Geräte auszuwählen.
Labels	Zeigt die Meldung nur auf Geräten an, die den ausgewählten Labels zugewiesen sind. Klicken Sie auf **Verknüpfte Labels verwalten**, um Gerätelabels auszuwählen. Klicken Sie bei gedrückter **STRG**- oder **Befehls**-Taste, um mehrere Labels auszuwählen.
Ablauf	Gibt den Zeitraum an, für den die Meldung gültig ist. Wenn die Zielgeräte mit der Appliance verbunden sind, wird die Benachrichtigung versendet und so lange angezeigt, bis der Benutzer sie durch Klicken auf **OK** bestätigt. **HINWEIS:** Falls ein Gerät nicht mit der Appliance verbunden ist, wird die Warnmeldung an die Warteschlange für Agentenbefehle gesendet und verbleibt dort, bis das Gerät eine Verbindung mit der Appliance herstellt. Wenn das Zielgerät eine Verbindung herstellt, wird die Meldung angezeigt, unabhängig davon, ob der *Ablauf*-Zeitraum abgelaufen ist oder nicht.

3. Geben Sie im Abschnitt *Zeitplan* folgende Zeitplanungseinstellungen an:

Option	Beschreibung
Kein(e)	Die Ausführung erfolgt im Zusammenhang mit einem Ereignis anstatt zu einem bestimmten Datum oder zu einem bestimmten Zeitpunkt.
Jeden	Die Ausführung erfolgt alle x Stunden.
Ausführen jeden Tag/an einem bestimmten Tag um HH:MM	Die Erfassung wird täglich zu einem bestimmten Zeitpunkt oder an einem bestimmten Wochentag um eine bestimmte Uhrzeit ausgeführt.
Ausführen am n-ten Wochentag **jedes Monats/ eines bestimmten Monats um HH:MM**	Die Erfassung wird jeden Monat oder in einem bestimmten Monat an einem festgelegten Datum zu einer festgelegten Uhrzeit ausgeführt.
Ausführen am n-ten Wochentag **jedes Monats/ eines bestimmten Monats um HH:MM**	Die Erfassung wird jeden Monat oder in einem bestimmten Monat an einem festgelegten Wochentag zu einer festgelegten Uhrzeit ausgeführt.

Benutzerdefiniert	Ausführung nach einem benutzerdefinierten Zeitplan.
	Verwenden Sie das Standard-5-Feld-Cron-Format (das erweiterte Cron-Format wird nicht unterstützt):
	`* * * * *`
	`| | | | +————Wochentag (0-6) (Sonntag=0)`
	`| | | +————Monat (1-12)`
	`| | +————Monatstag (1-31)`
	`| +————Stunde (0-23)`
	`+————Minute (0-59)`
	Verwenden Sie bei der Angabe von Werten die folgenden Zeichen:
	• **Leerzeichen( )**: Die einzelnen Felder mit einem Leerzeichen trennen.
	• **Sternchen (*)**: Ein Sternchen repräsentiert den gesamten Wertebereich in einem Feld. Zum Beispiel repräsentiert ein Sternchen im Stundenfeld eine beliebige Stunde.
	• **Kommas (,)**: Mehrere Werte in einem Feld werden mit einem Komma getrennt. Zum Beispiel werden mit `0,6` im Feld „Wochentag“ Sonntag und Samstag angegeben.
	• **Bindestriche (-)**: Mit einem Bindestrich wird ein Wertebereich in einem Feld angegeben. Zum Beispiel entspricht `1-5` im Feld „Wochentag“ `1,2,3,4,5`, d. h. Montag bis Freitag.
	• **Schrägstriche (/)**: Die Angabe der Zeitabstände, mit denen eine Aktion wiederholt werden soll, erfolgt mit einem Schrägstrich. Zum Beispiel entspricht `*/3` im Feld Stunde `0,3,6,9,12,15,18,21`. Das Sternchen (`*`) gibt jede Stunde an, mit `/3`

Option	Beschreibung
	erfolgt aber eine Einschränkung auf durch drei teilbare Stunden. Beispiele: • `15 * * * *` Jeden Tag 15 Minuten nach jeder vollen Stunde ausführen • `0 22 * * *` Jeden Tag um 22:00 Uhr ausführen • `0 0 1 1,6 *` Am 1. Januar und 1. Juni um 00:00 Uhr ausführen • `30 8,12 * * 1-5` An Wochentagen um 08:30 Uhr und 12:30 Uhr ausführen • `0 2 */2 * *` Jeden zweiten Tag um 02:00 Uhr ausführen
Aufgabenplan anzeigen	Klicken Sie, um den Aufgabenplan anzuzeigen. Im Dialogfeld *Taskplan* wird eine Liste der geplanten Ziele angezeigt. Klicken Sie auf eine Aufgabe, um die Aufgabendetails anzuzeigen. Weitere Informationen hierzu finden Sie unter Aufgabenpläne anzeigen.

4. Klicken Sie auf **Speichern**.

Ausführen von Skripten auf verwalteten Geräten

Sie können Skripte erstellen und auf verwalteten Geräten ausführen, um Aufgaben zu automatisieren und Einstellungen zu konfigurieren.

Informationen zu Skripten

Skripte verfügen über eine Schnittstelle, über die Aufgaben, die in der Regel eine manuelle Ausführung oder fortgeschrittene Programmierung erfordern, ganz einfach durch Zeigen und Klicken ausgeführt werden können. Sie können Skripte erstellen und ausführen, um Aufgaben auf Zielgeräten im gesamten Netzwerk auszuführen.

Mit Skripten können beispielsweise folgende Aufgaben automatisiert werden:

- Konfigurieren der Energieverwaltungseinstellungen
- Installation von Software
- Überprüfen des Virenschutzstatus
- Ändern der Registrierungseinstellungen
- Erstellen eines Zeitplans für die Softwarebereitstellung

Sie können folgende Arten von Skripten erstellen:

Option	Beschreibung
Offline-KScripts	Skripte, die zu einem geplanten Zeitpunkt nach der Uhr des Zielgeräts ausgeführt werden. Offline-KScripts können auch dann ausgeführt werden, wenn die Zielgeräte nicht mit der Appliance verbunden sind, beispielsweise beim Gerätestart oder bei der Benutzeranmeldung. Sie können diese Skripte mit den Skriptvorlagen erstellen.
Online-KScripts	Skripte, die nur dann ausgeführt werden, wenn ein Zielgerät mit der Appliance verbunden ist. Die Ausführung von Online-KScripts erfolgt zu geplanten Zeitpunkten gemäß der Uhr der Appliance. Sie können diese Skripte mit den Skriptvorlagen erstellen.
Online-Shellskripts	Skripte, die gemäß der Uhr der Appliance zu geplanten Zeitpunkten ausgeführt werden, jedoch nur, wenn das Zielgerät mit der Appliance verbunden ist. Online-Shellskripts werden mithilfe einfacher textbasierter Skripte (Bash, Perl, Batch und andere) erstellt, die vom Betriebssystem des Zielgeräts unterstützt werden. Windows unterstützt Batchdateien und die verschiedenen vom jeweiligen Betriebssystem der Zielgeräte unterstützten Shellskript-Formate.

Jedes Skript besteht aus folgenden Komponenten:

- Metadaten.
- Abhängigkeiten, einschließlich aller unterstützenden Programmdateien, die für die Ausführung eines Skripts erforderlich sind, wie zum Beispiel ZIP- und BAT-Dateien.
- Zu befolgende Regeln, wie etwa Offline-KScripts und Online-KScripts.
- Auszuführende Aufgaben, wie etwa Offline-KScripts und Online-KScripts. Jedes Skript kann eine beliebige Anzahl von Aufgaben umfassen und Sie können festlegen, ob die einzelnen Aufgaben erfolgreich abgeschlossen sein müssen, bevor die nächste Aufgabe ausgeführt wird.
- Bereitstellungseinstellungen.
- Zeitplanungseinstellungen.

Skriptabhängigkeiten abrufen

Zu Skriptabhängigkeiten zählen Dateien und andere von Skripten verwendete Elemente. Wenn ein Skript Abhängigkeiten besitzt und sich diese auf den Zielgeräten befinden, werden diese Abhängigkeiten verwendet. Andernfalls werden Repositorys in einer bestimmten Reihenfolge nach Abhängigkeiten durchsucht.

Skripte rufen Abhängigkeiten vom Zielgerät und aus Repositorys in der folgenden Reihenfolge ab:

1. Zielgerät
2. Alternative Download-Quelle: (KACE_ALT_LOCATION)
3. Eine Replikationsfreigabe
4. Appliance

HINWEIS: Informationen zu alternativen Download-Quellen und Replikationsfreigaben finden Sie unter Verteilen von Paketen über alternative Download-Quellen und Replikationsfreigaben.

Änderungsnachverfolgung für Skripteinstellungen

Wenn Verlaufsabonnements zur Aufbewahrung von Informationen konfiguriert wurden, können Sie Details zu den an Einstellungen, Assets und Objekten vorgenommenen Änderungen anzeigen.

Diese Informationen beinhalten auch das Datum der Änderung und den Benutzer, der diese vorgenommen hat. Dies kann bei der Fehlerbehebung nützlich sein. Siehe Informationen zu den Verlaufseinstellungen.

Informationen zu Standardskripten

Standardskripte sind vorkonfigurierte Skripte, mit denen Sie die Inventarmeldung von Geräten erzwingen, das Debugging auf Geräten aktivieren oder deaktivieren, Geräte herunterfahren und andere Geräteaufgaben per Remotezugriff durchführen können.

Standardskripte

Skriptname	Beschreibung
Laufwerk C: defragmentieren	Defragmentiert Laufwerk C auf dem Gerät.
Anmeldung erzwingen	Erzwingt auf Windows-Geräten, auf denen der KACE Agent installiert ist, die Erstellung eines Inventars und die Synchronisierung mit der Appliance. **WICHTIG: Führen Sie "Anmeldung erzwingen" auf maximal 50 Geräten aus, da die Appliance ansonsten möglicherweise durch zu viele Anforderungen überlastet wird.**
Anmeldung erzwingen (Mac/Linux)	Erzwingt auf Mac/Linux Geräten, auf denen der KACE Agent installiert ist, die Erstellung eines Inventars und die Synchronisierung mit der Appliance. **WICHTIG: Führen Sie "Anmeldung erzwingen" auf maximal 50 Geräten aus, da die Appliance ansonsten möglicherweise durch zu viele Anforderungen überlastet wird.**
Fix für Inventarisierungsstartprogramme	Aufgrund eines fehlenden Registrierungseintrags wird auf einigen Geräten der gesamte Inhalt des Verzeichnisses "system32" als Startprogramme gemeldet. Mit diesem Skript wird ein fehlender Registrierungseintrag ergänzt.
Beispiel für einen DOS-Befehl ausgeben	Gibt den Befehl `DOS-DIR` auf einem Windows Gerät aus. Wird als Beispiel für die Ausführung eines DOS-Befehls verwendet.

Skriptname	Beschreibung
Beispiel für einen Mac Befehl ausgeben	Gibt den Befehl `AppDir.txt` aus, um den Inhalt des Mac OS X Anwendungsverzeichnisses aufzulisten. Wird als Beispiel für die Ausführung eines Befehls auf einem Mac OS X System verwendet.
Detaillierte DDPE-Bestandsaufnahme für K1000 aktivieren (Windows)	Legt einen Registrierungsschlüssel fest, der bewirkt, dass der Dell Data Protection | Encryption Agent Richtliniendaten auf das Dateisystem schreibt. So kann der KACE Agent eine ausführlichere Inventarerfassung durchführen. Windows PowerShell 2.0 oder höher ist erforderlich.
Deaktivierung der K1000 Remote-Steuerung	Deaktiviert die Remote-Steuerungsfunktion der Appliance unter Windows XP Professional durch die entsprechende Konfiguration der Terminaldienste.
Aktivierung der K1000 Remote-Steuerung	Aktiviert die Remote-Steuerungsfunktion der Appliance unter Windows XP Professional durch die entsprechende Konfiguration der Terminaldienste.
Für Wechseldatenträger Schreibschutz festlegen	Erlaubt die schreibgeschützte Bereitstellung von Wechseldatenträgern. Dadurch wird der unbefugte Zugriff auf Daten verhindert.
Für Wechseldatenträger Lese-Schreib-Berechtigung festlegen	Legt die Eigenschaften von Wechseldatenträgern so fest, dass sie mit Lese-Schreib-Berechtigung bereitgestellt werden können.
Skriptbeispiel für Nachrichtenfenster	Veranschaulicht die Verwendung des Nachrichtenfensters. Damit das Skript ordnungsgemäß funktioniert, muss es entsprechend gepaarte create/destroy-Befehle für Nachrichtenfenster enthalten. Das Nachrichtenfenster wird so lange angezeigt, bis eines der folgenden Ereignisse eintritt: • Der Benutzer verwirft die Nachricht. • Das Skript wird bis zum Ende ausgeführt. • Die Zeitspanne für die Sitzungs-Timeout läuft ab.
Mac in Standbymodus versetzen	Versetzt ein Mac OS X Gerät in den Standbymodus. **HINWEIS:** Dieses Skript wird von Mac OS X 10.5 und höher unterstützt. Es wird von früheren Versionen von Mac OS X nicht unterstützt.
KUID zurücksetzen	Löscht den Registrierungsschlüssel, der ein Windows Gerät identifiziert, sodass ein neuer Schlüssel generiert werden kann. Wird mithilfe des Registrierungskennzeichens `ResetKUIDRunOnce` nur einmal pro Gerät ausgeführt.

Skriptname	Beschreibung
Mac herunterfahren	Schaltet ein Mac OS X Gerät ab.
Mac mit Snooze herunterfahren	Ein Beispiel für ein Online-KScript, das es Administratoren mithilfe der Funktion **Benutzer vor der Ausführung benachrichtigen** ermöglicht, das Herunterfahren per Snooze zu verschieben.
Windows System herunterfahren	Gibt die Verzögerung in Sekunden an, während der die Nachricht in Anführungszeichen für den Benutzer angezeigt wird. Wenn der Parameter `-t` weggelassen wird, werden die Geräte sofort und automatisch heruntergefahren.
Windows System mit Snooze herunterfahren	Ein Beispiel für ein Online-KScript, das es dem Administrator mithilfe der Funktion **Benutzer vor der Ausführung benachrichtigen** ermöglicht, das Herunterfahren per Snooze zu verschieben.
USB-Laufwerke deaktivieren	Deaktiviert die Verwendung von USB-Laufwerken
USB-Laufwerke aktivieren	Aktiviert die Verwendung von USB-Laufwerken

Hinzufügen und Bearbeiten von Skripten

Sie können Skripte mithilfe der **Administratorkonsole** hinzufügen oder bearbeiten.

Führen Sie zum Hinzufügen oder Bearbeiten von Skripten eine der folgenden Aktionen aus:

- Importieren eines vorhandenen Skripts im XML-Format. Siehe Struktur für importierbare Skripte.
- Duplizieren eines vorhandenen Skripts. Siehe Skripte duplizieren.
- Erstellen eines Skripts. Siehe Offline-KScripts, Online-KScripts oder Online-Shellskripte hinzufügen.

TIPP: Bei der Erstellung von Skripten wird iterativ vorgegangen. Nachdem Sie ein Skript erstellt haben, sollten Sie es auf einer begrenzten Anzahl von Geräten bereitstellen, um zu prüfen, ob es wie erwartet ausgeführt wird, bevor Sie es auf allen verwalteten Geräten bereitstellen. Für diese Überprüfung können Sie ein Test-Label erstellen. Skripte sollten erst nach dem Testen aktiviert werden.

Token-Ersetzungsvariablen

Verwenden Sie Token-Ersetzungswerte, um Skripten Variablen hinzuzufügen. Die folgende Liste zeigt die Token-Ersetzungswerte, die im Skript-XML verwendet werden kann. Diese Variablen werden während der Laufzeit auf dem Gerät durch zutreffende Werte ersetzt.

Token-Ersetzungswerte

Element	Beschreibung
$(KACE_DEPENDENCY_DIR)	Dies ist der Ordner, in dem alle Skript-Abhängigkeiten für dieses Skript auf den Client heruntergeladen werden.

Element	Beschreibung
	5.2 oder höher: `$(KACE_DATA_DIR)\kbots_cache\packages\kbots\xxx` **5.1**:`$(KACE_INSTALL)\packages\kbots\xxx`
$(KACE_SYS_DIR) **$(KBOX_SYS_DIR)**	Systemverzeichnis des Agentengeräts. Beide sind synonym. Bevorzugt: **$(KACE_SYS_DIR)**. **Windows**: `C:\Windows\System32` **Mac OS X**: `/` **Linux**: `/`
$(KACE_MAC_ADDRESS) **$(MAC_ADDRESS)** **$(KBOX_MAC_ADDRESS)**	Primäre Ethernet-MAC-Adresse des Agentengeräts. Sie sind alle synonym. Bevorzugt: **$(KACE_MAC_ADDRESS)**
$(KACE_IP_ADDRESS) **$(KBOX_IP_ADDRESS)**	Lokale IP-Adresse des Agenten (entspricht dem Netzwerkeintrag für KACE_MAC_ADDRESS) (`http://kace.kbox.com:80`). Beide sind synonym. Bevorzugt: **$(KACE_IP_ADDRESS)**
$(KACE_SERVER_URL)	Kombination aus Server, Port und URL-Präfix. (http://kace.kbox.com:80)
$(KACE_SERVER)	Hostname des Appliance-Servers. (kbox)
$(KACE_SERVER_PORT)	Port, der bei Verbindungsherstellung mit dem Appliance-Server verwendet werden soll. (80/433)
$(KACE_SERVER_URLPREFIX)	Webprotokoll, das bei der Verbindungsherstellung mit dem Appliance-Server verwendet werden soll. (http/https)
$(KACE_COMPANY_NAME)	Agentenkopie der Einstellung auf der Serverkonfigurationsseite.
$(KACE_KUID) **$(KBOX_MACHINE_ID)**	Die eindeutige, diesem Agenten zugewiesene Quest KACE ID. Beide sind synonym. Bevorzugt: **$(KACE_KUID)**
$(KACE_APP_DIR)	Das Installationsverzeichnis des Quest KACE Agenten und der Plug-Ins. Bei älteren Agenten ist dies **$(KACE_INSTALL)** zugeordnet. **Windows**: `C:\Programme\Quest\KACE` oder `C:\Programme (x86)\Quest\KACE` **Mac OS**: `/Library/Application Support/Quest/KACE/bin`

Element	Beschreibung
	Linux: `/opt/quest/kace/bin/`
$(KACE_DATA_DIR)	Installationsverzeichnis für ausführbare Dateien, Skripte, Pakete usw. Bei älteren Agenten ist dies **$(KACE_INSTALL)** zugeordnet. **Ab Windows Vista**: `C:\ProgramData\Quest\KACE` **Mac OS**: `/Library/Application Support/Quest/KACE/data` **Linux**: `/var/quest/kace`
$(KACE_AGENT_VERSION)	Ersetzt die Versionsnummer des installierten Agenten. „5.2.12345“. **Nur 5.2 oder höher**.
$(KACE_AGENT_ARCH)	Ersetzt die Architektur des installierten Agenten. „x86/x64“. **Nur 5.2 oder höher, Windows**.
$(KACE_HARDWARE_ARCH)	Ersetzt die Architektur der physischen Hardware. „x86/x64“. **Nur 5.2 oder höher, Windows**.
$(KACE_OS_FAMILY)	Ersetzt Windows, Mac oder Linux (abhängig vom Betriebssystem des Geräts mit Agentenverwaltung). **Nur 5.2 oder höher**.
$(KACE_OS_ARCH)	Ersetzt „x86“ oder „x64“ (abhängig von der installierten Version von Microsoft Windows). **Nur 5.2 oder höher, Windows**.

Offline-KScripts, Online-KScripts oder Online-Shellskripte hinzufügen

Sie können KScripts hinzufügen, die Geräte angeben, auf denen die Skripte ausgeführt werden sollen, und die Ausführung von Skripten nach Bedarf planen.

Offline- und Online-KScripts umfassen mindestens eine Aufgabe. Jeder *Aufgabenabschnitt* enthält Abschnitte zur *Überprüfung* und *Wiederherstellung*, in denen Sie das Skript-Verhalten näher definieren können. Wenn ein Abschnitt leer gelassen wird, wird er standardmäßig auf *Erfolg* eingestellt.

1. Rufen Sie die *Skriptdetailseite* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Skripterstellung** und anschließend auf **Skripte**.

c. Wählen Sie **Aktion auswählen** > **Neu**.

2. Legen Sie im Abschnitt *Konfiguration* die Skripteinstellungen fest:

Option	Beschreibung
Name	Ein aussagekräftiger Name für das Skript, der die Unterscheidung von den anderen auf der Registerkarte *Skripte* aufgeführten Skripten ermöglicht. **TIPP:** Sie können ein oder mehrere Skripte auf der Seite *Skripte* aktivieren oder deaktivieren. Wählen Sie dazu die gewünschten Optionen in der Tabelle aus, und klicken Sie auf, klicken Sie dann je nach Bedarf auf **Aktivieren** oder **Deaktivieren**.
Aktiviert	Wählen Sie aus, ob das Skript auf den Zielgeräten ausgeführt werden kann. Aktivieren Sie ein Skript erst, nachdem Sie es bearbeitet und getestet haben und es zur Ausführung bereit ist. Aktivieren Sie das Skript für ein Testlabel, bevor Sie es auf allen Geräten aktivieren.
Kategorie	Die Skriptkategorie. Wählen Sie eine vorhandene Kategorie aus der Dropdown-Liste aus, oder klicken Sie auf **Neue Kategorie**, um eine Kategorie hinzuzufügen. Wenn Sie diesem Skript keine Kategorie zuweisen möchten, stellen Sie sicher, dass dieses Feld auf **Keine** gesetzt ist. **TIPP:** Auf der Seite *Skripte* können Sie einem oder mehreren Skripts eine Kategorie zuweisen. Wählen Sie dazu die gewünschten Optionen in der Tabelle aus, klicken Sie auf **Aktion auswählen** > **Kategorie**, und wählen Sie dann eine Kategorie in der Liste aus.
Typ	Der Skripttyp. Es gibt folgende Skripttypen: • **Online-KScripts**: Skripte, die nur dann ausgeführt werden, wenn ein Zielgerät mit der Appliance verbunden ist. Die Ausführung von Online-KScripts erfolgt zu geplanten Zeitpunkten gemäß der Uhr der Appliance. Sie können diese Skripte mit den Skriptvorlagen erstellen. • **Offline-KScripts**: Skripte, die zu einem geplanten Zeitpunkt nach der Uhr des Zielgeräts ausgeführt werden. Diese Skripte können auch dann ausgeführt werden, wenn die Zielgeräte nicht mit der Appliance verbunden sind, beispielsweise beim Gerätestart oder bei der Benutzeranmeldung. Sie können diese Skripte mit den Skriptvorlagen erstellen. • **Online-Shellskripte**: Skripte, die gemäß der Uhr der Appliance zu geplanten Zeitpunkten

Option	Beschreibung
	ausgeführt werden, jedoch nur, wenn das Zielgerät mit der Appliance verbunden ist. Online-Shellskripts werden mithilfe einfacher textbasierter Skripte (Bash, Perl, Batch und andere) erstellt, die vom Betriebssystem des Zielgeräts unterstützt werden. Windows unterstützt Batchdateien und die verschiedenen vom jeweiligen Betriebssystem der Zielgeräte unterstützten Shellskript-Formate. PowerShell-Skripte werden auch auf Windows-basierten Zielgeräten unterstützt. **WICHTIG: Sie müssen sicherstellen, dass die richtige Dateierweiterung mit dem Skript verknüpft ist, damit es auf dem Ziel-Betriebssystem ausgeführt werden kann. Sie können beispielsweise `.sh`-Skripte auf Mac- und Linux-Geräten und `.ps1`-PowerShell-Skripte auf Windows-Geräten ausführen.**
Status	Geben Sie an, ob sich das Skript in der Entwicklung befindet (**Entwurf**) oder im Netzwerk bereitgestellt wurde (**Produktion**). Verwenden Sie den Status **Vorlage**, wenn Sie ein Skript erstellen, das als Grundlage für künftige Skripte dienen soll.
Beschreibung	(Optional) Eine kurze Beschreibung der Aktionen, die vom Skript ausgeführt werden. Dieses Feld hilft Ihnen dabei, ein Skript von den anderen auf der Liste *Skripte* aufgeführten Skripten zu unterscheiden.
Anmerkungen	Geben Sie nach Bedarf beliebige weitere Informationen ein.

3. Geben Sie im Abschnitt *Bereitstellung* die Bereitstellungsoptionen an:

Option	Beschreibung
Alle Geräte	Stellen Sie die Funktion auf allen Geräten bereit. Deaktivieren Sie das Kontrollkästchen, um die Bereitstellung auf bestimmte Labels oder Geräte zu beschränken.
Labels	Beschränken Sie die Bereitstellung auf Geräte, die zu angegebenen Labels gehören. Klicken Sie zum Auswählen von Labels auf **Bearbeiten**, ziehen Sie die Labels ins Fenster *Bereitstellung beschränken auf* und klicken Sie dann auf **Speichern**. Wenn Sie ein Label auswählen, das über eine Replikationsfreigabe oder eine alternative Download-Quelle verfügt, werden digitale Assets aus dieser Replikationsfreigabe oder aus dieser

Option	Beschreibung
	alternativen Download-Quelle kopiert und nicht direkt von der Appliance heruntergeladen. **HINWEIS:** Die Appliance nutzt eine Replikationsfreigabe, bevor sie den Alternativen KACE Speicherort verwendet.
Geräte	Mit dieser Option begrenzen Sie die Bereitstellung auf ein Gerät oder mehrere Geräte. Um nach Geräten zu suchen, beginnen Sie mit Ihrer Eingabe in das Feld.
Betriebssysteme	Das Betriebssystem, auf dem die Anwendung ausgeführt wird. Die Bereitstellung der Anwendungen erfolgt nur auf Geräten mit den ausgewählten Betriebssystemen. a. Klicken Sie auf **Betriebssysteme verwalten**. b. Wählen Sie im daraufhin angezeigten Dialogfeld **Betriebssysteme** die Betriebssystemversionen in der Navigationsstruktur aus. Sie haben die Möglichkeit, Betriebssystemversionen nach Familie, Produkt, Architektur, Versions-ID oder Build-Version auszuwählen. Je nach Bedarf können Sie eine bestimmte Build-Version oder einen übergeordneten Knoten auswählen. Wenn Sie einen übergeordneten Knoten im Baum auswählen, werden die zugehörigen untergeordneten Knoten automatisch mit ausgewählt. Aufgrund dieses Verhaltens können Sie beliebige zukünftige Betriebssystemversionen auswählen, da Geräte in Ihrer verwalteten Umgebung hinzugefügt oder aktualisiert werden. Wenn Sie beispielsweise alle aktuellen und zukünftigen Versionen auswählen möchten, die mit der Windows 10 x64-Architektur verbunden sind, wählen Sie unter **Alle** > **Windows** > **Windows 10** die Option **x64** aus.

4. Legen Sie Einstellungen für *Windows ausführen als* fest (nur für Online-Shellskripts und KScripts, die auf Windows-Geräten ausgeführt werden):

Option	Beschreibung
Lokales System	Sie führen das Skript mit Administratorrechten auf dem lokalen Gerät aus. Verwenden Sie diese Einstellung für alle Skripte, die mit einer Vorlage erstellt wurden.
Angemeldeter Benutzer	Sie führen das Skript als der Benutzer aus, der am lokalen Gerät angemeldet ist. Dies wirkt sich auf das Profil dieses Benutzers aus.

Option	Beschreibung
Alle angemeldeten Benutzer	Sie führen das Skript einmal für jeden Benutzer aus, der am lokalen Gerät angemeldet ist. Dies wirkt sich auf die Profile aller Benutzer aus.
Anmeldeinformationen	Das Online-Shellskript und KScripts werden im Kontext der hier angegebenen Anmeldeinformationen ausgeführt. Wählen Sie vorhandene Anmeldeinformationen in der Dropdown-Liste aus oder wählen Sie **Neue Anmeldeinformationen hinzufügen** aus, um nicht bereits aufgeführte Anmeldeinformationen hinzuzufügen. Siehe Hinzufügen und Bearbeiten von Benutzer-/Kennwort-Anmeldeinformationen. **HINWEIS:** Bei der Ausführung von Online-KScripts auf Windows-Geräten werden auf den Zielgeräten keine Benachrichtigungsfenster angezeigt, wenn Sie die Option zum Ausführen des Skripts als angegebener Benutzer mit Anmeldeinformationen auswählen. Führen Sie zum Anzeigen von Benachrichtigungsfenstern das Skript unter Verwendung von „Lokales System“, „Angemeldeter Benutzer“ oder „Alle angemeldeten Benutzer“ aus.

5. Legen Sie im Abschnitt *Benutzer benachrichtigen* die Warneinstellungen für den Benutzer fest. Warnungen stehen für Online-KScripts und Online-Shellskripte nur auf Windows und Mac Geräten zur Verfügung, die den KACE Agenten, Version 5.1 und höher, ausführen:

Option	Beschreibung
Benutzer vor der Ausführung benachrichtigen	Ermöglicht dem Benutzer, die Aktion auszuführen, abzubrechen oder zu verschieben. Diese Funktion ist besonders wichtig, wenn Neustarts erforderlich sind. Wenn kein Benutzer angemeldet ist, wird das Skript sofort ausgeführt.
Optionen	Dem Benutzer werden folgende Optionen im Warndialogfeld angezeigt (sofern Sie **Benutzer vor der Ausführung benachrichtigen** ausgewählt haben): • **OK**: Sofort ausführen. • **Abbrechen**: Abbrechen bis zur nächsten geplanten Ausführung. • **Snooze**: Der Benutzer erhält nach Ablauf der *Snooze-Dauer* erneut eine Eingabeaufforderung. Wenn der Benutzer bis zum Ablauf der unter *Timeout* festgelegten Zeit nicht reagiert hat, wird das Skript ausgeführt.

Option	Beschreibung
	Interaktion mit *Ausführen als*: • Nur der Konsolenbenutzer kann unabhängig von der Einstellung für *Ausführen als* das Warnungsdialogfeld sehen und somit entweder „Snooze“ oder „Abbrechen“ auswählen. • Durch Aktivieren einer Warnung erhält der Konsolenbenutzer auch dann eine Eingabeaufforderung, wenn für das Skript die Ausführung als alle Benutzer oder als ein anderer Benutzer eingestellt ist.
Timeout	Die Zeitspanne in Minuten, für die das Dialogfeld angezeigt werden soll, bevor eine Aktion ausgeführt wird. Wenn diese Zeitspanne verstreicht, ohne dass der Benutzer auf eine Schaltfläche klickt, führt die Appliance die in der Dropdown-Liste *Timeout* angegebene Aktion aus.
Timeout-Aktion	Die Aktion, die ausgeführt werden soll, wenn die Zeitspanne für den **Timeout** abgelaufen ist, ohne dass der Benutzer eine Option ausgewählt hat.
Snooze-Dauer	Die Wartezeit in Minuten, nachdem der Benutzer auf **Snooze** geklickt hat. Nach Ablauf dieser Zeit erscheint das Dialogfeld erneut.
Erste Meldung	Die Nachricht, die Benutzern vor dem Ausführen der Aktion angezeigt werden soll. Informationen zum Anpassen des im Dialogfeld angezeigten Logos finden Sie unter Allgemeine Appliance-Einstellungen ohne aktivierte Organisationskomponente konfigurieren.

6. Geben Sie im Abschnitt *Planen* die Ausführungsoptionen an:

Option	Beschreibung
Kein(e)	Die Ausführung erfolgt im Zusammenhang mit einem Ereignis anstatt zu einem bestimmten Datum oder zu einem bestimmten Zeitpunkt.
jede Stunde	Der Vorgang wird im angegebenen Intervall durchgeführt.
Täglich/an einem bestimmten Tag um HH:MM	Die Erfassung wird täglich zu einem bestimmten Zeitpunkt oder an einem bestimmten Wochentag um eine bestimmte Uhrzeit ausgeführt.
Ausführen am n-ten jedes Monats/eines bestimmten Monats um HH:MM	Die Erfassung wird jeden Monat oder in einem bestimmten Monat an einem festgelegten Datum zu einer festgelegten Uhrzeit ausgeführt.

Option	Beschreibung
Ausführen am n-ten Wochentag **jedes Monats/ eines bestimmten Monats um HH:MM**	Die Erfassung wird jeden Monat oder in einem bestimmten Monat an einem festgelegten Wochentag zu einer festgelegten Uhrzeit ausgeführt.

Benutzerdefiniert	Führen Sie die Erfassung nach einem benutzerdefinierten Zeitplan aus.
	Verwenden Sie das Standard-5-Feld-Cron-Format (das erweiterte Cron-Format wird nicht unterstützt):
	`* * * * *`
	`| | | | +————Wochentag (0-6) (Sonntag=0)`
	`| | | +————Monat (1-12)`
	`| | +————Monatstag (1-31)`
	`| +————Stunde (0-23)`
	`+————Minute (0-59)`
	Verwenden Sie bei der Angabe von Werten die folgenden Zeichen:
	• **Leerzeichen( )**: Die einzelnen Felder mit einem Leerzeichen trennen.
	• **Sternchen (*)**: Ein Sternchen repräsentiert den gesamten Wertebereich in einem Feld. Zum Beispiel repräsentiert ein Sternchen im Stundenfeld eine beliebige Stunde.
	• **Kommas (,)**: Mehrere Werte in einem Feld werden mit einem Komma getrennt. Zum Beispiel werden mit `0,6` im Feld „Wochentag“ Sonntag und Samstag angegeben.
	• **Bindestriche (-)**: Mit einem Bindestrich wird ein Wertebereich in einem Feld angegeben. Zum Beispiel entspricht `1-5` im Feld „Wochentag“ `1,2,3,4,5`, d. h. Montag bis Freitag.
	• **Schrägstriche (/)**: Die Angabe der Zeitabstände, mit denen eine Aktion wiederholt werden soll, erfolgt mit einem Schrägstrich. Zum Beispiel entspricht `*/3` im Feld Stunde `0,3,6,9,12,15,18,21`. Das Sternchen (`*`) gibt jede Stunde an, mit `/3` erfolgt aber eine Einschränkung auf durch drei teilbare Stunden.

Option	Beschreibung
	Beispiele: • `15 * * * * Jeden Tag 15 Minuten nach jeder vollen Stunde ausführen` • `0 22 * * * Jeden Tag um 22:00 Uhr ausführen` • `0 0 1 1,6 * Am 1. Januar und 1. Juni um 00:00 Uhr ausführen` • `30 8,12 * * 1-5 An Wochentagen um 08:30 Uhr und 12:30 Uhr ausführen` • `0 2 */2 * * Jeden zweiten Tag um 02:00 Uhr ausführen`
Aufgabenplan anzeigen	Klicken Sie, um den Aufgabenplan anzuzeigen. Im Dialogfeld *Aufgabenplan* wird eine Liste der geplanten Aufgaben angezeigt. Klicken Sie auf eine Aufgabe, um die Aufgabendetails anzuzeigen. Weitere Informationen hierzu finden Sie unter Aufgabenpläne anzeigen.

7. Wählen Sie im Abschnitt *Zeitplan-Optionen* die passenden Einstellungen aus.

Option	Beschreibung
Auch bei nächster Geräteanmeldung einmal ausführen (nur Offline-KScripts)	Führt das Offline-KScript einmal aus, wenn neue Skripte von der Appliance heruntergeladen werden.
Auch vor dem Anmelden ausführen (nur Offline-KScripts)	Führt das Offline-KScript beim Gerätestart aus. Hierdurch wird der Start der Geräte gegebenenfalls etwas verlangsamt. **HINWEIS:** Wenn auf einem Gerät eine Active Directory- oder Gruppenrichtlinienobjekt-Einstellung aktiv ist, mit der eine Meldung angezeigt wird, die der Benutzer vor dem Anmelden bestätigen muss, werden keine Skripte ausgeführt, bevor die Bestätigung erfolgt ist.
Auch nach dem Anmelden ausführen (bevor der Desktop lädt) (nur Offline-KScripts)	Führt das Offline-KScript aus, nachdem der Benutzer seine Windows Anmeldedaten eingegeben hat.
Ausführung bei getrennter Verbindung zulassen (nur Offline-KScripts)	Ermöglicht die Ausführung des Offline-KScripts, auch wenn das Zielgerät keine Verbindung zur Appliance herstellen kann, um die Ergebnisse zu übermitteln. In diesem Fall werden die Ergebnisse auf dem Gerät gespeichert und bei der nächsten Verbindungsherstellung in die Appliance geladen.
Ausführung ohne angemeldeten Benutzer zulassen	Ermöglicht die Ausführung des Skripts, auch wenn ein Benutzer nicht angemeldet ist. Deaktivieren Sie dieses Kontrollkästchen, um das Skript nur

Option	Beschreibung
	dann auszuführen, wenn der Benutzer am Gerät angemeldet ist.
Wenn offline, bei nächster Verbindung ausführen	Für Online-KScripts oder -Shellskripts aktiviert die Option das Skript für die Ausführung von Offline-Computern, wenn sie wieder online geschaltet werden. Wenn ein Skript ausgeführt wird, berechnet es die Anzahl der Computer, die es ausführen soll, basierend auf deren Labels oder deren Betriebssystemen, oder durch manuelle Identifikation ausgewählter Computer. Anhand des Computersatzes legt das Skript fest, welche dieser Computer online sind und richtet in der Warteschlange eine Aufgabe für die Online-Computer im Konductor ein. Wenn Sie diese Option auswählen, überspringt das Skript den Schritt, der Online-Computer identifiziert, und es wird auf den Online-Computern ausgeführt. Für die Offline-Computer wird die Aufgabe in der Warteschlange des Konductors hinzugefügt, und ausgeführt, wenn die Computer online geschaltet werden. Alle nachfolgenden Aufgaben für die Ausführung dieses Skripts (zum Beispiel für einen bereits in der Konductor-Warteschlange vorhandenen Offline-Computer) überschreibt die vorhandenen Aufgaben, so dass es nie mehr als eine Aufgabe in der Konductor-Warteschlange für den gleichen Computer gibt. Eine hohe Anzahl Aufgaben im Konductor können die Leistung des Geräts beeinflussen, so dass idealerweise Offline-Skripten für diese Computer verwendet werden, die typischerweise offline sind, und verwenden Sie diese Option nur mit Online-Skripten, wenn erwarten werden kann, dass die Zielmaschinen online sind, um die Überfüllung der Konductor-Warteschlange zu vermeiden. Standardmäßig ist diese Option deaktiviert.

8. So laden Sie vom Skript benötigte Dateien hoch:
   a. Klicken Sie im Abschnitt *Abhängigkeiten* auf **Neue Abhängigkeit hinzufügen**.
   b. Klicken Sie auf **Durchsuchen** oder **Datei auswählen**.
   c. Wählen Sie eine Datei und klicken Sie dann auf **Öffnen** oder **Auswählen**.

      Wenn eine Replikationsfreigabe angegeben und aktiviert ist, werden die Abhängigkeiten von der angegebenen Replikationsfreigabe heruntergeladen.

   HINWEIS: Wenn nicht auf die Replikationsfreigabe zugegriffen werden kann, werden die Abhängigkeiten von der Appliance heruntergeladen. Aktivieren Sie zum Aktivieren dieser Einstellung auf der *Detailseite für den Replikationszeitplan Failover zur Appliance*. Siehe Replikationsfreigaben erstellen.

   Wiederholen Sie bei Bedarf diesen Schritt, um weitere Abhängigkeiten hinzuzufügen.
9. **Nur Online- oder Offline-KScripts**. Klicken Sie im Abschnitt *Aufgaben* auf **Neue Aufgabe**.

Der Prozessablauf einer Aufgabe entspricht in etwa einem Skript wie dem folgenden:

```
IF Verify THEN
            Success
ELSE IF Remediation THEN
            Remediation Success
ELSE
            Remediation Failure
```

a. Legen Sie im Abschnitt *Richtlinie* oder *Job-Regeln* die folgenden Einstellungen für Aufgabe 1 fest:

Option	Beschreibung
Versuche	Geben Sie ein, wie oft die Appliance versuchen soll, das Skript auszuführen. Wenn die Skriptausführung fehlschlägt, die Wiederherstellung jedoch erfolgreich ist, sollten Sie unter Umständen die Aufgabe erneut ausführen, um den Wiederherstellungsschritt zu bestätigen. Legen Sie hierfür die Anzahl der Versuche auf zwei oder mehr fest. Wenn der Abschnitt *Bestätigung* fehlschlägt, erfolgt die Skriptausführung so oft, wie in diesem Feld angegeben.
Bei Fehler	• Wählen Sie **Abbrechen** aus, um die Ausführung bei einem Fehler anzuhalten. • Wählen Sie **Fortfahren** aus, um bei einem Fehler Wiederherstellungsschritte durchzuführen.

b. Klicken Sie im Abschnitt *Überprüfung* auf **Hinzufügen**, um einen Schritt hinzuzufügen. Wählen Sie dann mindestens einen Schritt aus, der ausgeführt werden soll.

Siehe Hinzufügen von Schritten zu Aufgabenbereichen von Skripten.

c. Wählen Sie in den Abschnitten *Erfolg* und *Wiederherstellung* mindestens einen Schritt aus, der ausgeführt werden soll.

Siehe Hinzufügen von Schritten zu Aufgabenbereichen von Skripten.

d. Wählen Sie in den Abschnitten *Wiederherstellungserfolg* und *Wiederherstellungsfehler* mindestens einen Schritt aus, der ausgeführt werden soll.

Siehe Hinzufügen von Schritten zu Aufgabenbereichen von Skripten.

TIPP: Wenn Sie eine Abhängigkeit entfernen möchten, klicken Sie neben dem Element auf die Schaltfläche **Löschen**: . Diese Schaltfläche wird angezeigt, wenn Sie mit dem Mauszeiger auf ein Element zeigen.

TIPP: Klicken Sie neben *Richtlinien- oder Job-Regeln* auf die Schaltfläche **Bearbeiten**, um die Token-Ersetzungsvariablen anzuzeigen, die an einer beliebigen Stelle im Skript verwendet werden können: . Die Variablen werden zur Laufzeit durch entsprechende Werte ersetzt.

TIPP: Siehe Token-Ersetzungsvariablen.

10. **Nur Online-Shellskripte**: Geben Sie im Abschnitt *Skript* folgende Einstellungen an:

Option	Beschreibung
Skripttext	Geben Sie den Skriptinhalt ein.

Option	Beschreibung
Name der Skriptdatei	Geben Sie den Namen und die Erweiterung der Datei ein, die das angegebene Skript enthalten soll. **WICHTIG: Sie müssen sicherstellen, dass die richtige Dateierweiterung mit dem Skript verknüpft ist, damit es auf dem Ziel-Betriebssystem ausgeführt werden kann. Sie können beispielsweise `.sh`-Skripte auf Mac- und Linux-Geräten und `.ps1`-PowerShell-Skripte auf Windows-Geräten ausführen.**
Timeout (Minuten)	Geben Sie die maximale Anzahl von Minuten an, die das Skript auf dem Zielgerät ausgeführt werden kann.
Datei hochladen	Wenn das Skript eine Datei generiert und Sie diese Datei auf die Appliance hochladen möchten, wählen Sie diese Option aus und geben Sie die folgenden Informationen an: • **Name der hochzuladenden Datei**: Geben Sie den Namen der Datei ein. • **Verzeichnispfad der hochzuladenden Datei**: Geben Sie das Verzeichnis an, in dem die Datei gespeichert werden soll. Wenn Sie das Standard-Skriptverzeichnis (`<appliance_installation_directory>/scripts`) verwenden möchten, lassen Sie dieses Feld leer.
Heruntergeladene Dateien löschen	Wenn für das Skript andere Dateien ausgeführt werden müssen, z. B. Installationsprogramme, und diese nach der Skriptausführung gelöscht werden sollen, wählen Sie diese Option aus.

11. Führen Sie einen der folgenden Schritte aus:
    - **Klicken Sie auf Jetzt ausführen, um das Skript sofort mittels Push an alle Geräte zu übertragen.**

      Verwenden Sie diese Option mit Vorsicht. Siehe Verwenden der Befehle "Ausführen" und "Jetzt ausführen".
    - **Klicken Sie auf Speichern.**

Skripte bearbeiten

Sie können die drei Arten von Skripten bearbeiten: Offline-KScripts, Online-KScripts und Online-Shellscripts. Sie können Offline-KScripts und Online-KScripts auch mit dem XML-Editor bearbeiten.

Benutzer mit eingeschränkten Zugriffsrechten können die Details aller Skripte anzeigen, aber nur Änderungen an denjenigen Skripten speichern, die Einfluss auf Geräte oder Labels haben, die mit dem für sie freigegebenen Bereich verknüpft sind. Weitere Informationen zu Benutzern mit eingeschränkten Zugriffsrechten finden Sie unter Benutzerrollen hinzufügen oder bearbeiten.

1. Rufen Sie die *Skriptdetailseite* auf:

a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.

b. Klicken Sie in der linken Navigationsleiste auf **Skripterstellung** und anschließend auf **Skripte**.

c. Führen Sie eine der folgenden Aktionen aus, um die *Skriptdetailseite* anzuzeigen:

- Klicken Sie auf den Namen eines Skripts.
- Wählen Sie **Aktion auswählen** > **Neu**.

2. Ändern Sie das Skript wie gewünscht.
3. Wählen Sie die Optionen für die Konfiguration, Bereitstellung und Zeitplanung. Siehe Offline-KScripts, Online-KScripts oder Online-Shellskripte hinzufügen.
4. Scrollen Sie zum Bearbeiten des unformatierten XML-Codes des Scripts zum Abschnitt *Planen* und klicken Sie auf **XML bearbeiten**.
5. Klicken Sie auf **Speichern**.

Skripte auf der Seite "Skripte" löschen

Sie können Skripte von der Seite Skripte löschen.

1. Rufen Sie die Liste *Skripte* auf:

   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.

   b. Klicken Sie in der linken Navigationsleiste auf **Skripterstellung** und anschließend auf **Skripte**.

2. Aktivieren Sie das Kontrollkästchen neben einem oder mehreren Skripten.
3. Wählen Sie **Aktion auswählen** > **Löschen** und klicken Sie dann zum Bestätigen auf **Ja**.

Skripte auf der Seite "Skriptdetail" löschen

Sie können Skripte von der Seite *Skriptdetail* löschen.

1. Rufen Sie die Seite *Skriptdetail* auf:

   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.

   b. Klicken Sie in der linken Navigationsleiste auf **Skripterstellung** und anschließend auf **Skripte**.

   c. Klicken Sie auf den Namen eines Skripts.

2. Klicken Sie auf **Löschen** und zur Bestätigung auf **Ja**.

Struktur für importierbare Skripte

Sie können ein Skript in einem externen XML-Editor erstellen und anschließend in die Appliance importieren.

Importierte Skripte müssen folgende Struktur aufweisen:

- Das Root-Element `<kbots></kbots>` enthält die URL der KACE DTD `"kbots xmlns="http://kace.com/Kbots.xsd">...<kbots>`.
- Mindestens ein `<kbot>`-Element.
- Genau ein `<config>`-Element in jedem `<kbot>`-Element.
- Genau ein `<execute>`-Element in jedem `<config>`-Element.
- Mindestens ein `<compliance>`-Element in jedem `<kbot>`-Element.

Im Folgenden finden Sie ein Beispiel für die XML-Struktur eines Appliance-Skripts:

```
<?xml version="1.0" encoding="utf-8" ?>
<kbots xmlns="http://kace.com/Kbots.xsd">
<kbot>
<config name="name="" type="policy" id="0" version="version="" description=
  "description="">
                        <execute disconnected="false" logged_off="false">
                        </execute>
</config>
<compliance>
</compliance>
</kbot>
</kbots>
```

Im vorangegangenen Beispiel entspricht das `</config>`-Element dem Abschnitt *Konfiguration* auf der Seite *Skriptdetail*. Hier legen Sie den Namen der Richtlinie oder des Jobs (optional) und den Skripttyp (Richtlinie oder Job) fest. In diesem Element können Sie auch angeben, ob das Skript ausgeführt werden kann, wenn das Zielgerät nicht mit der Appliance verbunden oder nicht bei ihr angemeldet ist.

Im **<compliance>**-Element können Sie den Aktivierungsstatus des Skripts festlegen und die spezifischen Aufgaben für das Skript beschreiben.

TIPP: Um ein Skript zu erstellen, das teilweise dieselben Aufgaben ausführt wie ein bereits vorhandenes Skript, duplizieren Sie das vorhandene Skript und öffnen es in einem XML-Editor. Das **<compliance>**-Element des Skripts gibt Ihnen eine Vorstellung von der Funktionsweise des Skripts und den Änderungsmöglichkeiten. Siehe Skripte duplizieren.

Skripte importieren

Sie können nach Bedarf Skripte in die Appliance importieren.

1. Rufen Sie die Liste *Skripte* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Skripterstellung** und anschließend auf **Skripte**.
2. Wählen Sie **Aktion auswählen > Importieren**.
3. Fügen Sie das vorhandene Skript in das entsprechende Feld ein und klicken Sie auf **Speichern**.

Skripte duplizieren

Wenn Sie ein Skript erstellen möchten, das einem bereits vorhandenen Skript ähnelt, können Sie das vorhandene Skript duplizieren und nach Bedarf bearbeiten. Dies geht möglicherweise schneller als das Erstellen eines völlig neuen Skripts.

1. Rufen Sie die Seite *Skriptdetail* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Skripterstellung** und anschließend auf **Skripte**.
   c. Klicken Sie auf den Namen eines Skripts.
2. Klicken Sie unten auf der Seite auf **Duplizieren**, um die Seite *Skripte* anzuzeigen.

   Das duplizierte Skript wird in der Liste angezeigt.
3. Klicken Sie auf den verknüpften Namen des duplizierten Skripts, um es zum Bearbeiten zu öffnen.

   Siehe Skripte bearbeiten.

Verwenden der Befehle "Ausführen" und "Jetzt ausführen"

Mithilfe der Befehle **Ausführen** und **Jetzt ausführen** können Sie Skripte sofort und ohne Zeitplan auf Zielgeräten ausführen.

Das Ausführung von Skripts ohne festgelegten Zeitplan ist in folgenden Fällen sinnvoll:

- Wenn Sie den Verdacht haben, dass Geräte in Ihrem Netzwerk mit einem Virus infiziert sind oder eine andere Sicherheitslücke aufweisen und das gesamte Netzwerk beeinträchtigen können, wenn das Problem nicht sofort behoben wird
- Wenn Sie Skripte während der Entwicklung auf einem bestimmten Gerät oder einer bestimmten Gruppe von Geräten testen und Fehler suchen und beheben möchten

Um Online-KScripts ausführen zu können, müssen die Zielgeräte über eine Agentenverbindung zur Appliance verfügen.

TIPP: Erstellen Sie ein Label, das die Geräte repräsentiert, auf denen der Befehl **Jetzt ausführen** ausgeführt werden soll, um die Gefahr einer Skriptbereitstellung auf nicht gewünschten Geräten zu minimieren.

Der Befehl **Jetzt ausführen** steht auf diesen Seiten der **Administratorkonsole** zur Verfügung:

- Seiten *Jetzt ausführen* und *Skriptdetails*: Über die Seite *Skripterstellung* > *Jetzt ausführen* können Sie das ausgewählte Skript auf den Zielgeräten ausführen.
- Seite *Skripte*: Wenn Sie Skripte auf der Seite *Skripte* mithilfe der Option **Jetzt ausführen** des Menüs *Aktion auswählen* ausführen, können Sie mehrere Skripte gleichzeitig laufen lassen.
- *Mac Profil-Detail*: Mit dem Befehl **Jetzt ausführen** auf der Seite *Mac Profil-Detail* wird ein Skript ausgeführt, das das ausgewählte Mac Profil auf Zielgeräten, die über eine Agentenverbindung zur Appliance verfügen, installiert oder entfernt.
- *Mac Profile*: Wählen Sie **Aktion auswählen > Ausführen** auf der Seite *Mac Profile* aus, um Skripte auszuführen, die gleichzeitig mehrere Mac Profile installieren oder entfernen, sofern die Zielgeräte über eine Agentenverbindung zur Appliance verfügen.

HINWEIS: Wenn bei der Ausführung eines Skripts ein Fehler auftritt, finden Sie unter Fehlercodes aufgrund von Patching und Skripterstellung eine Liste der Fehlercodes, die Ihnen bei der Diagnose des Problems helfen können.

Skripte über die Seite "Jetzt ausführen" ausführen

Sie können Skripte auf Zielgeräten über die Seite *Jetzt ausführen* ausführen.

VORSICHT: Skripte werden sofort bereitgestellt, wenn Sie auf Jetzt ausführen klicken.

- Verwenden Sie diese Funktion mit Vorsicht!
- Klicken Sie nur dann auf **Jetzt ausführen**, wenn Sie das Skript tatsächlich auf den Zielgeräten ausführen möchten.

1. Rufen Sie die Seite *Jetzt ausführen* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Skripterstellung** und anschließend auf **Jetzt ausführen**.
2. Wählen Sie aus der Dropdown-Liste *Skripte* ein Skript aus. Um nach einem Skript zu suchen, tippen Sie dessen Namen in die Liste.
3. Geben Sie im Abschnitt *Bereitstellung* die Bereitstellungsoptionen an:

Option	Optionen und Beschreibungen
Labels	Beschränken Sie die Bereitstellung auf Geräte, die zu angegebenen Labels gehören. Klicken Sie zum Auswählen von Labels auf **Bearbeiten**, ziehen Sie die Labels ins Fenster *Bereitstellung beschränken auf* und klicken Sie dann auf **Speichern**. Wenn Sie ein Label auswählen, das über eine Replikationsfreigabe oder eine alternative Download-Quelle verfügt, werden digitale Assets aus dieser Replikationsfreigabe oder aus dieser alternativen Download-Quelle kopiert und nicht direkt von der Appliance heruntergeladen. **HINWEIS:** Die Appliance nutzt eine Replikationsfreigabe, bevor sie den Alternativen KACE Speicherort verwendet.
Geräte	Mit dieser Option begrenzen Sie die Bereitstellung auf ein Gerät oder mehrere Geräte. Um nach Geräten zu suchen, beginnen Sie mit Ihrer Eingabe in das Feld. Benutzer mit eingeschränkten Zugriffsrechten sehen nur die Geräte, die mit ihrer Rolle verknüpft sind, wenn der Rolle ein Label zugewiesen ist. Weitere Informationen zur Zuordnung von Geräten zu Benutzerrollen finden Sie unter Benutzerrollen hinzufügen oder bearbeiten.

4. Klicken Sie auf **Jetzt ausführen**.

   Die Seite *Status von 'Jetzt ausführen'* wird angezeigt.

Skripte über die Skriptdetailseite ausführen

Sie können Skripte auf Zielgeräten über die *Skriptdetailseite* ausführen.

1. Rufen Sie die *Skriptdetailseite* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Skripterstellung** und anschließend auf **Skripte**.
   c. Klicken Sie auf den Namen eines Skripts.
2. Scrollen Sie an das Ende der Seite und klicken Sie auf **Jetzt ausführen**.

   Die Seite *Status von 'Jetzt ausführen'* wird angezeigt.

Skripte über die Seite Skripte ausführen

Sie können Skripte über die Seite *Skripte* ausführen.

1. Rufen Sie die Liste *Skripte* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Skripterstellung** und anschließend auf **Skripte**.
2. Aktivieren Sie das Kontrollkästchen neben einem oder mehreren Skripten.
3. Wählen Sie **Aktion auswählen** > **Jetzt ausführen**.

   Die Seite *Status von 'Jetzt ausführen'* wird angezeigt.

Den Status von "Jetzt ausführen" überwachen und Skriptdetails anzeigen

Sie können den Status von Skripten, die mithilfe des Befehls **Jetzt ausführen** gestartet wurden, anzeigen und die Skriptdetails aufrufen.

Stellen Sie sicher, dass keine Firewall-Einstellungen festgelegt sind, die die Überwachung von Port 443 durch den KACE Agent verhindern.

Der Befehl **Jetzt ausführen** verwendet Port 443 zur Datenübertragung. Die Bereitstellung eines Skripts kann fehlschlagen, wenn der KACE Agent durch die Firewall-Einstellung daran gehindert wird, diesen Port zu überwachen. Weitere Informationen zu den Port-Anforderungen finden Sie unter Überprüfen von Port-Einstellungen, NTP-Dienst und Website-Zugriff.

1. Rufen Sie die Liste *'Jetzt ausführen'-Status* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Skripterstellung** und anschließend auf **'Jetzt ausführen'-Status**.
2. Sehen Sie sich die Informationen in der Liste *'Jetzt ausführen'-Status* an.

Auf dieser Seite werden folgende Informationen angegeben:

- **Begonnen**: Der Zeitpunkt, zu dem der Befehl **Jetzt ausführen** gegeben wurde.
- **Name**: Name des Skripts. Klicken Sie auf diesen Skriptnamen, um die Detailseite zu *Jetzt ausführen* anzuzeigen.
- **Ziel**: Die Anzahl der Geräte, auf denen das Skript nach Zeitplan ausgeführt werden soll.
- **Mittels Push übertragen, Wird ausgeführt, Ausstehend**: Die Anzahl der Geräte, auf denen versucht wird, das Skript auszuführen
- **Erfolgreich, Fehler, Abgeschlossen**: Die Anzahl der Geräte, auf denen das Skript ausgeführt wurde
- **Erfolgsrate**: Der Prozentsatz der Skripte, die erfolgreich auf den Zielgeräten ausgeführt wurden.

Die Zahlen in den Spalten *Mittels Push übertragen*, *Wird ausgeführt*, *Ausstehend*, *Erfolgreich*, *Fehler* und *Abgeschlossen* werden schrittweise erhöht, während das Skript auf den Zielgeräten bereitgestellt wird. Falls bei der Übertragung der Skripte mittels Push auf die ausgewählten Geräte Fehler aufgetreten sind, können Sie die Skriptprotokolle durchsuchen, um die Ursache zu ermitteln. Siehe Die Skriptprotokolle durchsuchen.

3. Klicken Sie in der Spalte *Gestartet* eines Skripts auf den Link, um die Detailseite zum *"Jetzt ausführen"-Status* anzuzeigen.

   Auf dieser Seite werden folgende Informationen angegeben:

   - **Statistik zu 'Jetzt ausführen'**: Die Ergebnisse eines mittels Push übertragenen Skripts, die Push-Fehler, die Push-Erfolge, die abgeschlossenen Geräte, die ausgeführten Geräte sowie die Erfolge und Fehler in Zahlen und Prozentsätzen.
   - **Fehler bei Bereitstellung**: Die Geräte, die die Appliance nicht kontaktieren konnte und die daher die Richtlinie nicht erhalten haben. Nach der Übertragung des Skripts kann es einige Zeit dauern, bis das Gerät die Richtlinie vollständig umgesetzt hat.
   - **In Bearbeitung**: Die Geräte, die die Richtlinie empfangen, ihre Ergebnisse jedoch noch nicht gemeldet haben. Nachdem die Richtlinie ausgeführt wurde, wird über den Erfolg oder das Fehlschlagen berichtet. Die Ergebnisse werden unter dem entsprechenden Abschnitt dargestellt. Auf den einzelnen Geräteseiten werden auch die Ergebnisse der "Jetzt ausführen"-Ereignisse angezeigt, die auf diesem Gerät ausgeführt wurden.
   - **Fehlgeschlagene Ausführung**: Die Geräte, auf denen das Skript nicht erfolgreich ausgeführt wurde
   - **Erfolgreiche Ausführung**: Die Geräte, auf denen das Skript erfolgreich ausgeführt wurde

Informationen zu den Konfigurationsrichtlinienvorlagen

Mit Konfigurationsrichtlinienvorlagen können Sie richtlinienbezogene Skripte erstellen. Diese Skripte können bereitgestellt werden, um Richtlinien auf verwalteten Geräten zu konfigurieren.

Dieser Abschnitt enthält Beschreibungen der Einstellungen für die einzelnen Skripte, die Sie erstellen können.

Für Windows sind u.a. folgende Vorlagen verfügbar:

- Skripte für automatische Updates hinzufügen
- Dell Command | Monitor-Skripte hinzufügen
- Skripte für Desktop-Hintergrundbild hinzufügen
- Skripte für Desktop-Verknüpfungen hinzufügen
- Ereignisprotokoll-Reporter-Skripte hinzufügen
- MSI-Installationsskripte hinzufügen
- Energieverwaltungsskripte hinzufügen
- Registrierungsskripte hinzufügenRegistrierungsskripte hinzufügen
- Skripte für die Fehlerbehebung per Remote-Desktop-Steuerung hinzufügen
- UltraVNC-Skripte hinzufügen
- Deinstallationsskripte hinzufügen

Für Mac OS X sind u.a. folgende Vorlagen verfügbar:

- Skripte für Active Directory hinzufügen
- Energieverwaltungsskripte hinzufügen
- VNC-Skripte hinzufügen

Verwenden der Windows Konfigurationsrichtlinien

Sie können Konfigurationsrichtlinien oder Skripte für die Ausführung auf Windows-Geräten mithilfe von Konfigurationsrichtlinienvorlagen erstellen.

HINWEIS: Wenn Sie eine auf einer Vorlage basierende Richtlinie bearbeiten, sollte die Option *Ausführen als* auf das lokale System eingestellt bleiben.

Informationen zum Starten von automatischen Windows Updates auf Windows-Geräten

Automatische Windows Updates können auf verwalteten Windows-Geräten auf unterschiedliche Weise gestartet werden.

Führen Sie zum Starten von automatischen Windows Updates eine der folgenden Aktionen aus:

- Aktivieren Sie die Richtlinie Einstellungen für automatische Windows Updates der Appliance. Siehe Skripte für automatische Updates hinzufügen.
- Aktivieren Sie die lokale Richtlinie für automatische Windows Updates auf dem Gerät.
- Ändern Sie den Registrierungsschlüssel für automatische Windows Updates auf dem Gerät.
- Richten Sie die Gruppenrichtlinie in der Domäne für automatische Windows Updates auf dem Gerät ein.

Wenn Sie die Appliance-Patch-Funktion für die automatische Bereitstellung von Windows Updates auf dem Gerät verwenden, müssen Sie automatische Windows Updates auf dem Gerät durch alle anderen Prozesse deaktivieren, um Konflikte zwischen den verschiedenen Bereitstellungsprozessen zu vermeiden.

Skripte für automatische Updates hinzufügen

Mit der Vorlage "Automatische Aktualisierung" können Sie Skripte zum Steuern der Verwendung des Windows Update-Prozesses auf verwalteten Geräten erstellen.

Windows Update ist eine Funktion von Microsoft, die Windows Geräte automatisch mit Sicherheits- und anderen wichtigen Patches von Microsoft aktualisiert. Mithilfe der Richtlinie für automatische Windows Updates können Sie festlegen, wie und wann Windows Updates auf verwaltete Geräte heruntergeladen werden, sodass Sie den Aktualisierungsvorgang steuern können.

Weitere Informationen zu Windows Update finden Sie unter: http://support.microsoft.com/kb/328010.

1. Rufen Sie die Seite *Automatische Aktualisierungen für Windows* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Skripterstellung** und anschließend auf **Konfigurationsrichtlinien**.
   c. Klicken Sie im Fensterbereich *Konfigurationsrichtlinien* im Abschnitt *Windows* auf **Automatische Aktualisierungen**.
2. Geben Sie die folgenden Informationen an:

Option	Beschreibung
Name	Ein Name, der das Skript identifiziert. Dieser Name wird auf der Seite *Skripte* angezeigt.
(Empfohlen) Automatisch herunterladen ...	Aktiviert das automatische Herunterladen von Windows Updates
Aktualisierungen herunterladen, den Benutzer jedoch den Zeitpunkt der Patch-Installation wählen lassen	Lädt Updates herunter und stellt Installationsoptionen zur Auswahl, anstatt die Installation automatisch durchzuführen
Benutzer benachrichtigen, doch Patches nicht automatisch herunterladen und installieren	Sie erhalten Benachrichtigungen, wenn Updates zur Verfügung stehen, verhindern jedoch, dass die Appliance Updates herunterlädt oder installiert. **WICHTIG: Die Updates müssen regelmäßig abgerufen und installiert werden, da Ihr Netzwerk anderenfalls verstärkt der Gefahr von Angriffen ausgesetzt ist.**
Automatische Updates deaktivieren	Deaktiviert die automatischen Windows Updates auf dem Gerät. Diese Einstellung wird empfohlen, falls Sie die Patch-Funktion der Appliance verwenden möchten, um Windows Patch-Aktualisierungen zu verwalten.
Administrationsrichtlinie entfernen und Konfiguration vom Benutzer durchführen lassen	Benutzer können die heruntergeladenen Updates steuern.

Option	Beschreibung
	WICHTIG: Wenn Sie diese Option wählen, ist Ihr Netzwerk ggf. der Gefahr von Angriffen ausgesetzt.
Wartezeit neu planen	Das Intervall in Minuten, das gewartet werden soll, bevor ein Update im Fall einer fehlgeschlagenen Installation neu geplant wird.
Gerät nicht neu starten, solange ein Benutzer angemeldet ist	Verhindert den automatischen Neustart, solange Benutzer angemeldet sind
SUS-Server	Der Name des Servers für Windows Server® Update Services.
SUS-Statistik-Server	Der Name des Statistikservers, der für Windows Server Update Services verwendet wird.

3. Klicken Sie auf **Speichern**, um die Seite *Skriptdetail* anzuzeigen.
4. Wählen Sie die Optionen für die Konfiguration, Bereitstellung und Zeitplanung. Siehe Offline-KScripts, Online-KScripts oder Online-Shellskripte hinzufügen.
5. Klicken Sie zum Bearbeiten des unformatierten XML-Codes im Skript unter dem Abschnitt *Planen* auf **XML bearbeiten**.
6. Klicken Sie auf **Speichern**.

Informationen zu Dell Command | Monitor

Dell Command | Monitor ist das Überwachungstool der Dell Command Suite. Damit können Remote-Managementanwendungen wie die Appliance Verwaltungs- und Überwachungsaktivitäten ausführen.

Die Verwendung von Dell Command | Monitor bietet der Appliance die folgenden Funktionen für bestimmte Dell Geräte:

- Zugriff auf Verwaltungsinformationen
- Überwachen des Gerätestatus
- Ändern des Status von Unternehmens-Clientsystemen

Frühere Versionen von Dell Command | Monitor trugen den Namen Dell OpenManage™ Client Instrumentation (OMCI). Die Appliance unterstützt nur Dell Command | Monitor 9.0 oder höher.

Unterstützte physische Hardware

Dell Command | Monitor ist für folgende Dell Hardware verfügbar.

- Dell Venue 11 Pro
- Dell OptiPlex™
- Dell Precision Workstation™
- Dell Latitude™

Unterstützte Microsoft Betriebssysteme

Die folgenden Betriebssysteme werden für Dell Command | Monitor unterstützt.

- Microsoft Windows 8.1 (32 und 64 Bit), Microsoft Windows 8.1 Professional (32 und 64 Bit) und Enterprise (32 und 64 Bit)
- Microsoft Windows 8 (32 und 64 Bit), Microsoft Windows 8 Professional (32 und 64 Bit) und Enterprise (32 und 64 Bit)
- Microsoft Windows 7, Windows 7 (SP1), Professional, Enterprise sowie Ultimate x86 (32 Bit) und x64 (64 Bit)
- Microsoft Windows Vista Business (SP1) x86 (32 Bit) und x64 (64 Bit)
- Microsoft Windows Vista Ultimate (SP1 und SP2) x86 (32 Bit) und x64 (64 Bit)
- Microsoft Windows Vista Enterprise (SP1 und SP2) x86 (32 Bit) und x64 (64 Bit)

Für Informationen abgefragte Klassen und Eigenschaften

Die Appliance fragt unter Verwendung von Dell Command | Monitor folgende DCIM-Klassen und -Eigenschaften der Windows Verwaltungsinstrumentation ab.

Die von den Abfragen zurückgegebenen Informationen werden in der Gruppe *Dell Command | Monitor* auf der Seite *Gerätedetail* für das entsprechende Dell Hardwaregerät im Inventar angezeigt.

Sie können mithilfe des Berichtsassistenten benutzerdefinierte Berichte erstellen, die jegliche Kombination von Eigenschaften erfassen. Siehe Berichte mit dem Berichts-Assistenten erstellen.

Klasse	**Eigenschaften**	**Berichtsassistent** *Anzuzeigende Felder* **– Gruppe**	**Berichtsassistent** *Anzuzeigende Felder* **Elementname**
DCIM_FlatPanel	keine Angabe	Dell Command | Monitor – Flachbildschirm	Seitenverhältnis
	DisplayType		Displaytyp
	HorizontalResolution		Horizontale Auflösung
	PrimaryStatus		Status primärer Host
	VerticalResolution		Vertikale Auflösung
DCIM_DesktopMonitor	keine Angabe	Dell Command | Monitor – Monitor	Seitenverhältnis
	CurrentResolutionH		Aktuelle horizontale Auflösung
	CurrentResolutionV		Aktuelle vertikale Auflösung
	Beschreibung		Beschreibung
	InputDisplayPort		Unterstützt DisplayPort
	InputDVI		Unterstützt DVI
	InputHDMI		Unterstützt HDMI

Klasse	Eigenschaften	Berichtsassistent *Anzuzeigende Felder* – **Gruppe**	Berichtsassistent *Anzuzeigende Felder* **Elementname**
	ManufactureDate		Herstellungsdatum
	keine Angabe		Diagonale Abmessungen (cm)
	keine Angabe		Diagonale Abmessungen (Zoll)
	PhysicalSizeH		Horizontale Abmessungen (cm)
	PhysicalSizeV		Vertikale Abmessungen (cm)
	PrimaryStatus		PrimaryStatus
	SerialNumber		Seriennummer
	StandbyModeSupported		Unterstützt Standby-Modus
	SuspendModeSupported		Unterstützt Ruhezustandsmodus
	VeryLowPowerSupported		Unterstützt Extremniedrigstrom-Modus
DCIM_VProSettings	VProCharacteristics	Dell Command | Monitor – vPro Einstellungen	VPro Eigenschaften
DCIM_AMTSettings	AMTSupported	Dell Command | Monitor – AMT Einstellungen	AMT unterstützt
	IDEREnabled		IDE-R aktiviert
	SOLEnabled		SOL aktiviert
DCIM_PhysicalMemory	BankLabel	Dell Command | Monitor – Physischer Speicher	Bank-Label
	Kapazität		Kapazität (Byte)
	ElementName		Name
	ManufactureDate		Herstellungsdatum
	Hersteller		Hersteller

Klasse	Eigenschaften	Berichtsassistent *Anzuzeigende Felder* – **Gruppe**	Berichtsassistent *Anzuzeigende Felder* **Elementname**
	MemoryType		Speichertyp
	Modell		Modell
	PartNumber		Teilenummer
	PrimaryStatus		Status primärer Host
	SerialNumber		Seriennummer
	Geschwindigkeit		Geschwindigkeit (MHz)
DCIM_Processor	Titel	Dell Command | Monitor – Prozessor	Titel
	CurrentClockSpeed		Aktuelle Taktfrequenz (MHz)
	ElementName		Name
	MaxClockSpeed		Maximale Taktfrequenz (MHz)
	NumberOfEnabledCores		Anzahl der aktivierten Kerne
	PrimaryStatus		Status primärer Host
	Version		Version
DCIM_ProcessorCapabilities	NumberOfHardwareThreads		Hardware-Threads
	NumberOfProcessorCores		Anzahl der Kerne
DCIM_Battery	keine Angabe	Dell Command | Monitor – Akku	Ladezustand (%)
	Chemie		Chemie
	DesignCapacity		Vorgesehene Kapazität (mWh)
	DesignVoltage		Vorgesehene Spannung (mV)
	ExpectedLife		Erwartete Lebensdauer (Minuten)
	FullChargeCapacity		Vollständige Ladekapazität (mWh)

Klasse	Eigenschaften	Berichtsassistent *Anzuzeigende Felder* – **Gruppe**	Berichtsassistent *Anzuzeigende Felder* **Elementname**
	HealthState		Integritätsstatus
	Name		Name
	PrimaryStatus		Status primärer Host
	RechargeCount		Anzahl der Aufladungen
DCIM_LogEntry	CreationTimeStamp	keine Angabe	keine Angabe
	RecordData		
	RecordFormat		

In Berichten von Dell Command | Monitor verfügbare Hardwarewarnungen

Die folgenden Einstellungen bestimmen, wie viele Warnungsinformationen in einem über den Berichtsassistenten erstellten Bericht enthalten sind.

Berichtsassistent *Anzuzeigende Felder* – **Gruppe**	Berichtsassistent *Anzuzeigende Felder* – **Elementname**
Dell Command | Monitor – Hardwarewarnungen	Kategorie
	Beschreibung
	Schweregrad
	Zeitstempel

Dell Command | Monitor-Skripte hinzufügen

Dell Command | Monitor ist das Überwachungstool der Dell Command Suite. Damit können Remote-Managementanwendungen wie die Appliance Verwaltungs- und Überwachungsaktivitäten ausführen. Auf der Seite *Dell Command | Monitor* können Sie eine verwaltete Installation für die Bereitstellung von Dell Command | Monitor für mit der Appliance verwaltete Geräte, die das Tool unterstützen, bzw. für dessen Entfernung von diesen Geräten benennen und speichern.

Sie verfügen über Geräte mit unterstützter Dell Hardware und Betriebssystemen von Microsoft. Siehe Informationen zu Dell Command | Monitor.

Sie haben Dell Command | Monitor vom Dell TechCenter unter http://en.community.dell.com/techcenter/enterprise-client/w/wiki/7531.dell-command-monitor heruntergeladen.

HINWEIS: Obwohl sich dieses Thema auf die Installation bezieht, können Sie die Seite *Dell Command | Monitor* auch für die Entfernung von Dell Command | Monitor von einem Gerät verwenden.

1. Rufen Sie die Seite *Windows Dell Command | Monitor* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen*

aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.

b. Klicken Sie in der linken Navigationsleiste auf **Skripterstellung** und anschließend auf **Konfigurationsrichtlinien**.

c. Klicken Sie im Fensterbereich *Konfigurationsrichtlinien* im Abschnitt *Windows* auf **Dell Command | Monitor**.

2. **Optional**: Ändern Sie den Namen, wenn ein genauerer Name als die Standardeinstellung erforderlich ist.
3. Legen Sie die *Aktion* fest. Behalten Sie entweder die Standardeinstellung **Installation** bei oder ändern Sie sie auf **Deinstallation**.
4. Klicken Sie auf **Speichern**, um die Seite *Detail zu verwalteter Installation* anzuzeigen. Die Konfigurationsinformationen für die von Ihnen gewählte Aktion werden automatisch eingetragen.

   Die Appliance trägt automatisch in den Feldern *Name*, *Software*, *Verknüpfte Software* und *Vollständige Befehlszeile* entsprechende Werte ein.

Vervollständigen Sie die erforderlichen Informationen auf der Seite *Detail zu verwalteter Installation*. Siehe Verwaltete Installationen für Windows Geräte erstellen.

Skripte für Desktop-Hintergrundbild hinzufügen

Mit dieser Vorlage können Sie Skripte zum Steuern der Desktop-Hintergrundbildeinstellungen von Windows-Geräten erstellen.

Für Hintergrundbilddateien wird das Bitmap-Format (*.BMP) empfohlen. Die angegebene Datei mit dem Hintergrundbild wird an Geräte verteilt, auf denen das Skript ausgeführt wird.

1. Rufen Sie die Seite *Desktop-Hintergrundbild* auf:

   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.

   b. Klicken Sie in der linken Navigationsleiste auf **Skripterstellung** und anschließend auf **Konfigurationsrichtlinien**.

   c. Klicken Sie im Fensterbereich *Konfigurationsrichtlinien* im Abschnitt *Windows* auf **Desktop-Hintergrundbild**.

2. Geben Sie die folgenden Informationen an:

Option	Beschreibung
Name	Ein Name, der das Skript identifiziert. Dieser Name wird auf der Seite *Skripte* angezeigt.
Hintergrundbild verwenden	Die Hintergrundbilddatei auf dem Desktop der Zielgeräte anzeigen
Hintergrundbild-Bitmap-Datei	Klicken Sie auf **Durchsuchen** oder **Datei auswählen**, um die Datei auszuwählen und hochzuladen, die für das Hintergrundbild verwendet werden soll. Die Datei muss im BMP- oder JPG-Format vorliegen.

Option	Beschreibung
Position	Wählen Sie in der Dropdown-Liste *Position* eine Option aus. • **Gestreckt**: Strecken Sie das Bild so, dass es den gesamten Bildschirm füllt. • **Zentriert**: Zeigen Sie das Bild in der Bildschirmmitte an. • **Nebeneinander**: Wiederholen Sie das Bild über den gesamten Bildschirm.

3. Klicken Sie auf **Speichern**, um die Seite *Skriptdetail* anzuzeigen.
4. Wählen Sie die Optionen für die Konfiguration, Bereitstellung und Zeitplanung. Siehe Offline-KScripts, Online-KScripts oder Online-Shellskripte hinzufügen.
5. Klicken Sie zum Bearbeiten des unformatierten XML-Codes im Skript unter dem Abschnitt *Planen* auf **XML bearbeiten**.
6. Klicken Sie auf **Speichern**.

Skripte für Desktop-Verknüpfungen hinzufügen

Mit dieser Vorlage können Sie Skripte erstellen, die Internetverknüpfungen auf dem Desktop oder im *Startmenü* von Windows-Geräten hinzufügen.

Mit diesem Skript können Sie beispielsweise eine Verknüpfung mit einer Unternehmenswebsite oder einer anderen URL hinzufügen.

1. Rufen Sie die Seite *Windows Desktop-Verknüpfungen* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Skripterstellung** und anschließend auf **Konfigurationsrichtlinien**.
   c. Klicken Sie im Fensterbereich *Konfigurationsrichtlinien* im Abschnitt *Windows* auf **Desktop-Verknüpfungen**.
2. Geben Sie die folgenden Informationen an:

Option	Beschreibung
Name	Ein Name, der das Skript identifiziert. Dieser Name wird auf der Seite *Skripte* angezeigt.

3. Klicken Sie auf **Verknüpfung hinzufügen**.
4. Legen Sie die Verknüpfungseinstellungen fest:

Option	Beschreibung
Name	Die Beschriftung wird unter oder neben der Verknüpfung angezeigt.
Ziel	Der vollständige Pfad zur Anwendung, Datei oder URL, die bei Auswahl der Verknüpfung gestartet werden soll. Beispiel:

Option	Beschreibung

	Verwenden Sie folgendes Format, um eine Verknüpfung für explorer.exe zu erstellen: `C:\WINDOWS\explorer.exe`
	Verwenden Sie folgendes Format, um eine Verknüpfung von der UNC-Freigabe für explorer.exe zu erstellen:
	`\\192.168.1.1\WINDOWS\explorer.exe`
	oder
	`\\HostName\WINDOWS\explorer.exe`

Parameter	Die für die Verknüpfung erforderlichen Befehlszeilenparameter Beispiel: `/S /IP=123.4`
Arbeitsverzeichnis	Die Änderungen am aktuellen Arbeitsverzeichnis ein Beispiel: `C:\Windows\Temp`
Standort	Der Ort, an dem die Verknüpfung angezeigt werden soll Zur Auswahl stehen folgende Optionen: **Desktop** und **Startmenü**.

5. Klicken Sie auf **Änderungen speichern**, um die Verknüpfung zu speichern.
6. Klicken Sie auf **Verknüpfung hinzufügen**, um weitere Verknüpfungen hinzuzufügen. Wenn Sie eine Verknüpfung bearbeiten oder löschen möchten, zeigen Sie mit dem Mauszeiger auf sie und klicken auf die Schaltfläche **Bearbeiten** oder **Löschen**: .
7. Klicken Sie auf **Speichern**, um die Seite *Skriptdetail* anzuzeigen.
8. Wählen Sie die Optionen für die Konfiguration, Bereitstellung und Zeitplanung. Siehe Offline-KScripts, Online-KScripts oder Online-Shellskripte hinzufügen.
9. Klicken Sie zum Bearbeiten des unformatierten XML-Codes im Skript unter dem Abschnitt *Planen* auf **XML bearbeiten**.
10. Klicken Sie auf **Speichern**.

Ereignisprotokoll-Reporter-Skripte hinzufügen

Mit dieser Vorlage können Sie Skripte erstellen, die das Windows Ereignisprotokoll abfragen und die Ergebnisse an die Appliance hochladen.

1. Rufen Sie die Seite *Ereignisprotokoll-Reporter von Windows* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Skripterstellung** und anschließend auf **Konfigurationsrichtlinien**.
   c. Klicken Sie im Fensterbereich *Konfigurationsrichtlinien* im Abschnitt *Windows* auf **Ereignisprotokoll-Reporter**.
2. Geben Sie die folgenden Informationen an:

Option	Beschreibung
Name	Ein Name, der das Skript identifiziert. Dieser Name wird auf der Seite *Skripte* angezeigt.
Name der Ausgabedatei	Der Name der Protokolldatei, die von dem Skript erstellt wird
Protokolldatei	Die Art des Protokolls, das abgefragt werden soll: Software, System oder Sicherheit
Ereignistyp	Die Art des Ereignisses, das abgefragt werden soll: Information, Warnung oder Fehler.
Quellenname	(Optional) Die Namen der Quellen, auf die die Abfrage beschränkt ist

3. Klicken Sie auf **Speichern**, um die Seite *Skriptdetail* anzuzeigen.
4. Wählen Sie die Optionen für die Konfiguration, Bereitstellung und Zeitplanung. Siehe Offline-KScripts, Online-KScripts oder Online-Shellskripte hinzufügen.
5. Klicken Sie zum Bearbeiten des unformatierten XML-Codes im Skript unter dem Abschnitt *Planen* auf **XML bearbeiten**.
6. Klicken Sie auf **Speichern**.
7. Um das Ereignisprotokoll eines Geräts anzuzeigen, klicken Sie auf **Inventar** und anschließend auf einen Gerätenamen.
8. Klicken Sie im Bereich *Skriptprotokolle* unter *Derzeit bereitgestellte Jobs & Richtlinien* auf die Verknüpfung **Protokolle anzeigen** neben *Ereignisprotokoll*.

MSI-Installationsskripte hinzufügen

Mit dieser Vorlage können Sie Skripte erstellen, die die grundlegenden Befehlszeilenargumente für die Ausführung MSI-basierter Installationsprogramme auf Windows-Geräten festlegen.

Informationen zu Befehlszeilenoptionen finden Sie in der Dokumentation zur Microsoft MSI-Befehlszeile: http://msdn.microsoft.com/en-us/library/windows/desktop/aa367988%28v=vs.85%29.aspx.

1. Rufen Sie die Seite *Windows MSI-Installationsprogramm* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Skripterstellung** und anschließend auf **Konfigurationsrichtlinien**.
   c. Klicken Sie im Fensterbereich *Konfigurationsrichtlinien* im Abschnitt *Windows* auf **MSI-Installationsprogramm**.
2. Geben Sie die folgenden Informationen an:

Option	Beschreibung
Name	Ein Name, der das Skript identifiziert. Dieser Name wird auf der Seite *Skripte* angezeigt.

Option	Beschreibung
Aktion	Die auszuführende Aufgabe. Mögliche Aufgaben sind **Installieren**, **Deinstallieren**, **Fehlende Dateien reparieren** und **Alle Dateien erneut installieren**.
Software	Die Anwendung für das Skript. Um nach einer Anwendung zu suchen, beginnen Sie mit Ihrer Eingabe in das Feld.
MSI-Dateiname	Der MSI-Dateiname (erforderlich, wenn es sich bei der Datei um ein ZIP-Archiv handelt).
Benutzerinteraktion	Wie die Installation Benutzern angezeigt wird. Zur Auswahl stehen folgende Optionen: **Standard**, **Im Hintergrund**, **Minimale Benutzeroberfläche**, **Reduzierte Benutzeroberfläche** und **Vollständige Benutzeroberfläche**.
Installationsverzeichnis	Das Verzeichnis auf dem Zielgerät, in dem die Anwendung installiert werden soll.
Zusätzliche Optionen	Zusätzliche Installationsoptionen. Es werden zusätzliche Optionen zwischen den Argumenten `msiexe.exe` und `/i foo.msi` eingefügt.
Zusätzliche Eigenschaften	Alle zusätzlichen Eigenschaften. Diese Eigenschaften werden am Ende der Befehlszeile eingefügt. Beispiel: `msiexec.exe /s1 /switch2 /i patch123.msi TARGETDIR=C:\patcher PROP=A PROP2=B`
Funktionsliste	Die zu installierenden Funktionen. Trennen Sie Funktionen durch Kommas.
Konfiguration pro Gerät speichern	Angabe darüber, ob die Konfigurationsinformationen für einzelne Geräte gespeichert werden sollen
Nach der Installation	Die nach der Installation auszuführende Aktion.
Neustart-Optionen	Die nach dem Systemneustart auszuführende Aktion
Protokollierung	Die im Installationsprotokoll aufzuzeichnenden Informationen. Um mehrere Elemente auszuwählen, klicken Sie mit gedrückt gehaltener **STRG-Taste** oder **Befehlstaste**.

Option	Beschreibung
Name der Protokolldatei	Der Name der Protokolldatei

3. Klicken Sie auf **Speichern**, um die Seite *Skriptdetail* anzuzeigen.
4. Wählen Sie die Optionen für die Konfiguration, Bereitstellung und Zeitplanung. Siehe Offline-KScripts, Online-KScripts oder Online-Shellskripte hinzufügen.
5. Klicken Sie zum Bearbeiten des unformatierten XML-Codes im Skript unter dem Abschnitt *Planen* auf **XML bearbeiten**.
6. Klicken Sie auf **Speichern**.

Informationen zur Energieverwaltung und zum Stromverbrauch

Sie können Energieverwaltungsberichte für einen bestimmten Zeitraum (beispielsweise für einen Monat) ausführen, um sich einen Überblick über den Stromverbrauch der Geräte zu verschaffen.

Weitere Informationen zur Berichtkategorie *Energieverwaltung* finden Sie unter Erstellen von Berichten.

Sie können auch konfigurieren, wie lange Informationen zur Betriebszeit von Geräten gespeichert werden. Siehe Allgemeine Appliance-Einstellungen bei aktivierter Organisationskomponente konfigurieren. Diese Option ist eine der letzten Konfigurationsoptionen.

So erfassen Sie Informationen zum Stromverbrauch von Desktop-Geräten:

- Erstellen Sie ein Smart Label im Inventar für den Gehäusetyp.
- Erstellen Sie Berichte, in denen die Geräte nach Gehäusetyp gruppiert werden.
- Erstellen Sie im Inventar ein Smart Label für **Betriebszeit seit letztem Neustart**, das die Anzahl der Tage enthält, die für Sie relevant sind.

Energieverwaltungsskripte für Windows Geräte hinzufügen

Mit dieser Vorlage können Sie Energieverwaltungsprofile für Windows Geräte erstellen. Die Einstellungen für den Energieverbrauch bilden einen Kompromiss zwischen CPU-Nutzung und Energieverbrauch.

Auf Windows-Geräten wird die Energieverwaltung mithilfe des integrierten Befehls **powercfg** konfiguriert.

1. Rufen Sie die Seite *Windows Energieverwaltung* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Skripterstellung** und anschließend auf **Konfigurationsrichtlinien**.
   c. Klicken Sie im Fensterbereich *Konfigurationsrichtlinien* im Abschnitt *Windows* auf **Energieverwaltung**.
2. Wählen Sie auf der Seite *Konfigurationsrichtlinie: Windows Energieverwaltung* das Zielbetriebssystem aus.
3. Wählen Sie ein Profil aus: **Ausgeglichen**, **Höchstleistung**, **Energiesparmodus** oder **Benutzerdefiniert**.

   HINWEIS: Wenn Sie als Profil *Benutzerdefiniert* auswählen und unter *Festplatte* die Option *Festplatte ausschalten nach (Sekunden)* auf *0* (Null) setzen, wird die Festplatte nie ausgeschaltet.
4. Klicken Sie auf **Speichern**, um die Seite *Skript: Details bearbeiten* anzuzeigen.
5. Wählen Sie Optionen für Konfiguration, Bereitstellung und Zeitplanung aus und klicken Sie auf **Speichern**. Siehe Hinzufügen und Bearbeiten von Skripten.

Registrierungsskripte hinzufügen

Mit dieser Vorlage können Sie Skripte zum Erzwingen von Registrierungseinstellungen auf Windows-Geräten erstellen.

1. Mithilfe von `regedit.exe` können Sie in der Registrierung nach den gewünschten Werten suchen und diese exportieren.
2. Öffnen Sie die .reg-Datei mit den gewünschten Registrierungswerten in notepad.exe und kopieren Sie den Text.
3. Rufen Sie die Seite *Windows Registrierung* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Skripterstellung** und anschließend auf **Konfigurationsrichtlinien**.
   c. Klicken Sie im Fensterbereich *Konfigurationsrichtlinien* im Abschnitt *Windows* auf **Registrierung**.
4. Geben Sie die folgenden Informationen an:

Option	Beschreibung
Name	Ein Name, der das Skript identifiziert. Dieser Name wird auf der Seite *Skripte* angezeigt.
Registrierungsdatei	Die Registrierungswerte, die bei der Skriptausführung angewendet werden sollen.

5. Klicken Sie auf **Speichern**, um die Seite *Skriptdetail* anzuzeigen.
6. Wählen Sie die Optionen für die Konfiguration, Bereitstellung und Zeitplanung. Siehe Offline-KScripts, Online-KScripts oder Online-Shellskripte hinzufügen.
7. Klicken Sie zum Bearbeiten des unformatierten XML-Codes im Skript unter dem Abschnitt *Planen* auf **XML bearbeiten**.
8. Klicken Sie auf **Speichern**.

Es wird ein neues Skript erstellt, das überprüft, ob die Werte in der Registrierungsdatei mit den auf den Zielgeräten ermittelten Werten übereinstimmen. Alle fehlenden oder nicht korrekten Werte werden ersetzt.

Skripte für die Fehlerbehebung per Remote-Desktop-Steuerung hinzufügen

Mit dieser Vorlage können Sie ein Fehlerbehebungsskript für die Remote-Desktop-Steuerung auf Windows-Geräten erstellen.

Dieses Skript testet folgende Punkte:

- **Terminaldienste**: Damit Sie per Remotedesktop auf ein Windows-Gerät zugreifen können, müssen die Terminaldienste ausgeführt werden. Dieses Skript überprüft, ob die Terminaldienste ausgeführt werden.
- **Firewall-Konfiguration**: Falls die Windows-Firewall auf dem Gerät ausgeführt wird, testet das Skript auf Konfigurationen, die möglicherweise die Remote-Desktop-Steuerungsanfragen blockieren.

1. Rufen Sie die Seite *Fehlerbehebung per Remote-Desktop-Steuerung* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen*

aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.

b. Klicken Sie in der linken Navigationsleiste auf **Skripterstellung** und anschließend auf **Konfigurationsrichtlinien**.

c. Klicken Sie im Fensterbereich *Konfigurationsrichtlinien* im Abschnitt *Windows* auf **Fehlerbehebung per Remote-Desktop-Steuerung**.

2. Geben Sie die folgenden Informationen an:

Option	Beschreibung
Name	Ein Name, der das Skript identifiziert. Dieser Name wird auf der Seite *Skripte* angezeigt.
Firewall-Konfiguration	Geben Sie die Einstellungen an, die bei der Skriptausführung angewendet werden sollen.

3. Klicken Sie auf **Speichern**, um die Seite *Skriptdetail* anzuzeigen.
4. Wählen Sie die Optionen für die Konfiguration, Bereitstellung und Zeitplanung. Siehe Offline-KScripts, Online-KScripts oder Online-Shellskripte hinzufügen.
5. Klicken Sie zum Bearbeiten des unformatierten XML-Codes im Skript unter dem Abschnitt *Planen* auf **XML bearbeiten**.
6. Klicken Sie auf **Speichern**.

UltraVNC-Skripte hinzufügen

Mit dieser Vorlage können Sie ein Skript erstellen, das UltraVNC an Windows Geräte verteilt. UltraVNC ist eine kostenlose Anwendung, mit der sich Administratoren von einem Remote-Standort aus bei Geräten anmelden können.

Weitere Informationen zu UltraVNC finden Sie unter http://www.uvnc.com.

1. Rufen Sie die Seite *Windows UltraVNC* auf:

   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.

   b. Klicken Sie in der linken Navigationsleiste auf **Skripterstellung** und anschließend auf **Konfigurationsrichtlinien**.

   c. Klicken Sie im Fensterbereich *Konfigurationsrichtlinien* im Abschnitt *Windows* auf **UltraVNC**.

2. Geben Sie die folgenden Informationen an:

Option	Beschreibung
Name	Ein Name, der das Skript identifiziert. Dieser Name wird auf der Seite *Skripte* angezeigt.
Mirror-Treiber installieren	Installieren Sie den optionalen UltraVNC Mirror Video Driver. Mirror Video Driver ist ein Treiber, der schnellere und präzisere Aktualisierungen ermöglicht. Er stellt zudem eine direkte Verbindung zwischen dem Framebuffer-Speicher des Videotreibers und dem UltraWinVNC Server her. Indem der Framebuffer direkt verwendet wird, muss die CPU nicht für intensives Bildschirm-Blitting

Option	Beschreibung
	genutzt werden, wodurch die Geschwindigkeit erhöht und die CPU-Auslastung verringert wird.
Anzeigeprogramm installieren	Installieren Sie den optionalen UltraVNC Viewer. UltraVNC Viewer ist ein Tool zum Herstellen von Verbindungen zu VNC-Servern und dient dazu, Desktop-PC remote anzuzeigen. Installieren Sie UltraVNC Viewer nur, wenn Sie Remote-Sitzungen vom verwalteten Gerät aus starten müssen.
Taskleistensymbol deaktivieren	Deaktiviert das UltraVNC-Taskleistensymbol auf dem Gerät
Client-Optionen in der Taskleiste im Symbolmenü deaktivieren	Deaktiviert die Client-Optionen in der Taskleiste der Geräte Diese Option steht nur zur Verfügung, wenn **TrayIcon deaktivieren** aktiviert ist.
Eigenschaftenbereich deaktivieren	Deaktiviert den Eigenschaftenbereich von UltraVNC auf den Geräten
Schließen von UltraVNC durch Benutzer sperren	Untersagt es Gerätebenutzern, WinVNC zu schließen
Kennwort und **Schreibgeschütztes Kennwort**	Geben Sie ein Kennwort für die Authentifizierung an.
Windows Anmeldung erforderlich	Verwenden Sie die Authentifizierung per Windows Anmeldung und exportieren Sie die Zugriffssteuerungsliste (Access Control List, ACL) aus Ihrer VNC® Installation. Verwenden Sie `MSLogonACL.exe /e acl.txt`. Kopieren Sie den Inhalt der Textdatei in das Feld *ACL*.
Verschlüsselungsschlüssel	Verwendet die schlüsselbasierte Kodierung. Erstellen Sie einen Schlüssel und laden Sie diesen hoch, um die schlüsselbasierte Kodierung zu verwenden. a. Wählen Sie im UltraVNC Viewer in der Liste DSPLugin die Option MSRC4Plugin aus. b. Klicken Sie auf **Config** (Konfigurieren) und geben Sie dann den vollständigen Pfad der Datei ein. c. Klicken Sie auf **Gen Key** (Schlüssel erstellen) und laden Sie anschließend die Schlüsseldatei hoch.

3. Klicken Sie auf **Speichern**, um die Seite *Skriptdetail* anzuzeigen.
4. Sehen Sie das von der Vorlage erzeugte Skript durch, um die Ergebnisse zu überprüfen.
5. Wählen Sie die Optionen für die Konfiguration, Bereitstellung und Zeitplanung. Siehe Offline-KScripts, Online-KScripts oder Online-Shellskripte hinzufügen.
6. Klicken Sie zum Bearbeiten des unformatierten XML-Codes im Skript unter dem Abschnitt *Planen* auf **XML bearbeiten**.
7. Klicken Sie auf **Speichern**.

Deinstallationsskripte hinzufügen

Mit dieser Vorlage können Sie ein Skript zum Verwalten von Anwendungen und Prozessen auf Windows-Geräten erstellen. Skripte können Deinstallationsbefehle ausführen, Prozesse beenden und Verzeichnisse löschen.

1. Rufen Sie die Seite *Windows Deinstallationsprogramm* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Skripterstellung** und anschließend auf **Konfigurationsrichtlinien**.
   c. Klicken Sie im Fensterbereich *Konfigurationsrichtlinien* im Abschnitt *Windows* auf **Deinstallationsprogramm**.
2. Geben Sie die folgenden Informationen an:

Option	Beschreibung
Name	Ein Name, der das Skript identifiziert. Dieser Name wird auf der Seite *Skripte* angezeigt.
Software	Die Anwendung für das Skript. Um nach einer Anwendung zu suchen, beginnen Sie mit Ihrer Eingabe in das Feld.
Datei	Die Befehlsinformationen. Wenn Sie die Anwendung auswählen, versucht die Vorlage, das Verzeichnis, die Datei und die Parameter für den Deinstallationsbefehl bereitzustellen. Überprüfen Sie, ob die Werte korrekt sind.
Parameter	
Verzeichnis	
Verzeichnis löschen	Der vollständige Name des Verzeichnisses, das gelöscht werden soll, bevor der Deinstallationsbefehl ausgeführt wird. Beispiel: `C:\Programme\`**Beispielanwendung**`\`.
Prozess abbrechen	Der vollständige Name des Prozesses, der beendet werden soll, bevor der Deinstallationsbefehl ausgeführt wird. Beispiel: `notepad.exe`.

3. Klicken Sie auf **Speichern**, um die Seite *Skriptdetail* anzuzeigen.
4. Wählen Sie die Optionen für die Konfiguration, Bereitstellung und Zeitplanung. Siehe Offline-KScripts, Online-KScripts oder Online-Shellskripte hinzufügen.
5. Klicken Sie zum Bearbeiten des unformatierten XML-Codes im Skript unter dem Abschnitt *Planen* auf **XML bearbeiten**.
6. Klicken Sie auf **Speichern**.

Verwenden der Mac OS X Konfigurationsrichtlinien

Sie können mithilfe von Konfigurationsrichtlinienvorlagen Skripte zum Konfigurieren von Richtlinien auf Mac OS X Geräten erstellen.

Skripte für Active Directory hinzufügen

Verwenden Sie diese Vorlage, um Skripte zu erstellen, die Geräte zu Domänen auf Mac OS X Geräten hinzufügen oder sie daraus entfernen. Mit einem solchen Skript können Sie auch sicherstellen, dass sich Ihre Mac OS X Geräte bei den Active Directory Datenbanken anmelden.

Beim Erstellen des Skripts müssen Sie einen Benutzernamen und ein Kennwort für ein Netzwerkkonto mit Administratorrechten angeben, um Geräte zu der angegebenen Domäne hinzuzufügen oder aus dieser zu entfernen.

1. Rufen Sie die Seite *Mac Active Directory* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Skripterstellung** und anschließend auf **Konfigurationsrichtlinien**.
   c. Klicken Sie im Fensterbereich *Konfigurationsrichtlinien* im Abschnitt *Mac* auf **Active Directory**.
2. Geben Sie die folgenden Informationen an:

Option	Beschreibung
Name	Ein Name, der das Skript identifiziert. Dieser Name wird auf der Seite *Skripte* angezeigt.
Aktion	Geben Sie an, ob Sie ein Gerät zur aktuellen Domäne hinzufügen bzw. davon entfernen möchten.
Netzwerk-Anmeldeinformationen	Geben Sie Ihren Administratorbenutzernamen und das Kennwort ein. **HINWEIS:** Das erstellte Skript geht davon aus, dass Sie über Root-Zugriff verfügen, und zeigt Ihr Kennwort unverschlüsselt (Klartext) an. Stellen Sie deshalb sicher, dass dieses Skript nur von vertrauenswürdigen Personen verwendet wird.

Option	Beschreibung
Zu konfigurierende Domäne	Geben Sie den LDAP-Domänennamen, die Benutzerauthentifizierungsinformationen sowie weitere Informationen ein.

3. Klicken Sie auf **Speichern**, um die Seite *Skriptdetail* anzuzeigen.
4. Wählen Sie die Optionen für die Konfiguration, Bereitstellung und Zeitplanung. Siehe Offline-KScripts, Online-KScripts oder Online-Shellskripte hinzufügen.
5. Klicken Sie zum Bearbeiten des unformatierten XML-Codes im Skript unter dem Abschnitt *Planen* auf **XML bearbeiten**.
6. Klicken Sie auf **Speichern**.

Energieverwaltungsskripte hinzufügen

Mit dieser Vorlage können Sie Energieverwaltungsprofile für Mac OS X Geräte erstellen. Die Einstellungen für den Energieverbrauch bilden einen Kompromiss zwischen CPU-Nutzung und Energieverbrauch.

Um auf jede Energiequelle eindeutige Einstellungen anzuwenden, erstellen Sie mehrere Konfigurationsskripte. Auf einigen Geräten werden einige Funktionen möglicherweise nicht unterstützt.

1. Rufen Sie die Seite *Energieverwaltungseinstellungen für Mac* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Skripterstellung** und anschließend auf **Konfigurationsrichtlinien**.
   c. Klicken Sie im Fensterbereich *Konfigurationsrichtlinien* im Abschnitt *Mac* auf **Energieverwaltung**.
2. Geben Sie die folgenden Informationen an:

Option	Beschreibung
Name	Ein Name, der das Skript identifiziert. Dieser Name wird auf der Seite *Skripte* angezeigt.
Profilname	Wählen Sie die zu verwendende Profiloption: • **Höhere Energieeinsparungen**: Erzwingt Einstellungen, die Energie sparen. Dies führt ggf. zu einer geringeren Leistung. Wenn Sie diese Einstellung wählen, können Sie die Optionen im Abschnitt *Profiloptionen* nicht bearbeiten. • **Normal**: Verwenden Sie die Standardeinstellungen. Wenn Sie diese Einstellung wählen, können Sie die Optionen im Abschnitt *Profiloptionen* nicht bearbeiten. • **Bessere Leistung**: Erzwingt Einstellungen, die die Leistung optimieren. Dies führt ggf. zu einem höheren Stromverbrauch. Wenn Sie diese Einstellung wählen, können Sie die

Option	Beschreibung
	Optionen im Abschnitt *Profiloptionen* nicht bearbeiten. • **Benutzerdefiniert**: Verwendet benutzerdefinierte Profiloptionen. Wenn Sie diese Einstellung wählen, können Sie die Optionen im Abschnitt *Profiloptionen* bearbeiten.
Energiequelle	Wählen Sie eine Energiequelle: • **Alle**: Die Richtlinie wird immer angewandt, unabhängig von der Energiequelle des Geräts. • **Akku**: Die Richtlinie wird nur angewandt, wenn das Gerät die interne Akkuversorgung nutzt. • **Ladegerät (Netzanschluss)**: Die Richtlinie wird nur angewandt, wenn das Gerät mit einer Steckdose verbunden ist. • **UPS**: Die Richtlinie wird nur angewandt, wenn das Gerät mit einer unterbrechungsfreien Stromversorgung verbunden ist.
Betriebssystem	Wenn Sie in der Dropdown-Liste *Profil* die Option **Benutzerdefiniert** auswählen, geben Sie das Betriebssystem an, für das diese Richtlinie gilt. Die *Profiloptionen* werden aktualisiert, sodass nur noch die verfügbaren Optionen für die ausgewählte Version angezeigt werden.

3. Klicken Sie auf **Speichern**, um die Seite *Skriptdetail* anzuzeigen.
4. Wählen Sie die Optionen für die Konfiguration, Bereitstellung und Zeitplanung. Siehe Offline-KScripts, Online-KScripts oder Online-Shellskripte hinzufügen.
5. Klicken Sie zum Bearbeiten des unformatierten XML-Codes im Skript unter dem Abschnitt *Planen* auf **XML bearbeiten**.
6. Klicken Sie auf **Speichern**.

VNC-Skripte hinzufügen

Mit dieser Vorlage können Sie Skripte erstellen, die die integrierten VNC-Einstellungen auf Mac OS®-Geräten konfigurieren. Die VNC-Einstellungen bestimmen, ob Anzeigeprogramme den Gerätebildschirm steuern können.

Mit diesem Skript können Sie außerdem die Bildschirmfreigabe aktivieren oder deaktivieren. Dafür sind ein Benutzername und ein Kennwort eines Kontos auf dem Mac erforderlich, um eine Verbindung von einem anderen Mac, auf dem Mac OS X ausgeführt wird, herzustellen. Gehen Sie bei Verwendung dieses Skripts vorsichtig vor: Die Anmeldeinformationen sind zwar verschlüsselt, doch die VNC-Sitzung ist es möglicherweise nicht.

1. Rufen Sie die Seite *Mac VNC* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.

b. Klicken Sie in der linken Navigationsleiste auf **Skripterstellung** und anschließend auf **Konfigurationsrichtlinien**.

c. Klicken Sie im Fensterbereich *Konfigurationsrichtlinien* im Abschnitt *Mac* auf **VNC**.

2. Geben Sie die folgenden Informationen an:

Option	Beschreibung
Name	Ein Name, der das Skript identifiziert. Dieser Name wird auf der Seite *Skripte* angezeigt.
Aktiviert	Aktivieren Sie die Richtlinie.
Kennwort	Geben Sie ein Kennwort für den VNC ein.

3. Klicken Sie auf **Speichern**, um die Seite *Skriptdetail* anzuzeigen.
4. Wählen Sie die Optionen für die Konfiguration, Bereitstellung und Zeitplanung. Siehe Offline-KScripts, Online-KScripts oder Online-Shellskripte hinzufügen.
5. Klicken Sie zum Bearbeiten des unformatierten XML-Codes im Skript unter dem Abschnitt *Planen* auf **XML bearbeiten**.
6. Klicken Sie auf **Speichern**.

Richtlinien und Skripte bearbeiten

Sie können Richtlinien und Skripte nach Bedarf bearbeiten.

1. Rufen Sie die *Skriptdetailseite* auf:

   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.

   b. Klicken Sie in der linken Navigationsleiste auf **Skripterstellung** und anschließend auf **Skripte**.

   c. Führen Sie eine der folgenden Aktionen aus, um die *Skriptdetailseite* anzuzeigen:

   - Klicken Sie auf den Namen eines Skripts.
   - Wählen Sie **Aktion auswählen** > **Neu**.

2. Ändern Sie die Optionen für die Konfiguration, Bereitstellung und Zeitplanung.

   Siehe Offline-KScripts, Online-KScripts oder Online-Shellskripte hinzufügen.

3. Klicken Sie unten auf der Seite auf **klicken Sie hier** neben eine der folgenden Optionen:

   - *Zur Überarbeitung der Richtlinie mit dem ursprünglichen Editor*: **Anzeigen und Bearbeiten der ursprünglichen Einstellungen in der Vorlage**
   - *Zur Bearbeitung der Richtlinie mit diesem Editor*: **Alle Einstellungen anzeigen und bearbeiten**

4. Bearbeiten Sie die Richtlinie und klicken Sie auf **Speichern**.

Die Skriptprotokolle durchsuchen

Sie können in den Skriptprotokollen nach Textfolgen suchen. Wenn auf der Appliance die Organisationskomponente aktiviert wurde, können Sie für jede Organisation individuelle Skriptprotokolle durchsuchen.

Beim Ausführen von Skripten auf verwalteten Geräten werden Protokolle erstellt und auf die Appliance hochgeladen. Sie können in den Skriptprotokollen nach Textzeichenfolgen suchen und Labels auf Geräte anwenden, deren Protokolle dem Suchtext entsprechen. Dann können Sie für die Geräte mit den Labels nach Bedarf Aktionen ausführen.

1. Rufen Sie die Seite *Skriptprotokolle durchsuchen* auf.
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Skripterstellung** und anschließend auf **Skriptprotokolle durchsuchen**.
2. Geben Sie im Feld *Suchen nach* die Suchkriterien oder die Textfolge ein, nach denen bzw. der Sie suchen möchten. Textfolgen müssen mindestens vier Zeichen lang sein. Bei Suchen mit kürzeren Textfolgen werden keine Übereinstimmungen gefunden.

   Sie können die Suchkriterien mithilfe folgender Operatoren konkretisieren:

Operator	Function
+	Mit einem vorangestellten Pluszeichen suchen Sie nach Einträgen, die den Text enthalten.
-	Mit einem vorangestellten Minuszeichen suchen Sie nach Einträgen, die den Text nicht enthalten.
*****	Mit einem nachgestellten Stern suchen Sie in den Protokollen nach Wörtern, die mit den angegebenen Zeichen beginnen.
„	Mit Text zwischen doppelten Anführungszeichen suchen Sie nach exakten Treffern für den Suchausdruck.

3. Wählen Sie Suchkriterien aus:

Option	Beschreibung
Alle hochgeladenen Protokolle	Durchsucht alle verfügbaren Skriptprotokolle. Wenn für Ihre Appliance die Organisationskomponente aktiviert ist, werden alle Protokolle für die ausgewählte Organisation durchsucht. **HINWEIS:** Skriptprotokolle werden bei Appliance-Upgrades gelöscht. Nach einem Appliance-Upgrade stehen vor dem Upgrade hochgeladene Protokolle nicht mehr zur Verfügung.
Zuletzt hochgeladene Protokolle	Durchsucht die aktuellen Skriptprotokolle Wenn für Ihre Appliance die Organisationskomponente aktiviert ist, werden alle Protokolle für die ausgewählte Organisation durchsucht.
Skripte	Durchsucht Protokolle zu allen Skripten oder nur das angegebene Skript.

Option	Beschreibung
Protokoll	Durchsucht alle Protokolle oder nur das angegeben Protokoll.
Label	Durchsucht von allen Geräten hochgeladene Protokolle oder Protokolle, die von Geräten hochgeladen wurden, die dem angegebenen Label zugeordnet sind.

4. Klicken Sie auf **Suchen**.

   In den Suchergebnissen werden die Protokolle und die Geräte angezeigt, von denen die Protokolle hochgeladen wurden.
5. Sie können den angezeigten Geräten ein Label zuweisen, indem Sie in den Suchergebnissen ein Label aus der Dropdown-Liste auswählen.

Exportieren von Skripten

Wenn Sie über mehrere Organisationen oder Appliances verfügen, können Sie Skripte exportieren und nach Bedarf an andere Organisationen und Appliances übertragen.

Siehe Informationen zum Importieren und Exportieren von Anwendungsressourcen.

Verwalten von Mac Profilen

Sie können die Appliance verwenden, um Mac Profile an vom Agenten verwaltete Geräte mit Mac OS X zu verteilen. Mac Profile beinhalten Payloads oder Konfigurationseinstellungen für Richtlinien auf Benutzer- oder Systemebene.

Die Verteilung von Mac Profilen über die Appliance stellt eine effiziente Methode dar, Einstellungen auf von Ihnen verwalteten Mac Geräten zu konfigurieren, und bietet eine Alternative zur Konfiguration und Verteilung von Profilen über OS X Server.

Sie können Mac Profil-Payloads und -Konfigurationseinstellungen auf Benutzer- und Systemebene über die **Administratorkonsole** der Appliance konfigurieren. Darüber hinaus können Sie mithilfe des Apple Profile Manager benutzerdefinierte Payloads erstellen, die `MOBILECONFIG`-Datei mit diesen Payloads herunterladen und diese Datei zur Verteilung auf die Appliance hochladen.

Weitere Informationen zu Mac Profilen finden Sie unter http://help.apple.com/profilemanager/mac/4.0.

Verteilung von Profilen durch den KACE Agent

Wenn Sie ein neues Mac Profil hinzufügen oder hochladen, erstellt die Appliance das Online-KScript, das für die Installation oder Entfernung der Profile auf/von den Geräten erforderlich ist. Wie andere Online-KScripts werden Skripte, die Mac Profile enthalten, ausgeführt, wenn der KACE Agent gemäß dem Zeitplan und den Bereitstellungsoptionen im Profil mit dem Zielgerät verbunden wird.

Verfolgen von Änderungen an Mac Profileinstellungen

Wenn Verlaufsabonnements zur Aufbewahrung von Informationen konfiguriert wurden, können Sie Details zu den an Einstellungen, Assets und Objekten vorgenommenen Änderungen anzeigen. Diese Informationen

beinhalten auch das Datum der Änderung und den Benutzer, der diese vorgenommen hat. Dies kann bei der Fehlerbehebung nützlich sein.

Siehe Informationen zu den Verlaufseinstellungen.

Hinzufügen, Bearbeiten und Hochladen von Mac Profilen

Sie können Mac Benutzer- und Systemprofile auf der Appliance erstellen und die Mac Profile nach Bedarf anpassen. Darüber hinaus können Sie `MOBILECONFIG`-Dateien hochladen, die die Konfigurationsinformationen zur Appliance enthalten.

Mac Benutzerprofile hinzufügen oder bearbeiten

Mit der **Administratorkonsole** können Sie Mac Benutzerprofile zur Appliance hinzufügen. Benutzerprofile enthalten Konfigurationseinstellungen, die für Benutzer gelten, z. B. E-Mail-Einstellungen. Zur Appliance hinzugefügte Benutzerprofile können für Mac OS X Geräte mit Agentenverwaltung bereitgestellt werden. Eine Liste der unterstützten Mac OS X Versionen finden Sie in den *technischen Spezifikationen*, die auf der Produktdokumentationsseite verfügbar sind: https://support.quest.com/kace-systems-management-appliance/technical-documents.

Beim Hinzufügen oder Bearbeiten von Profilen werden für die Konfiguration von Exchange-, LDAP- und Mail-Payloads die entsprechenden Konto-, Server- und Portinformationen benötigt.

HINWEIS: Sie können die von Ihnen in der **Administratorkonsole** konfigurierten Payloads von Profilen bearbeiten. Es ist jedoch nicht möglich, die auf die **Administratorkonsole** hochgeladenen Payloads von Profilen anzuzeigen oder zu bearbeiten.

1. Rufen Sie die Seite *Mac Profil-Detail* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Skripterstellung** und anschließend auf **Mac Profile**.
   c. Führen Sie einen der folgenden Schritte aus:
   - Klicken Sie auf den Namen eines Profils.
   - Klicken Sie auf **Aktion auswählen** > **Neues Benutzerprofil**.
2. Geben Sie im Bereich *Allgemeine Optionen* die folgenden Informationen ein:

Option	Beschreibung
Profilname	Der in der Liste *Mac Profile* anzuzeigende Name. Dieser Name muss nicht eindeutig sein, sollte aber aussagekräftig genug sein, um das Profil in einer Liste zu erkennen. **HINWEIS:** Sie können den Namen eines Profils jederzeit ändern. Wenn Sie jedoch den Namen eines Profils nach seiner Installation auf einem Gerät ändern möchten, wird der Profilname nicht auf dem Gerät aktualisiert. Das Profil wird weiterhin anhand des Namens identifiziert, den es bei der Installation hatte.

Option	Beschreibung
Beschreibung	Zusätzliche Informationen zum Profil, z. B. die Konfigurationseinstellungen oder der Verwendungszweck.
Benutzer kann Profil entfernen	Gibt an, ob die Benutzer das Profil von ihren Geräten entfernen können. Zur Auswahl stehen folgende Optionen: • **Nie**: Die Benutzer können das Profil nicht entfernen. • **Immer**: Die Benutzer können das Profil jederzeit ohne Eingabe eines Kennworts entfernen. • **Mit Kennwort**: Die Benutzer können das Profil entfernen, wenn sie das mit dem Profil verknüpfte Kennwort eingeben.
Profil automatisch entfernen	Gibt an, ob das Profil nach einem angegebenen Zeitraum automatisch entfernt wird. Diese Aktion ist hilfreich, wenn Sie Geräte konfigurieren, für die nach einem bestimmten Datum andere Profile bereitgestellt werden müssen, z. B. am Ende eines Schulhalbjahrs. Zur Auswahl stehen folgende Optionen: • **Nie**: Das Profil wird nicht nach Zeitplan automatisch entfernt. • **An einem bestimmten Datum**: Das Profil wird am angegebenen Datum automatisch entfernt. Das Datum muss im Format **mm/tt/jjjj** angegeben werden. • **Nach**: Das Profil wird nach dem Ablauf des angegebenen Zeitraums entfernt. Der Zeitraum kann in Tagen oder Stunden angegeben werden.

3. **Optional**: Im Abschnitt *Payloads* können Sie Konfigurationseinstellungen für Exchange, LDAP oder Mail hinzufügen.
   - Hinzufügen oder Bearbeiten von Exchange-Konfigurationsinformationen:

> **HINWEIS:** Um die Benutzer zur Eingabe ihrer Informationen aufzufordern, z. B. des Benutzernamens, der E-Mail-Adresse oder des Kennworts, lassen Sie die entsprechenden Felder leer. Einige Felder, z. B. *Kontoname*, dürfen jedoch nicht leer gelassen werden.

Option	Beschreibung
Kontoname	Der Name für die Identifizierung des Kontos.
Benutzer	Der Name des Benutzers.
E-Mail-Adresse	Die Adresse für das E-Mail-Konto.
Kennwort	Das Kennwort für das E-Mail-Konto.

Option	Beschreibung
Interner Exchange Host und Port	Der Hostname des internen Exchange-Servers und der für die E-Mail-Kommunikation verwendete Port.
Externer Exchange Host und Port	Der Hostname des externen Exchange-Servers und der für die E-Mail-Kommunikation verwendete Port.
Pfad interner Server	Der Pfad zum Server im internen Netzwerk.
Pfad externer Server	Der Pfad zum Server im externen Netzwerk.
SSL für internen Exchange Host verwenden	Gibt an, ob Secure Sockets Layer für innerhalb der Domäne übertragene E-Mails verwendet werden soll.
SSL für externen Exchange Host verwenden	Gibt an, ob Secure Sockets Layer für außerhalb der Domäne übertragene E-Mails verwendet werden soll.

- Hinzufügen oder Bearbeiten von LDAP-Konfigurationsinformationen:

> **HINWEIS:** Um die Benutzer zur Eingabe ihrer Informationen aufzufordern, z. B. des Benutzernamens oder des Kennworts, lassen Sie die entsprechenden Felder leer. Einige Felder, z. B. *Konto-Hostname*, dürfen jedoch nicht leer gelassen werden.

Option	Beschreibung
Kontobeschreibung	Der Name des LDAP-Kontos, z. B. `Beispielunternehmen LDAP-Konto`.
Kontobenutzername	Der Benutzername des Kontos, das für die Anmeldung am LDAP-Server verwendet werden soll.
Kontokennwort	Das Kennwort des Kontos, das für die Anmeldung beim LDAP-Server verwendet werden soll.
Kontohostname	Der Hostname oder die IP-Adresse des LDAP-Servers.
SSL verwenden	Gibt an, ob Secure Sockets Layer für Verbindungen mit dem LDAP-Server verwendet werden soll.

Option	Beschreibung
Sucheinstellungen	Die für die Suche nach Informationen auf dem LDAP-Server verwendeten Einstellungen.
• **Beschreibung**	Informationen zur Unterscheidung der Suchinformationen in einer Liste.
• **Bereich**	Die Suchtiefe. Gibt an, wo die Suche durchgeführt wird: • **Basis**: Beinhaltet nur Objekte der Basis- oder Nullklasse. • **Eine Klasse**: Beinhaltet Objekte, die der Basisklasse unmittelbar untergeordnet sind, nicht aber die Basisklasse selbst. • **Unterstruktur**: Beinhaltet Objekte der Basisklasse und der Unterstruktur.
• **Suchbasis**	**Suchbasis**: Der Speicherort im Verzeichnis, an dem die Suche beginnt. Die Suchbasis legt einen Speicherort oder Container in der LDAP- oder Active Directory-Struktur fest. Die Kriterien sollten alle Benutzer umfassen, die authentifiziert werden sollen. Geben Sie für die Basis-DN die genaueste Kombination aus OUs, DCs oder CNs ein, die Ihren Kriterien entsprechen, die von links (sehr genau) bis rechts (sehr allgemein) reichen. Dieser Pfad führt beispielsweise zum Container mit den Benutzern, die Sie authentifizieren müssen: OU=end_users,DC=company,DC=com.

◦ Hinzufügen oder Bearbeiten von Mail-Konfigurationsinformationen:

> **HINWEIS:** Um die Benutzer zur Eingabe ihrer Informationen aufzufordern, z. B. des Anzeigenamens oder der E-Mail-Adresse, lassen Sie die entsprechenden Felder leer. Einige Felder, z. B. *Server für eingehende E-Mails*, dürfen jedoch nicht leer gelassen werden.

Option	Beschreibung
Kontobeschreibung	Der Name des Kontos, z. B. `Beispielunternehmen Mail-Konto`.
Kontotyp	Das für den Zugriff auf das Konto verwendete Protokoll (POP oder IMAP).
Benutzeranzeigename	Darstellung des Benutzernamens im Feld *Von* in E-Mail-Nachrichten.
E-Mail-Adresse	Die E-Mail-Adresse des Benutzers.
Server und Port für eingehende E-Mails	Der Hostname oder die IP-Adresse und die Port-Nummer für eingehende E-Mails.

Option	Beschreibung
Server und Port für ausgehende E-Mails	Der Hostname oder die IP-Adresse und die Port-Nummer für ausgehende E-Mails. Verwenden Sie die folgenden Standard-Port-Zuweisungen: • SMTP: 25 (465 mit SSL) • POP3: 110 (995 mit SSL) • IMAP: 143 (993 mit SSL)
Benutzername für eingehende E-Mails	Der Benutzername für den Server für eingehende E-Mails.
Benutzername für ausgehende E-Mails	Der Benutzername für den Server für ausgehende E-Mails.
Authentifizierungsmethode für eingehende E-Mails	Die Methode für die Authentifizierung des Benutzers für eingehende E-Mails. Mögliche Authentifizierungsmethoden sind Kennwort, MD5 Challenge-Response, NTLM und HTTP MD5 Digest.
Authentifizierungsmethode für ausgehende E-Mails	Die Methode für die Authentifizierung des Benutzers für ausgehende E-Mails. Mögliche Authentifizierungsmethoden sind Kennwort, MD5 Challenge-Response, NTLM und HTTP MD5 Digest.
SSL für eingehende E-Mails verwenden	Gibt an, ob Secure Socket Layer für an das Benutzerkonto gelieferte E-Mails verwendet wird.
SSL für ausgehende E-Mails verwenden	Gibt an, ob Secure Socket Layer für vom Benutzerkonto gesendete E-Mails verwendet wird.

4. (Optional) Wählen Sie im Abschnitt *Bereitstellen* die Zielgeräte für das Profil aus:

TIPP: Sie können ein Profil ohne Auswahl von Zielgeräten erstellen. Profile können jedoch erst nach der Auswahl der Zielgeräte bereitgestellt werden.

Option	Beschreibung
Alle Geräte	Das Profil wird an alle KACE Geräte mit Agentenverwaltung mit einer unterstützten Version von Mac OS X (Version 10.8, 10.9 oder 10.10) verteilt. Wenn auf Ihrer Appliance die Organisationskomponente aktiviert ist, werden alle unterstützten Mac Geräte der ausgewählten Organisation in die Verteilung einbezogen.
Labels	Das Profil wird nur an die Geräte verteilt, die das von Ihnen ausgewählte Label aufweisen. Durch Begrenzen der Verteilung auf Labels, insbesondere auf Smart Labels, wird sichergestellt, dass Profile richtig angewendet werden. Um diese Option verwenden zu können, müssen Sie bereits Labels oder Smart Labels erstellt haben. Siehe Smart Labels für Geräte hinzufügen.

Option	Beschreibung
Geräte	Das Profil wird an die von Ihnen ausgewählten unterstützten Mac OS X Geräte (Version 10.8, 10.9 oder 10.10) verteilt. Um nach Geräten zu suchen, beginnen Sie mit einer entsprechenden Eingabe in das Feld.
Betriebssysteme	Das Betriebssystem, auf dem die Anwendung ausgeführt wird. Die Bereitstellung der Anwendungen erfolgt nur auf Geräten mit den ausgewählten Betriebssystemen. a. Klicken Sie auf **Betriebssysteme verwalten**. b. Wählen Sie im daraufhin angezeigten Dialogfeld **Betriebssysteme** die Betriebssystemversionen in der Navigationsstruktur aus. Sie haben die Möglichkeit, Betriebssystemversionen nach Familie, Produkt, Architektur, Versions-ID oder Build-Version auszuwählen. Je nach Bedarf können Sie eine bestimmte Build-Version oder einen übergeordneten Knoten auswählen. Wenn Sie einen übergeordneten Knoten im Baum auswählen, werden die zugehörigen untergeordneten Knoten automatisch mit ausgewählt. Aufgrund dieses Verhaltens können Sie beliebige zukünftige Betriebssystemversionen auswählen, da Geräte in Ihrer verwalteten Umgebung hinzugefügt oder aktualisiert werden. Wenn Sie beispielsweise alle aktuellen und zukünftigen Versionen auswählen möchten, die mit einem Mac 10.11 El Capitan x86-Architektur verbunden sind, wählen Sie unter **Mac** > **10.11 El Capitan** die Option **x86** aus.
Alle entfernen	Alle ausgewählten Geräte aus der Liste *Geräte* in diesem Abschnitt entfernen.

5. Wählen Sie im Abschnitt *Planen* die Optionen für die Verteilung des Profils an die Zielgeräte aus:

Option	Beschreibung
Kein(e)	Keine Verteilung des Profils per Zeitplan. Profile, deren Zeitpläne auf **Kein(e)** eingestellt sind, haben auf der Liste *Mac Profile* den Status **Deaktiviert**. Profile, deren Zeitpläne auf **Kein(e)** eingestellt sind, können jedoch trotzdem bereitgestellt werden, wenn Sie unten auf der Seite **Jetzt ausführen** auswählen.
Alle n Minuten/Stunden	Der Vorgang wird im angegebenen Intervall durchgeführt.
Täglich/an einem bestimmten Tag um HH:MM	Die Erfassung wird täglich zu einem bestimmten Zeitpunkt oder an einem bestimmten Wochentag um eine bestimmte Uhrzeit ausgeführt.

Option	Beschreibung
Ausführen am n-ten jedes Monats/eines bestimmten Monats um HH:MM	Die Erfassung wird jeden Monat oder in einem bestimmten Monat an einem festgelegten Datum zu einer festgelegten Uhrzeit ausgeführt.
Ausführen am n-ten Wochentag **jedes Monats/ eines bestimmten Monats um HH:MM**	Die Erfassung wird jeden Monat oder in einem bestimmten Monat an einem festgelegten Wochentag zu einer festgelegten Uhrzeit ausgeführt.

Benutzerdefiniert	Ausführung nach einem benutzerdefinierten Zeitplan.
	Verwenden Sie das Standard-5-Feld-Cron-Format (das erweiterte Cron-Format wird nicht unterstützt):
	`* * * * *`
	`| | | | +————————Wochentag (0-6) (Sonntag=0)`
	`| | | +————————Monat (1-12)`
	`| | +————————Monatstag (1-31)`
	`| +————————Stunde (0-23)`
	`+————————Minute (0-59)`
	Verwenden Sie bei der Angabe von Werten die folgenden Zeichen:
	• **Leerzeichen( )**: Die einzelnen Felder mit einem Leerzeichen trennen.
	• **Sternchen (*)**: Ein Sternchen repräsentiert den gesamten Wertebereich in einem Feld. Zum Beispiel repräsentiert ein Sternchen im Stundenfeld eine beliebige Stunde.
	• **Kommas (,)**: Mehrere Werte in einem Feld werden mit einem Komma getrennt. Zum Beispiel werden mit `0,6` im Feld „Wochentag“ Sonntag und Samstag angegeben.
	• **Bindestriche (-)**: Mit einem Bindestrich wird ein Wertebereich in einem Feld angegeben. Zum Beispiel entspricht `1-5` im Feld „Wochentag“ `1,2,3,4,5`, d. h. Montag bis Freitag.
	• **Schrägstriche (/)**: Die Angabe der Zeitabstände, mit denen eine Aktion wiederholt werden soll, erfolgt mit einem Schrägstrich. Zum Beispiel entspricht `*/3` im Feld Stunde `0,3,6,9,12,15,18,21`. Das Sternchen (`*`) gibt jede Stunde an, mit `/3` erfolgt aber eine Einschränkung auf durch drei teilbare Stunden.

Option	Beschreibung
	Beispiele: • `15 * * * * Jeden Tag 15 Minuten nach jeder vollen Stunde ausführen` • `0 22 * * * Jeden Tag um 22:00 Uhr ausführen` • `0 0 1 1,6 * Am 1. Januar und 1. Juni um 00:00 Uhr ausführen` • `30 8,12 * * 1-5 An Wochentagen um 08:30 Uhr und 12:30 Uhr ausführen` • `0 2 */2 * * Jeden zweiten Tag um 02:00 Uhr ausführen`
Aufgabenplan anzeigen	Klicken Sie, um den Aufgabenplan anzuzeigen. Im Dialogfeld *Taskplan* wird eine Liste der geplanten Ziele angezeigt. Klicken Sie auf eine Aufgabe, um die Aufgabendetails anzuzeigen. Weitere Informationen hierzu finden Sie unter Aufgabenpläne anzeigen.

6. Wählen Sie im Abschnitt *Bereitstellungsoptionen* die Optionen für die Benutzerführung bezüglich der Profilinstallation:

Option	Beschreibung
Laufzeit-Aufforderung für angemeldete Benutzer	Wenn der Agent mit der Profilinstallation beginnt, wird den am Zielgerät angemeldeten Benutzern eine Aufforderung angezeigt.
Anmelde-Aufforderung für alle Benutzer	Bei jeder Anmeldung am Zielgerät werden die Benutzer zur Installation des Profils aufgefordert, wenn sie die Installation nicht bereits vorgenommen haben.
Sowohl Laufzeit- als auch Anmelde-Aufforderungen	Wenn der Agent mit der Profilinstallation beginnt, werden die am Zielgerät angemeldeten Benutzer zur Installation des Profils aufgefordert, wenn sie die Installation nicht bereits vorgenommen haben. Benutzer, die sich nach der Ausführung des Skripts anmelden, werden ebenfalls zur Installation des Profils aufgefordert.

7. Wählen Sie unten auf der Seite eine der folgenden Aktionen aus:

Option	Beschreibung
Speichern	Das Profil speichern und zur Liste *Mac Profile* zurückkehren.
Jetzt ausführen	Auf Zielgeräten mit einer aktiven Agentenverbindung mit der Appliance das Profil jetzt gemäß den ausgewählten Bereitstellungsoptionen installieren. Siehe Verwenden der Befehle "Ausführen" und "Jetzt ausführen".

Option	Beschreibung
Duplizieren	Eine Kopie des Profils erstellen, wobei dem Profilnamen `Kopie von` vorangestellt wird. Diese Option ist nicht für neue Profile verfügbar, die noch nicht gespeichert wurden. Siehe Mac Profile zu vorhandenen Profilen als Vorlage hinzufügen.
Entfernen	Erstellen eines Profils, das für die Entfernung des Profils von Zielgeräten verwendet werden kann. Diese Option ist nicht für neue Profile verfügbar, die noch nicht gespeichert wurden. Siehe Mac Profile von verwalteten Geräten entfernen.
Löschen	Entfernen des Profils von der Appliance. Dadurch wird das Profil nicht von Geräten entfernt, auf denen es installiert ist. Diese Option ist nicht für neue Profile verfügbar, die noch nicht gespeichert wurden. Siehe Mac Profile aus der Appliance löschen.
Abbrechen	Änderungen verwerfen und zur Liste *Mac Profile* zurückkehren.

Mac Systemprofile hinzufügen oder bearbeiten

Mit der **Administratorkonsole** können Sie Mac Systemprofile zur Appliance hinzufügen. Systemprofile enthalten Konfigurationseinstellungen, die für Geräte gelten, z. B. Kennungsanforderungen. Zur Appliance hinzugefügte Systemprofile können für Mac OS X Geräte mit Agentenverwaltung bereitgestellt werden. Eine Liste der unterstützten Mac OS X Versionen finden Sie in den *technischen Spezifikationen*, die auf der Produktdokumentationsseite verfügbar sind: https://support.quest.com/kace-systems-management-appliance/technical-documents.

Sie haben Richtlinien für den Zugriff auf Apps und die Einstellung von Kennungen festgelegt.

HINWEIS: Sie können die von Ihnen in der **Administratorkonsole** konfigurierten Payloads von Systemprofilen bearbeiten. Es ist jedoch nicht möglich, die auf die **Administratorkonsole** hochgeladenen Payloads von Profilen anzuzeigen oder zu bearbeiten.

1. Rufen Sie die Seite *Mac Profil-Detail* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Skripterstellung** und anschließend auf **Mac Profile**.
   c. Führen Sie einen der folgenden Schritte aus:
   - Klicken Sie auf den Namen eines Profils.
   - Klicken Sie auf **Aktion auswählen** > **Neues Systemprofil**.
2. Geben Sie im Bereich *Allgemeine Optionen* die folgenden Informationen ein:

Option	Beschreibung
Profilname	Der in der Liste *Mac Profile* anzuzeigende Name. Dieser Name muss nicht eindeutig sein, sollte aber

Option	Beschreibung
	aussagekräftig genug sein, um das Profil in einer Liste zu erkennen. **HINWEIS:** Sie können den Namen eines Profils jederzeit ändern. Wenn Sie jedoch den Namen eines Profils nach seiner Installation auf einem Gerät ändern möchten, wird der Profilname nicht auf dem Gerät aktualisiert. Das Profil wird weiterhin mit dem Namen identifiziert, den es bei der Installation hatte.
Beschreibung	Zusätzliche Informationen zum Profil, z. B. die Konfigurationseinstellungen oder der Verwendungszweck.
Benutzer kann Profil entfernen	Gibt an, ob die Benutzer das Profil von ihren Geräten entfernen können. Zur Auswahl stehen folgende Optionen: • **Nie**: Die Benutzer können das Profil nicht entfernen. • **Immer**: Die Benutzer können das Profil jederzeit ohne Eingabe eines Kennworts entfernen. • **Mit Kennwort**: Die Benutzer können das Profil entfernen, wenn sie das mit dem Profil verknüpfte Kennwort eingeben.
Profil automatisch entfernen	Gibt an, ob das Profil nach einem angegebenen Zeitraum automatisch entfernt wird. Das ist hilfreich, wenn Sie Geräte konfigurieren, für die nach einem angegebenen Datum andere Profile bereitgestellt werden müssen, z. B. am Ende eines Schulhalbjahrs. Zur Auswahl stehen folgende Optionen: • **Nie**: Das Profil wird nicht nach Zeitplan automatisch entfernt. • **An einem bestimmten Datum**: Das Profil wird am angegebenen Datum automatisch entfernt. Das Datum muss im Format **mm/tt/jjjj** angegeben werden. • **Nach**: Das Profil wird nach dem Ablauf des angegebenen Zeitraums entfernt. Der Zeitraum kann in Tagen oder Stunden angegeben werden.

3. Im Abschnitt *Payloads* können Sie *Gatekeeper*-Konfigurationsinformationen hinzufügen oder bearbeiten.

Option	Beschreibung
Apps-Download zulassen von	Gibt an, ob die Benutzer Apps herunterladen dürfen von: • **Mac App Store**: Die Benutzer können Apps nur vom Mac App Store herunterladen. • **Mac App Store und angegebene Entwickler**: Die Benutzer können Apps vom Mac App Store und von Entwicklern herunterladen, die ihre Apps mit einer eindeutigen Entwickler-ID von Apple digital signiert haben. • **Überall**: Die Benutzer können Apps von überall ohne Einschränkung herunterladen.
Benutzern nicht erlauben, die Gatekeeper-Einstellungen außer Kraft zu setzen	Gibt an, ob die Benutzer die App-Download-Einstellungen ändern dürfen.

4. Fügen Sie Konfigurationsinformation für die *Kennung* hinzu oder bearbeiten Sie diese.

HINWEIS: In diesem Abschnitt ist der Begriff **Kennung** gleichbedeutend mit dem Begriff **Kennwort**.

Option	Beschreibung
Einfachen Wert zulassen	Ermöglicht den Benutzern die Auswahl von Kennungen mit sich wiederholenden, aufsteigenden und absteigenden Zeichenfolgen.
Alphanumerischer Wert erforderlich	Die Benutzer müssen Kennungen wählen, die mindestens einen Buchstaben und eine Ziffer enthalten.
Mindestlänge der Kennung	Die kleinste Anzahl von Zeichen, die in Kennungen zulässig ist.
Mindestanzahl komplexer Zeichen	Die kleinste Anzahl nicht-alphanumerischer Zeichen, z. B. "*" oder "!", die in Kennungen zulässig ist.
Maximale Anzahl fehlgeschlagener Versuche	Die Anzahl der Eingaben falscher Kennungen, die Benutzer zum Entsperren von Geräten vornehmen können, bevor ihre Konten gesperrt werden.
Maximale Toleranzperiode für Gerätesperre	Wenn in den Systemeinstellungen angegeben ist, dass Geräte nach einem bestimmten Inaktivitätszeitraum gesperrt werden sollen, ermöglicht diese Einstellung ein Zeitfenster, in dem Benutzer ihre Geräte ohne Eingabe ihres Kennworts entsperren können. Wenn die Toleranzperiode abgelaufen ist, müssen Benutzer zum Entsperren von Geräten ihr Kennwort eingeben.
Maximales Kennungsalter in Tagen	Die Anzahl der Tage, nach denen Kennungen geändert werden müssen.

Option	Beschreibung
Kennungsverlauf	Die Anzahl der Kennungen, die eindeutig sein müssen, bevor eine Kennung erneut verwendet werden kann.
Verzögerung nach fehlgeschlagenen Anmeldeversuchen in Minuten	Die Anzahl der Minuten, die vergehen müssen, bevor Benutzer wieder Anmeldeversuche unternehmen können, nachdem die maximale Anzahl von fehlgeschlagenen Anmeldeversuchen erreicht worden ist.

5. Wählen Sie im Abschnitt *Bereitstellen* die Zielgeräte für das Profil:

Option	Beschreibung
Alle Geräte	Das Profil wird an alle KACE Geräte mit Agentenverwaltung mit einer unterstützten Version von Mac OS X (Version 10.8, 10.9 oder 10.10) verteilt. Wenn auf Ihrer Appliance die Organisationskomponente aktiviert ist, werden alle unterstützten Mac Geräte der ausgewählten Organisation einbezogen.
Labels	Das Profil wird nur an die Geräte verteilt, die das von Ihnen ausgewählte Label aufweisen. Durch Begrenzen der Verteilung auf Labels, insbesondere auf Smart Labels, wird sichergestellt, dass Profile richtig angewendet werden. Um diese Option verwenden zu können, müssen Sie bereits Labels oder Smart Labels erstellt haben. Siehe Smart Labels für Geräte hinzufügen.
Geräte	Das Profil wird an die von Ihnen ausgewählten unterstützten Mac OS X Geräte (Version 10.8, 10.9 oder 10.10) verteilt. Um nach Geräten zu suchen, beginnen Sie mit einer entsprechenden Eingabe in das Feld.
Betriebssysteme	Das Betriebssystem, auf dem die Anwendung ausgeführt wird. Die Bereitstellung der Anwendungen erfolgt nur auf Geräten mit den ausgewählten Betriebssystemen. a. Klicken Sie auf **Betriebssysteme verwalten**. b. Wählen Sie im daraufhin angezeigten Dialogfeld **Betriebssysteme** die Betriebssystemversionen in der Navigationsstruktur aus. Sie haben die Möglichkeit, Betriebssystemversionen nach Familie, Produkt, Architektur oder Build-Version auszuwählen. Je nach Bedarf können Sie eine bestimmte Build-Version oder einen übergeordneten Knoten auswählen. Wenn Sie einen übergeordneten Knoten im Baum auswählen, werden die zugehörigen untergeordneten Knoten automatisch mit ausgewählt. Aufgrund dieses

Option	Beschreibung
	Verhaltens können Sie beliebige zukünftige Betriebssystemversionen auswählen, da Geräte in Ihrer verwalteten Umgebung hinzugefügt oder aktualisiert werden. Wenn Sie beispielsweise alle aktuellen und zukünftigen Versionen auswählen möchten, die mit einem Mac 10.11 El Capitan x86-Architektur verbunden sind, wählen Sie unter **Mac > 10.11 El Capitan** die Option **x86** aus.
Alle entfernen	Alle Geräte von der Liste *Geräte* in diesem Abschnitt entfernen.

6. Wählen Sie im Abschnitt *Planen* die Optionen für die Verteilung des Profils an die Zielgeräte aus:

Option	Beschreibung
Kein(e)	Keine Verteilung des Profils per Zeitplan. Profile, deren Zeitpläne auf **Kein(e)** eingestellt sind, haben auf der Liste *Mac Profile* den Status **Deaktiviert**. Profile, deren Zeitpläne auf **Kein(e)** eingestellt sind, können jedoch trotzdem bereitgestellt werden, wenn Sie unten auf der Seite **Jetzt ausführen** auswählen.
Alle n Minuten/Stunden	Der Vorgang wird im angegebenen Intervall durchgeführt.
Täglich/an einem bestimmten Tag um HH:MM	Die Erfassung wird täglich zu einem bestimmten Zeitpunkt oder an einem bestimmten Wochentag um eine bestimmte Uhrzeit ausgeführt.
Ausführen am n-ten jedes Monats/eines bestimmten Monats um HH:MM	Die Erfassung wird jeden Monat oder in einem bestimmten Monat an einem festgelegten Datum zu einer festgelegten Uhrzeit ausgeführt.

Benutzerdefiniert	Ausführung nach einem benutzerdefinierten Zeitplan.
	Verwenden Sie das Standard-5-Feld-Cron-Format (das erweiterte Cron-Format wird nicht unterstützt):
	`* * * * *`
	`| | | | +————Wochentag (0-6) (Sonntag=0)`
	`| | | +————Monat (1-12)`
	`| | +————Monatstag (1-31)`
	`| +————Stunde (0-23)`
	`+————Minute (0-59)`
	Verwenden Sie bei der Angabe von Werten die folgenden Zeichen:
	• **Leerzeichen( )**: Die einzelnen Felder mit einem Leerzeichen trennen.
	• **Sternchen (*)**: Ein Sternchen repräsentiert den gesamten Wertebereich in einem Feld.

Option	Beschreibung
	Zum Beispiel repräsentiert ein Sternchen im Stundenfeld eine beliebige Stunde. • **Kommas (,)**: Mehrere Werte in einem Feld werden mit einem Komma getrennt. Zum Beispiel werden mit `0,6` im Feld „Wochentag“ Sonntag und Samstag angegeben. • **Bindestriche (-)**: Mit einem Bindestrich wird ein Wertebereich in einem Feld angegeben. Zum Beispiel entspricht `1-5` im Feld „Wochentag“ `1,2,3,4,5`, d. h. Montag bis Freitag. • **Schrägstriche (/)**: Die Angabe der Zeitabstände, mit denen eine Aktion wiederholt werden soll, erfolgt mit einem Schrägstrich. Zum Beispiel entspricht `*/3` im Feld Stunde `0,3,6,9,12,15,18,21`. Das Sternchen (`*`) gibt jede Stunde an, mit `/3` erfolgt aber eine Einschränkung auf durch drei teilbare Stunden. Beispiele: • `15 * * * * Jeden Tag 15 Minuten nach jeder vollen Stunde ausführen` • `0 22 * * * Jeden Tag um 22:00 Uhr ausführen` • `0 0 1 1,6 * Am 1. Januar und 1. Juni um 00:00 Uhr ausführen` • `30 8,12 * * 1-5 An Wochentagen um 08:30 Uhr und 12:30 Uhr ausführen` • `0 2 */2 * * Jeden zweiten Tag um 02:00 Uhr ausführen`

7. Wählen Sie unten auf der Seite eine der folgenden Aktionen aus:

Option	Beschreibung
Speichern	Das Profil speichern und zur Liste *Mac Profile* zurückkehren.
Jetzt ausführen	Auf Zielgeräten mit einer aktiven Agentenverbindung mit der Appliance das Profil jetzt gemäß den ausgewählten Bereitstellungsoptionen installieren. Siehe Verwenden der Befehle "Ausführen" und "Jetzt ausführen".
Duplizieren	Eine Kopie des Profils erstellen, wobei dem Profilnamen `Kopie von` vorangestellt wird. Diese Option ist nicht für neue Profile verfügbar, die noch nicht gespeichert wurden. Siehe Mac Profile zu vorhandenen Profilen als Vorlage hinzufügen.
Entfernen	Erstellen eines Profils, das für die Entfernung des Profils von Zielgeräten verwendet werden kann.

Option	Beschreibung
	Diese Option ist nicht für neue Profile verfügbar, die noch nicht gespeichert wurden. Siehe Mac Profile von verwalteten Geräten entfernen.
Löschen	Entfernen des Profils von der Appliance. Dadurch wird das Profil nicht von Geräten entfernt, auf denen es installiert ist. Diese Option ist nicht für neue Profile verfügbar, die noch nicht gespeichert wurden. Siehe Mac Profile aus der Appliance löschen.
Abbrechen	Änderungen verwerfen und zur Liste *Mac Profile* zurückkehren.

Mac Profile zu vorhandenen Profilen als Vorlage hinzufügen

Sie können Mac Profile durch Duplizieren vorhandener Profile hinzufügen. Das ist praktisch, wenn Sie ein vorhandenes Profil auf unterschiedlichen Geräten installieren oder Profil-Installationen zu verschiedenen Zeitpunkten vornehmen möchten. Sie können Profile duplizieren und die Zielgeräte oder Zeitpläne nach Bedarf ändern.

Sie haben einen Benutzer oder ein Systemprofil zur Appliance hinzugefügt.

Importierte Profile können nicht dupliziert werden.

1. Rufen Sie die Seite *Mac Profile* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Skripterstellung** und anschließend auf **Mac Profile**.
2. Klicken Sie auf den Namen eines Profils, um die Seite *Mac Profil-Detail* anzuzeigen.
3. Klicken Sie unten auf der Seite auf **Duplizieren**.

   Das Profil wird dupliziert und in der Liste der *Mac Profile* mit dem Zusatz `Kopie von` vor dem Profilnamen angezeigt. Duplizierte Profile haben die gleichen Eigenschaften und Identifikationsnummern wie die ursprünglichen Profile, aber ihre Zeitpläne werden automatisch auf **Kein(e)** gesetzt, um das Ausführen doppelter Aktionen auf den gleichen Geräten zu verhindern.

Mac Profile in die Appliance hochladen

Sie können `MOBILECONFIG`-Dateien in die Appliance hochladen, die Konfigurationseinstellungen zum Erstellen von Mac Profilen enthalten.

Sie haben eine Datei erhalten, die die Konfigurationseinstellungen oder Payloads enthält, die Sie für das Profil benötigen. Diese Datei verwendet die Dateierweiterung `MOBILECONFIG`. Beispiel: `mail.mobileconfig`. Weitere Informationen über das Erstellen und Herunterladen von Mac Profilen vom Mac OS X Server finden Sie unter http://help.apple.com/profilemanager/mac/4.0.

HINWEIS: Es ist nicht möglich, die auf die **Administratorkonsole** hochgeladenen Payloads von Profilen anzuzeigen oder zu bearbeiten. Sie können jedoch die Payloads in der Datei `MOBILECONFIG` außerhalb der **Administratorkonsole** ändern und dann die bearbeitete Datei als neues Profil hochladen.

1. Rufen Sie die Listenseite *Mac Profile* auf:

a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.

b. Klicken Sie in der linken Navigationsleiste auf **Skripterstellung** und anschließend auf **Mac Profile**.

2. Klicken Sie auf **Aktion auswählen** > **Ein Profil hochladen**.
3. Klicken Sie auf **Durchsuchen** oder auf **Datei auswählen** und suchen Sie nach der `MOBILECONFIG`-Datei.
4. Klicken Sie auf **Hochladen**.

   Das Profil wird in der Liste *Mac Profile* mit *Importiert* in der Spalte *Quelle* angezeigt.

Wählen Sie die Bereitstellungs- und Zeitplanoptionen für das Profil aus. Siehe:

- Mac Benutzerprofile hinzufügen oder bearbeiten
- Mac Systemprofile hinzufügen oder bearbeiten

Installieren und Verwalten von Mac Profilen

Sie können Mac Profile installieren, die Geräte anzeigen, die Mac Profile installiert haben und die Liste der Profile exportieren, die der Appliance hinzugefügt wurden.

Mac Profile per Zeitplan verteilen

Sie können die Appliance verwenden, um Mac Profile an vom Agenten verwaltete Geräte mit Mac OS X nach einem Zeitplan zu verteilen. Diese Konfiguration ist nützlich, wenn es beim Auswählen der Option *Ausführen* Geräte gibt, die offline und für die Installation nicht verfügbar sind, und wenn Sie regelmäßig Profile auf neuen Geräten installieren, die zum Inventar hinzugefügt werden sollen.

Sie haben ein Mac Profil hinzugefügt oder hochgeladen und verfügen über Mac OS X Geräte mit Agentenverwaltung in Ihrem Inventar.

1. Rufen Sie die Seite *Mac Profil-Detail* auf:

   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.

   b. Klicken Sie in der linken Navigationsleiste auf **Skripterstellung** und anschließend auf **Mac Profile**.

   c. Klicken Sie auf den Namen eines Profils.

2. Wählen Sie im Abschnitt *Planen* die Optionen für die Verteilung des Profils an die Zielgeräte aus:

Option	Beschreibung
Kein(e)	Keine Verteilung des Profils per Zeitplan. Profile, deren Zeitpläne auf **Kein(e)** eingestellt sind, haben auf der Liste *Mac Profile* den Status **Deaktiviert**. Profile, deren Zeitpläne auf **Kein(e)** eingestellt sind, können jedoch trotzdem bereitgestellt werden, wenn Sie unten auf der Seite **Jetzt ausführen** auswählen.
Alle n Minuten/Stunden	Der Vorgang wird im angegebenen Intervall durchgeführt.

Option	Beschreibung
Täglich/an einem bestimmten Tag um HH:MM	Die Erfassung wird täglich zu einem bestimmten Zeitpunkt oder an einem bestimmten Wochentag um eine bestimmte Uhrzeit ausgeführt.
Ausführen am n-ten jedes Monats/eines bestimmten Monats um HH:MM	Die Erfassung wird jeden Monat oder in einem bestimmten Monat an einem festgelegten Datum zu einer festgelegten Uhrzeit ausgeführt.

Benutzerdefiniert	Ausführung nach einem benutzerdefinierten Zeitplan.
	Verwenden Sie das Standard-5-Feld-Cron-Format (das erweiterte Cron-Format wird nicht unterstützt):
	`* * * * *`
	`| | | | +————————Wochentag (0-6) (Sonntag=0)`
	`| | | +————————Monat (1-12)`
	`| | +————————Monatstag (1-31)`
	`| +————————Stunde (0-23)`
	`+————————Minute (0-59)`
	Verwenden Sie bei der Angabe von Werten die folgenden Zeichen:
	• **Leerzeichen( )**: Die einzelnen Felder mit einem Leerzeichen trennen.
	• **Sternchen (*)**: Ein Sternchen repräsentiert den gesamten Wertebereich in einem Feld. Zum Beispiel repräsentiert ein Sternchen im Stundenfeld eine beliebige Stunde.
	• **Kommas (,)**: Mehrere Werte in einem Feld werden mit einem Komma getrennt. Zum Beispiel werden mit `0,6` im Feld „Wochentag“ Sonntag und Samstag angegeben.
	• **Bindestriche (-)**: Mit einem Bindestrich wird ein Wertebereich in einem Feld angegeben. Zum Beispiel entspricht `1-5` im Feld „Wochentag“ `1,2,3,4,5`, d. h. Montag bis Freitag.
	• **Schrägstriche (/)**: Die Angabe der Zeitabstände, mit denen eine Aktion wiederholt werden soll, erfolgt mit einem Schrägstrich. Zum Beispiel entspricht `*/3` im Feld Stunde `0,3,6,9,12,15,18,21`. Das Sternchen (`*`) gibt jede Stunde an, mit `/3` erfolgt aber eine Einschränkung auf durch drei teilbare Stunden.

Option	Beschreibung
	Beispiele: • `15 * * * *` Jeden Tag 15 Minuten nach jeder vollen Stunde ausführen • `0 22 * * *` Jeden Tag um 22:00 Uhr ausführen • `0 0 1 1,6 *` Am 1. Januar und 1. Juni um 00:00 Uhr ausführen • `30 8,12 * * 1-5` An Wochentagen um 08:30 Uhr und 12:30 Uhr ausführen • `0 2 */2 * *` Jeden zweiten Tag um 02:00 Uhr ausführen

3. Klicken Sie auf **Speichern**.

   Die Seite *Mac Profile* wird angezeigt. Die Spalte *Ziel* zeigt die Anzahl der Geräte, auf denen das Profil per Zeitplan installiert werden soll. Die Spalte *Erfolgreich* zeigt die Anzahl der Geräte, auf denen das Profil installiert wurde. Agenten auf Zielgeräten erhalten Anweisungen, das Profil bei der nächsten Verbindungen gemäß dem Zeitplan und den angegebenen Bereitstellungsoptionen zu installieren.

Mac Profile auf Geräten mit der Option "Ausführen" installieren

Nach dem Hinzufügen oder Hochladen von Mac Profilen auf die Appliance können Sie mit der Option *Ausführen* diese Profile an vom Agenten verwaltete Geräte mit Mac OS X 10.8, 10.9 oder 10.10 verteilen.

Sie haben ein Mac Profil hinzugefügt und verfügen über Mac OS X Geräte mit Agentenverwaltung in Ihrem Inventar.

> **TIPP:** Wenn Sie die Option *Ausführen* zum Installieren von Mac Profilen auf Geräten verwenden, werden nur dann Profile installiert, wenn während der Skriptausführung eine Verbindung zwischen Agent und Appliance besteht. Damit Profile auch sicher auf Offline-Geräten installiert werden, richten Sie am besten Zeitpläne für die Profilbereitstellung ein. Siehe Mac Profile per Zeitplan verteilen.

1. Rufen Sie die Seite *Mac Profil-Detail* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Skripterstellung** und anschließend auf **Mac Profile**.
   c. Klicken Sie auf den Namen eines Profils.
2. Zum Installieren des Profils auf einer anderen Gerätegruppe, klicken Sie unten auf der Seite auf **Duplizieren** und klicken dann auf den Namen des duplizierten Profils, um zur Seite *Mac Profil-Detail* zurückzukehren.
3. Wählen Sie auf der Seite *Mac Profil-Detail* die Zielgeräte und die Bereitstellungsoptionen aus. Siehe:
   - Mac Benutzerprofile hinzufügen oder bearbeiten
   - Mac Systemprofile hinzufügen oder bearbeiten
4. Klicken Sie unten auf der Seite auf **Jetzt ausführen**.

   Die Seite *Mac Profile* wird angezeigt. Die Spalte *Ziel* zeigt die Anzahl der Geräte, auf denen das Profil per Zeitplan installiert werden soll. Die Spalte *Erfolgreich* zeigt die Anzahl der Geräte, auf denen das Profil

installiert wurde. Auf Zielgeräten mit einer aktiven Agentenverbindung mit der Appliance ist das Profil jetzt gemäß den ausgewählten Bereitstellungsoptionen installiert.

5. Zum gleichzeitigen Ausführen mehrerer Profile aktivieren Sie die Kontrollkästchen neben den Profilen auf der Seite *Mac Profile* und klicken dann auf **Aktion auswählen** > **Ausführen**.
6. Zum Anzeigen weiterer Einzelheiten über die Profilinstallation klicken Sie in der linken Navigationsleiste auf **'Jetzt ausführen'-Status**.

Geräte mit installierten Mac Profilen identifizieren

Die Seiten "Gerätedetail" zeigen die Mac Profile, die auf Geräten installiert wurden. Die Seiten "Mac Profil-Detail" zeigen Geräte mit installierten Mac Profilen.

1. Rufen Sie die Seite *Mac Profil-Detail* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Skripterstellung** und anschließend auf **Mac Profile**.
   c. Klicken Sie auf den Namen eines Profils.
2. Scrollen Sie auf dieser Seite nach unten zum Abschnitt *Ergebnisse*.

   Die Tabelle enthält die Namen der Geräte, auf denen das Profil installiert ist. Die Spalte *Installiert* zeigt das Datum, wann das Profil auf dem Gerät installiert wurde. Die Spalte *Letzte Aktualisierung* zeigt den letzten Zeitpunkt, zu dem der KACE Agent erkannt hat, dass das Profil auf dem Gerät installiert wurde.
3. Rufen Sie die *Gerätedetailseite* auf:
   a. Klicken Sie in der linken Navigationsleiste auf **Inventar** und anschließend auf **Dashboard**.
   b. Klicken Sie auf den Namen eines Geräts.
4. Scrollen Sie nach unten zum Abschnitt *Mac Profile*.

   Die Tabelle listet alle Profile auf, die auf dem Gerät installiert sind. Die Spalte *Installiert* zeigt das Datum, wann das Profil auf dem Gerät installiert wurde. Die Spalte *Letzte Aktualisierung* zeigt den letzten Zeitpunkt, zu dem der KACE Agent erkannt hat, dass das Profil auf dem Gerät installiert wurde.

Mac Profile anzeigen

Mit der Liste *Anzeigen nach* können Sie Mac Profile nach Quelle, Aktion und Bereich sortieren.

Sie haben Mac Profile in der Appliance hinzugefügt oder hochgeladen.

1. Rufen Sie die Liste *Mac Profile* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Skripterstellung** und anschließend auf **Mac Profile**.
2. Wählen Sie rechts über der Tabelle aus der Dropdown-Liste *Anzeigen nach* eine der folgenden Optionen aus:

Option	Beschreibung
Alle Elemente	Zeigt die vollständige Liste der Profile an.

Option	Beschreibung
Quelle	Zeigt nur die Profile an, die mit der ausgewählten Quelle übereinstimmen: • **Importiert**: Profile, die auf die Appliance hochgeladen wurden. • **Konfiguriert**: Profile mit Payloads, die mit der **Administratorkonsole** konfiguriert wurden.
Aktion	Zeigt nur die Profile an, die mit der ausgewählten Aktion übereinstimmen: • **Hinzufügen**: Profile, die für die Installation von Konfigurationseinstellungen auf den Zielgeräten konfiguriert sind. • **Entfernen**: Profile, die für die Entfernung von Konfigurationseinstellungen auf den Zielgeräten konfiguriert sind.
Bereich	Zeigt nur die Profile an, die mit dem ausgewählten Bereich übereinstimmen: • **System**: Profile, die Systemeinstellungen wie die Kennworteinstellungen konfigurieren. • **Benutzer**: Profile, die Benutzereinstellungen wie die Einstellungen des E-Mail-Kontos konfigurieren.
Status	Zeigt nur die Profile an, die mit dem ausgewählten Status übereinstimmen: • **Aktiv**: Profile, die für das Ausführen eines Zeitplans konfiguriert sind. • **Deaktiviert**: Profile, deren Zeitpläne auf **Kein(e)** gesetzt sind.

Mac Profil-Listen exportieren

Sie können die Profile auf der Liste *Mac Profile* in den Formaten CSV (Comma Separated Value – kommagetrennte Werte), Excel oder TSV (Tab-Separated Values – tabgetrennte Werte) exportieren.

Sie haben Mac Profile erstellt oder hochgeladen.

1. Rufen Sie die Liste *Mac Profile* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.

b. Klicken Sie in der linken Navigationsleiste auf **Skripterstellung** und anschließend auf **Mac Profile**.

2. **Optional**: Zum Exportieren der ausgewählten Profile aktivieren Sie die Kontrollkästchen neben den Profilen, die Sie exportieren möchten.
3. Führen Sie einen der folgenden Schritte aus:
   - **Zum Exportieren aller Profile klicken Sie auf Aktion auswählen > Exportieren > Alle in Formatname exportieren.**
   - **Sollen nur die ausgewählten Profile exportiert werden, klicken Sie auf Aktion auswählen > Export in Formatname ausgewählt.**

Entfernen und Löschen von Mac Profilen

Sie können mithilfe der Appliance Mac Profile von verwalteten Geräten entfernen. Diese entfernten Profile können Sie dann von der Appliance löschen.

Mac Profile von verwalteten Geräten entfernen

Mac Profile können so konfiguriert werden, dass Benutzer- und Systemprofile von vom Agenten verwalteten Mac OS X Geräten entfernt werden. Diese Konfiguration ist nützlich, wenn ein Profil auf vielen Geräten installiert wurde und Sie dieses Profil von all diesen Geräten – oder von einer Untergruppe dieser Geräte – löschen müssen.

Sie haben die Appliance verwendet, um ein Profil auf verwalteten Geräten zu installieren, und das ursprüngliche Mac Profil wurde nicht von der Appliance gelöscht.

WICHTIG: Wenn Sie ein Profil von der Appliance löschen, können Sie die Appliance nicht mehr zum Entfernen dieses Profils von verwalteten Geräten verwenden.

1. Rufen Sie die Seite *Mac Profil-Detail* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Skripterstellung** und anschließend auf **Mac Profile**.
   c. Klicken Sie auf den Namen eines Profils.
2. Klicken Sie unten auf der Seite auf **Entfernen**.

   Ein Dialogfeld wird angezeigt, das den Entfernen-Prozess erklärt.
3. Klicken Sie auf **Vom Gerät entfernen**.

   Die Seite *Mac Profil-Detail* wird für ein neues Profil angezeigt, die *Aktion* ist auf *Entfernen* gesetzt. Das neue Profil hat denselben *Profilnamen* und *Profilbezeichner* wie das ursprüngliche Profil. Das ursprüngliche Profil, bei dem die *Aktion* auf *Hinzufügen* gesetzt ist, verbleibt in der Liste mit seinem *Zeitplan*, der auf *Kein(e)* gesetzt ist. Dies verhindert, dass das identische Profil auf der gleichen Gerätegruppe gelöscht bzw. installiert wird. Auch können Sie so das ursprüngliche Profil später bei Bedarf erneut aktivieren.
4. Wählen Sie auf der Seite *Mac Profil-Detail* im Abschnitt *Bereitstellen* die Geräte aus, bei denen Sie das Profil löschen wollen:

Option	Beschreibung
Alle Geräte	Entfernen Sie alle Profile von allen KACE Geräten mit Agentenverwaltung mit einer unterstützten Version von Mac OS X (Version 10.8, 10.9 oder 10.10). Wenn auf Ihrer Appliance die

Option	Beschreibung
	Organisationskomponente aktiviert ist, werden alle Mac Geräte der ausgewählten Organisation einbezogen.
Labels	Entfernen Sie die Profile von den Geräten in den Labels, die Sie ausgewählt haben. Durch Begrenzen des Entfernens auf Labels, insbesondere auf Smart Labels, wird sichergestellt, dass die Profile richtig entfernt werden. Um diese Option verwenden zu können, müssen Sie bereits Labels oder Smart Labels erstellt haben. Siehe Smart Labels für Geräte hinzufügen.
Geräte	Entfernen Sie das Profil von den von Ihnen ausgewählten unterstützten Mac OS X Geräten (Version 10.8, 10.9 oder 10.10). Um nach Geräten zu suchen, beginnen Sie mit einer entsprechenden Eingabe in das Feld.
Betriebssysteme	Wählen Sie die Betriebssysteme der Geräte aus, von denen Sie das Profil löschen möchten. Es werden nur unterstützte Betriebssysteme angezeigt (Mac OS X Version 10.8, 10.9 oder 10.10). Wenn das Profil von allen unterstützten Mac Betriebssystemen entfernt werden soll, wählen Sie kein Betriebssystem aus.
Alle entfernen	Alle ausgewählten Geräte aus der Liste *Geräte* in diesem Abschnitt entfernen.

5. Im Abschnitt *Planen* wählen Sie die Optionen zum Entfernen der Profile von den Zielgeräten aus:

Option	Beschreibung
Kein(e)	Entfernen Sie nicht das Profil in einem Zeitplan. Profile, deren Zeitpläne auf **Kein(e)** eingestellt sind, haben auf der Liste *Mac Profile* den Status **Deaktiviert**. Profile, deren Zeitpläne auf Kein(e) eingestellt sind, können jedoch trotzdem entfernt werden, wenn Sie unten auf der Seite **Jetzt ausführen** auswählen.
Alle n Minuten/Stunden	Der Vorgang wird im angegebenen Intervall durchgeführt.
Täglich/an einem bestimmten Tag um HH:MM	Die Erfassung wird täglich zu einem bestimmten Zeitpunkt oder an einem bestimmten Wochentag um eine bestimmte Uhrzeit ausgeführt.
Ausführen am n-ten jedes Monats/eines bestimmten Monats um HH:MM	Die Erfassung wird jeden Monat oder in einem bestimmten Monat an einem festgelegten Datum zu einer festgelegten Uhrzeit ausgeführt.
Benutzerdefiniert	Ausführung nach einem benutzerdefinierten Zeitplan.

Option	Beschreibung

	Verwenden Sie das Standard-5-Feld-Cron-Format (das erweiterte Cron-Format wird nicht unterstützt):
	`* * * * *`
	`| | | | +————————Wochentag (0-6) (Sonntag=0)`
	`| | | +————————Monat (1-12)`
	`| | +————————Monatstag (1-31)`
	`| +————————Stunde (0-23)`
	`+————————Minute (0-59)`
	Verwenden Sie bei der Angabe von Werten die folgenden Zeichen:
	• **Leerzeichen( )**: Die einzelnen Felder mit einem Leerzeichen trennen.
	• **Sternchen (*)**: Ein Sternchen repräsentiert den gesamten Wertebereich in einem Feld. Zum Beispiel repräsentiert ein Sternchen im Stundenfeld eine beliebige Stunde.
	• **Kommas (,)**: Mehrere Werte in einem Feld werden mit einem Komma getrennt. Zum Beispiel werden mit `0,6` im Feld „Wochentag“ Sonntag und Samstag angegeben.
	• **Bindestriche (-)**: Mit einem Bindestrich wird ein Wertebereich in einem Feld angegeben. Zum Beispiel entspricht `1-5` im Feld „Wochentag“ `1,2,3,4,5`, d. h. Montag bis Freitag.
	• **Schrägstriche (/)**: Die Angabe der Zeitabstände, mit denen eine Aktion wiederholt werden soll, erfolgt mit einem Schrägstrich. Zum Beispiel entspricht `*/3` im Feld Stunde `0,3,6,9,12,15,18,21`. Das Sternchen (`*`) gibt jede Stunde an, mit `/3` erfolgt aber eine Einschränkung auf durch drei teilbare Stunden.
	Beispiele:
	• `15 * * * *` Jeden Tag 15 Minuten nach jeder vollen Stunde ausführen
	• `0 22 * * *` Jeden Tag um 22:00 Uhr ausführen
	• `0 0 1 1,6 *` Am 1. Januar und 1. Juni um 00:00 Uhr ausführen
	• `30 8,12 * * 1-5` An Wochentagen um 08:30 Uhr und 12:30 Uhr ausführen
	• `0 2 */2 * *` Jeden zweiten Tag um 02:00 Uhr ausführen

6. Wählen Sie unten auf der Seite eine der folgenden Aktionen aus:

Option	Beschreibung
Speichern	Das Profil speichern und zur Liste *Mac Profile* zurückkehren.
Jetzt ausführen	Auf Zielgeräten mit einer aktiven Agentenverbindung mit der Appliance das Profil jetzt gemäß den ausgewählten Bereitstellungsoptionen entfernen. Siehe Verwenden der Befehle "Ausführen" und "Jetzt ausführen".
Duplizieren	Eine Kopie des Profils erstellen, wobei dem Profilnamen `Kopie von` vorangestellt wird.
Löschen	Entfernen des Profils von der Appliance. Dadurch wird das Profil nicht von Geräten entfernt, auf denen es installiert ist. Siehe Mac Profile aus der Appliance löschen.
Abbrechen	Änderungen verwerfen und zur Liste *Mac Profile* zurückkehren.

Die Seite *Mac Profile* wird angezeigt. Die Spalte *Ziel* zeigt die Anzahl der Geräte, von denen das Profil per Zeitplan entfernt werden soll. Die Spalte *Erfolgreich* zeigt die Anzahl der Geräte, von denen das Profil entfernt wurde. Von Zielgeräten mit einer aktiven Agentenverbindung mit der Appliance ist das Profil jetzt gemäß den ausgewählten Optionen entfernt worden.

Beispiel: Profil entfernen, das für bestimmte Geräte bereitgestellt wurde

Wenn Sie versehentlich Profile für Zielgeräte bereitgestellt haben, können Sie diese durch Erstellen eines *Entfernen*-Profils löschen.

1. Sie haben ein Mac System-Profil mit diesen Zeitplan- und Bereitstellungsoptionen erstellt:
   - Geplante Installation täglich um 8:00 Uhr
   - Vorhandene oder geplante Installation auf 100 Zielgeräten
2. Nach der Profilerstellung fällt Ihnen ein, dass das Profil auf 10 der 100 Zielgeräte nicht installiert werden soll. Sie müssen das Profil von den 10 Geräten entfernen, aber für die anderen 90 Geräte beibehalten.

   HINWEIS: In diesem Beispiel wird ein Mac Systemprofil verwendet. Sie können aber bei Bedarf beides entfernen: Mac System- und Mac Benutzerprofile.

1. Rufen Sie die Seite *Mac Profil-Detail* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Skripterstellung** und anschließend auf **Mac Profile**.
   c. Klicken Sie auf den Namen des Profils. In diesem Beispiel nennen wir dieses Profil **Profil A**.
2. Klicken Sie auf der Seite *Mac Profil-Detail* bei **Profil A** auf **Entfernen**.

   Ein Dialogfeld wird angezeigt, das den **Entfernen**-Prozess erklärt.
3. Klicken Sie auf **Vom Gerät entfernen**.

Die Seite *Mac Profil-Detail* wird für ein neues Profil angezeigt, die *Aktion* ist auf *Entfernen* gesetzt. Das neue Profil hat denselben *Profilnamen* und *Profilbezeichner* wie das ursprüngliche Profil. In diesem Beispiel ist dies **Profil A entfernen**. Das ursprüngliche Profil, bei dem die *Aktion* auf *Hinzufügen* gesetzt ist, verbleibt in der Liste mit seinem *Zeitplan*, der auf *Kein(e)* gesetzt ist. Dies verhindert, dass das identische Profil auf der gleichen Gerätegruppe gelöscht bzw. installiert wird. Auch können Sie so das **Profil A** später bei Bedarf erneut aktivieren.

4. Wählen Sie auf der Seite *Mac Profil-Detail* für **Profil A entfernen** im Abschnitt *Bereitstellen* die Geräte aus, bei denen Sie das Profil löschen wollen.
5. Führen Sie einen der folgenden Schritte aus:
   - Soll das Profil nach Zeitplan ausgeführt werden, klicken Sie unten auf der Seite auf **Speichern**.
   - Soll das Profil auf Geräten ausgeführt werden, die derzeit über eine Verbindung zur Appliance verfügen, klicken Sie auf **Jetzt ausführen**.

   Die Seite *Mac Profile* zeigt für den Profilbezeichner **Profil A entfernen** die Anzahl der Zielgeräte in der Spalte *Ziel* und die Anzahl der Geräte, von denen das Profil entfernt wurde, in der Spalte *Erfolgreich*.
6. Wenn die Spalte *Erfolgreich* zeigt, dass das Profil von allen Zielgeräten entfernt wurde, brauchen Sie den Profilbezeichner **Profil A entfernen** nicht mehr und können ihn von der Appliance löschen. Siehe Mac Profile aus der Appliance löschen.
7. Überprüfen Sie für **Profil A**, dass die richtigen Geräte als Ziel ausgewählt sind und aktivieren Sie das Profil:
   a. Rufen Sie die Seite *Mac Profil-Detail* für **Profil A** auf.
   b. Ändern Sie die Liste der Zielgeräte so, dass nur die richtigen 90 Geräte enthalten sind.
   c. Aktivieren Sie das Profil. Siehe:
   - Mac Benutzerprofile hinzufügen oder bearbeiten
   - Mac Systemprofile hinzufügen oder bearbeiten

Mac Profile aus der Appliance löschen

Sie können bei Bedarf Mac Profile von der Appliance löschen.

Durch Löschen eines Profils wird dieses nicht von Geräten entfernt, auf denen Sie es bereitgestellt haben. Zum Löschen von Profilen von Geräten verwenden Sie die Option **Entfernen**. Siehe Mac Profile von verwalteten Geräten entfernen.

HINWEIS: Wenn Sie ein Profil von der Appliance löschen, können Sie die Appliance nicht mehr zum Entfernen dieses Profils von verwalteten Geräten verwenden.

1. Rufen Sie die Seite *Mac Profil-Detail* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Skripterstellung** und anschließend auf **Mac Profile**.
   c. Klicken Sie auf den Namen eines Profils.
2. Klicken Sie unten auf der Seite auf **Löschen**.

   Ein Dialogfeld wird angezeigt.
3. Überprüfen Sie, ob Sie das Profil von der Appliance löschen wollen und klicken Sie dann auf **Profil löschen**.

   Das Profil wird von der Appliance entfernt und nicht mehr in der Liste *Mac Profile* angezeigt. Der Profilbezeichner wird jedoch weiterhin auf der Seite *Gerätedetail* für die Geräte angezeigt, auf denen das Profil installiert ist.

Verwenden von Aufgabenabfolgen

Mit Aufgabenabfolgen können Sie eine Abfolge von Aufgaben erstellen, die in einer bestimmten Reihenfolge ausgeführt werden.

Sie können einen oder mehrere Patch-Zeitpläne, verwaltete Installationen, Skripte, Dateisynchronisierungselemente und Wake On LAN-Anfragen zu einer Aufgabenabfolge hinzufügen. Verwenden Sie Aufgabenabfolgen beispielsweise, wenn Sie verwaltete Installationen bereitstellen und Skripte auf Zielgeräten ausführen müssen. Die Reihenfolge der Aufgaben in einer Aufgabenabfolge kann beliebig geändert werden.

Jede Aufgabenabfolge wird auf einem konfigurierten Satz von Geräten ausgeführt, wie in der Aufgabenabfolge definiert.

Wenn ein Zielgerät in einer Aufgabenabfolge offline ist, können Sie die Aufgabenabfolge so konfigurieren, dass sie ausgeführt wird, sobald das Gerät verbunden wird. Wenn ein Zielgerät in mehreren Aufgabenabfolgen referenziert wird, wird nur eine Aufgabenabfolge gleichzeitig mit dem Gerät ausgeführt.

Die folgenden Konzepte gelten für die Geräteauswahl in einer Aufgabenabfolge:

- Geräte, die in einer Aufgabenabfolge ausgewählt sind, setzen diese Sets für Patching-Zeitpläne und Skripte außer Kraft, wenn Sie als Teil einer Aufgabenabfolge ausgeführt werden.
- In einer Aufgabenabfolge ausgewählte Geräte wirken sich nicht auf die mit diesen Geräten verbundenen verwalteten Installationen (MI) oder Dateisynchronisierung (FS) aus. Alle Bestands-, MI- und FS-Aufgaben werden für jedes Gerät in der Aufgabenabfolge in die Warteschlange gestellt, und alle MI und FS, die für jede Maschine konfiguriert sind, werden bereitgestellt.
- Wake on LAN (WoL)-Zeitpläne werden einmal pro Aufgabenabfolge ausgeführt, wenn das erste Gerät in der Aufgabenabfolge die WoL-Aufgabe findet. Die WoL-Aufgabe wird anhand der in der Aufgabenabfolge ausgewählten Geräte ausgeführt.

  HINWEIS: Eine WoL-Aufgabe sollte immer als erste Aufgabe in einer Aufgabenabfolge geplant werden. Dadurch werden WoL-Pakete an alle Geräte gleichzeitig weitergeleitet, und die Geräte warten auf diese Aufgabe, da es sich um die erste Aufgabe handelt. Wenn eine WoL-Aufgabe nicht die erste Aufgabe in der Aufgabenabfolge ist, werden WoL-Pakete an alle Geräte gleichzeitig weitergeleitet, unabhängig vom aktuellen Status der ausgeführten Aufgaben in der Aufgabenabfolge.

Aufgabenabfolgen hinzufügen und bearbeiten

Eine Aufgabenabfolge ist eine Sammlung von Aufgaben, die in einer bestimmten Reihenfolge ausgeführt werden können. Verwenden Sie die Seite *Aufgabenabfolgedetails*, um Aufgabenabfolgen hinzuzufügen und zu bearbeiten.

1. Rufen Sie die Listenseite *Aufgabenabfolge* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Verteilung** und anschließend auf **Aufgabenabfolge**.
2. Führen Sie einen der folgenden Schritte aus:
   - Wählen Sie **Aktion auswählen** > **Neu**.
   - Klicken Sie auf den Namen einer Aufgabenabfolge.
3. Geben Sie im Abschnitt *Konfigurieren* folgende Einstellungen an:

Option	Beschreibung
Name	Der Name der Aufgabenabfolge.
Aktiviert	Aktivieren Sie dieses Kontrollkästchen, um diese Aufgabenabfolge auszuführen.
Beschreibung	Eine kurze Beschreibung der Aufgabenabfolge.

4. Geben Sie im Abschnitt *Konfigurieren* die Geräte an, auf denen die Aufgabenabfolge ausgeführt werden soll.
   - **Um Geräte zu wählen, die zu Labels gehören, klicken Sie im Abschnitt** *Konfigurieren* **unter** *Labels* **auf Verknüpfte Labels verwalten. Wählen Sie in dem nun angezeigten Dialogfeld** *Labels auswählen* **ein oder mehrere Labels aus, die mit den einzuschaltenden Geräten verknüpft sind. Schließen Sie das Dialogfeld.**
   - **Um Geräte über das Betriebssystem zu wählen, klicken Sie auf Verwaltung von Betriebssystemen. Wählen Sie im daraufhin angezeigten Dialogfeld Betriebssysteme die Betriebssystemversionen in der Navigationsstruktur aus.**

     Sie haben die Möglichkeit, Betriebssystemversionen nach Familie, Produkt, Architektur, Versions-ID oder Build-Version auszuwählen. Je nach Bedarf können Sie eine bestimmte Build-Version oder einen übergeordneten Knoten auswählen. Wenn Sie einen übergeordneten Knoten im Baum auswählen, werden die zugehörigen untergeordneten Knoten automatisch mit ausgewählt. Aufgrund dieses Verhaltens können Sie beliebige zukünftige Betriebssystemversionen auswählen, da Geräte in Ihrer verwalteten Umgebung hinzugefügt oder aktualisiert werden. Wenn Sie beispielsweise alle aktuellen und zukünftigen Versionen auswählen möchten, die mit der Windows 10 x64-Architektur verbunden sind, wählen Sie unter **Alle** > **Windows** > **Windows 10** die Option **x64** aus.
5. Geben Sie im Abschnitt *Zeitplan* folgende Zeitplanungseinstellungen an:

Option	Beschreibung
Kein(e)	Die Ausführung erfolgt im Zusammenhang mit einem Ereignis anstatt zu einem bestimmten Datum oder zu einem bestimmten Zeitpunkt.
jede Stunde	Der Vorgang wird im angegebenen Intervall durchgeführt.
Täglich/an einem bestimmten Tag um HH:MM	Die Erfassung wird täglich zu einem bestimmten Zeitpunkt oder an einem bestimmten Wochentag um eine bestimmte Uhrzeit ausgeführt.
Ausführen am n-ten jedes Monats/eines bestimmten Monats um HH:MM	Die Erfassung wird jeden Monat oder in einem bestimmten Monat an einem festgelegten Datum zu einer festgelegten Uhrzeit ausgeführt.
Ausführen am n-ten Wochentag **jedes Monats/ eines bestimmten Monats um HH:MM**	Die Erfassung wird jeden Monat oder in einem bestimmten Monat an einem festgelegten Wochentag zu einer festgelegten Uhrzeit ausgeführt.

Benutzerdefiniert	Führen Sie die Erfassung nach einem benutzerdefinierten Zeitplan aus.
	Verwenden Sie das Standard-5-Feld-Cron-Format (das erweiterte Cron-Format wird nicht unterstützt):
	`* * * * *`
	`| | | | +————————Wochentag (0-6) (Sonntag=0)`

Option	Beschreibung

	`| | | +————————Monat (1-12)`
	`| | +————————Monatstag (1-31)`
	`| +————————Stunde (0-23)`
	`+————————Minute (0-59)`
	
	Verwenden Sie bei der Angabe von Werten die folgenden Zeichen:
	
	• **Leerzeichen( )**: Die einzelnen Felder mit einem Leerzeichen trennen.
	• **Sternchen (*)**: Ein Sternchen repräsentiert den gesamten Wertebereich in einem Feld. Zum Beispiel repräsentiert ein Sternchen im Stundenfeld eine beliebige Stunde.
	• **Kommas (,)**: Mehrere Werte in einem Feld werden mit einem Komma getrennt. Zum Beispiel werden mit `0,6` im Feld „Wochentag“ Sonntag und Samstag angegeben.
	• **Bindestriche (-)**: Mit einem Bindestrich wird ein Wertebereich in einem Feld angegeben. Zum Beispiel entspricht `1-5` im Feld „Wochentag“ `1,2,3,4,5`, d. h. Montag bis Freitag.
	• **Schrägstriche (/)**: Die Angabe der Zeitabstände, mit denen eine Aktion wiederholt werden soll, erfolgt mit einem Schrägstrich. Zum Beispiel entspricht `*/3` im Feld Stunde `0,3,6,9,12,15,18,21`. Das Sternchen (`*`) gibt jede Stunde an, mit `/3` erfolgt aber eine Einschränkung auf durch drei teilbare Stunden.
	
	Beispiele:
	
	• `15 * * * * Jeden Tag 15 Minuten nach jeder vollen Stunde ausführen`
	• `0 22 * * * Jeden Tag um 22:00 Uhr ausführen`
	• `0 0 1 1,6 * Am 1. Januar und 1. Juni um 00:00 Uhr ausführen`
	• `30 8,12 * * 1-5 An Wochentagen um 08:30 Uhr und 12:30 Uhr ausführen`
	• `0 2 */2 * * Jeden zweiten Tag um 02:00 Uhr ausführen`

Aufgabenplan anzeigen	Klicken Sie, um den Aufgabenplan anzuzeigen. Im Dialogfeld *Aufgabenplan* wird eine Liste der geplanten Aufgaben angezeigt. Klicken Sie auf eine Aufgabe, um die Aufgabendetails anzuzeigen. Weitere Informationen hierzu finden Sie unter Aufgabenpläne anzeigen.

6. Fügen Sie im Abschnitt *Aufgaben* eine oder mehrere Aufgaben hinzu.
   a. Klicken Sie auf **Neue Aufgabe**, um eine Aufgabe hinzuzufügen.

b. Klicken Sie im Bereich *Neue Aufgabe*, der angezeigt wird, auf **Aufgabentyp** und treffen Sie eine Auswahl aus den verfügbaren Typen nach Bedarf.

Einige Vorgangsarten:

- Haben eine Option **Bei Fehler abbrechen.** Bei Auswahl dieser Option wird die Ausführung der Aufgabenabfolge auf einer bestimmten Maschine angehalten, wenn sie auf dieser Maschine fehlschlägt.
- Ermöglicht die Auswahl einer bestimmten benutzerdefinierten Aufgabe, z. B. Wake On LAN, Skripte und Patch-Zeitpläne.
- Führen Sie alle zutreffenden Aufgaben auf der Maschine aus, z. B. die verwaltete Installation (MI) und die Dateisynchronisierung (FS).

Außerdem können Sie bei bestimmten Aufgabentypen eine bestimmte benutzerdefinierte Aufgabe auswählen. Andere Aufgabentypen, z. B. die verwaltete Installation (MI) und die Dateisynchronisierung (FS) führen alle zutreffenden MI- oder FS-Aufgaben auf der Maschine aus.

Die ausgewählte Aufgabe wird im Abschnitt *Aufgaben* angezeigt.

7. Um die Aufgaben in der Aufgabenabfolge neu anzuordnen, klicken Sie in der rechten oberen Ecke des Aufgabenbereichs auf ☰ und ziehen Sie die Aufgabe an einen gewünschten Ort in der Sequenz.
8. Um eine Aufgabe aus der Aufgabenabfolge zu löschen, klicken Sie in der rechten unteren Ecke des Aufgabenbereichs auf 🗑.
9. Klicken Sie auf **Speichern**.

Um eine Aufgabenabfolge auszuführen, wählen Sie sie auf der Seite *Aufgabenabfolgenliste* aus und klicken Sie auf **Aktion wählen** > **Ausführen**.

Patchen von Geräten und Aufrechterhalten der Sicherheit

Mit der Appliance können Sie verwaltete Geräte patchen, um Funktionen der Software zu verbessern und Geräte und Netzwerke vor Sicherheitslücken zu schützen.

Verwenden des Sicherheits-Dashboards

Das Sicherheits-Dashboard bietet einen Überblick über den Patching-Prozess für die ausgewählte Organisation (falls zutreffend) oder die Appliance.

Wenn auf der Appliance die Organisationskomponente aktiviert ist und Sie bei der Administratorkonsole angemeldet sind (`http://`**appliance_hostname**`/admin`), zeigt das Sicherheits-Dashboard Informationen zur ausgewählten Organisation an.

Sie können auf das Sicherheits-Dashboard zugreifen, wenn eine oder mehrere Rollen, die mit Ihrem Benutzerkonto verknüpft sind, Zugriff auf dieses Dashboard haben. Wenn Sie es ausblenden möchten, bearbeiten Sie Ihre Benutzerrollen nach Bedarf. Weitere Informationen hierzu finden Sie unter Benutzerrollen hinzufügen oder bearbeiten.

TIPP: Die Appliance aktualisiert die Übersichtswidgets regelmäßig. Um die meisten Widgets zu aktualisieren, klicken Sie auf die Schaltfläche **Aktualisieren** in der oberen rechten Seite: . Um die meisten einzelne Widgets zu aktualisieren, zeigen Sie mit dem Mauszeiger auf das Widget und klicken Sie oberhalb des Widgets auf die Schaltfläche **Aktualisieren**. Einige Widgets erfordern möglicherweise zusätzliche Schritte.

Informationen über die Sicherheits-Dashboard-Widgets

Sicherheits-Dashboard-Widgets enthalten Informationen zur allgemeinen Patch-Compliance Ihrer verwalteten Geräte.

In diesem Abschnitt werden die im Sicherheits-Dashboard verfügbaren Widgets beschrieben. Wenn die Organisationskomponente für Ihre Appliance aktiviert ist, zeigt das Widget Informationen für die jeweils ausgewählte Organisation auf Administratorebene an.

Dieses Dashboard bietet einen Überblick über die Patch-Compliance in Ihrer Umgebung und über die Patching-Prozesse. Dadurch können Sie schnell die Stufe der auf den verwalteten Geräten installierten System-Patches überprüfen und nach Indikatoren suchen, mit denen Sie die Systemsicherheit verbessern können. Sie können sich beispielsweise auf die Compliance von Geräte-Patches konzentrieren und Ihre Patch-Pläne überprüfen, um sicherzustellen, dass die neuesten Systemaktualisierungen auf Ihren verwalteten Geräten installiert und ausgeführt werden.

Widget	Beschreibung
Compliance der kritischen Patches	Dieses Widget zeigt den Fortschritt in der Bereitstellung der Patches an, die als kritisch gekennzeichnet sind. Wenn für Ihre Appliance die Organisationskomponente aktiviert ist, zeigt das Widget Informationen für die jeweils ausgewählte Organisation an.
Dell Aktualisierungen	Dieses Widget zeigt die Anzahl der Dell Anwendungen, die BIOS-Anzahl und die Anzahl der Firmwareaktualisierungen, die auf verwaltete Geräte angewendet werden können. Die Aktualisierungen werden abhängig von der Priorität der Aktualisierung als *Angemessen*, *Wichtig* oder *Kritisch* kategorisiert. Nach dem Erstellen eines Dell Aktualisierungszeitplans werden Daten im Widget angezeigt. Siehe Dell Aktualisierungszeitpläne konfigurieren. Wenn für Ihre Appliance die Organisationskomponente aktiviert ist, zeigt das Widget Informationen für die jeweils ausgewählte Organisation an.
Compliance nach Computer	Dieses Widget zeigt ein Ringdiagramm an, in dem die einzelnen Abschnitte des Diagramms den freien Speicherplatz in Prozent auf den verwalteten Geräten angeben. Wenn Sie den Mauszeiger über die einzelnen Abschnitte des Diagramms bewegen, wird der Prozentsatz der Patch-Compliance des ausgewählten Geräts angezeigt. Sie können die im Widget angezeigten Informationen ändern, indem Sie den Patch-Herausgeber, das Betriebssystem, das Label, die Klassifizierung, den Schweregrad, die KB-Nummer und das Verfügbarkeitsdatum auswählen. Sie können je nach Bedarf auch zwischen Balkendiagramm- und Ringdiagramm-Ansichten wechseln. Sie können auch mehrere Instanzen des Widgets auf dem Sicherheits-Dashboard installieren, wobei in jeder Instanz ein anderer Parametersatz verwendet wird.
Compliance nach Patch	Dieses Widget zeigt ein Ringdiagramm an, in dem die Abschnitte des Diagramms den Prozentsatz der Compliance für die einzelnen anwendbaren Patches angeben. Wenn Sie den Mauszeiger über die einzelnen Abschnitte des Diagramms bewegen, wird der Prozentsatz der Compliance für den ausgewählten Patch angezeigt. Sie können die im Widget angezeigten Informationen ändern, indem Sie den Patch-Herausgeber, das Betriebssystem, das Label, die Klassifizierung, den Schweregrad, die KB-Nummer und das Verfügbarkeitsdatum auswählen. Sie können je nach Bedarf auch zwischen Balkendiagramm- und Ringdiagramm-Ansichten wechseln. Sie können auch mehrere Instanzen des

Widget	Beschreibung
	Widgets auf dem Sicherheits-Dashboard installieren, wobei in jeder Instanz ein anderer Parametersatz verwendet wird.
Patch-Installationsfortschritt	Dieses Widget zeigt den Fortschritt der Patch-Aufgaben an, die derzeit auf verwalteten Geräten laufen. Wenn für Ihre Appliance die Organisationskomponente aktiviert ist, zeigt das Widget Informationen für die jeweils ausgewählte Organisation an.
Bereitgestellte Patches	Dieses Widget zeigt die Anzahl der derzeit bereitgestellten Patches an. Sie können die im Widget angezeigten Informationen ändern, indem Sie den Patch-Herausgeber, das Betriebssystem, das Label, die Klassifizierung, den Schweregrad, die KB-Nummer und das Verfügbarkeitsdatum auswählen. Sie können je nach Bedarf auch zwischen Balkendiagramm- und Ringdiagramm-Ansichten wechseln. Sie können auch mehrere Instanzen des Widgets auf dem Sicherheits-Dashboard installieren, wobei in jeder Instanz ein anderer Parametersatz verwendet wird.
Fehlerhafte Patches	Dieses Widget zeigt die Anzahl der Patches an, die nicht bereitgestellt werden konnten. Sie können die im Widget angezeigten Informationen ändern, indem Sie den Patch-Herausgeber, das Betriebssystem, das Label, die Klassifizierung, den Schweregrad, die KB-Nummer und das Verfügbarkeitsdatum auswählen. Sie können je nach Bedarf auch zwischen Balkendiagramm- und Ringdiagramm-Ansichten wechseln. Sie können auch mehrere Instanzen des Widgets auf dem Sicherheits-Dashboard installieren, wobei in jeder Instanz ein anderer Parametersatz verwendet wird.
Freigegebene Patches	Dieses Widget zeigt die Anzahl der Patches an, die freigegeben und für die Bereitstellung verfügbar sind. Sie können die im Widget angezeigten Informationen ändern, indem Sie den Patch-Herausgeber, das Betriebssystem, das Label, die Klassifizierung, den Schweregrad, die KB-Nummer und das Verfügbarkeitsdatum auswählen. Sie können je nach Bedarf auch zwischen Balkendiagramm- und Ringdiagramm-Ansichten wechseln. Sie können auch mehrere Instanzen des Widgets auf dem Sicherheits-Dashboard installieren, wobei in jeder Instanz ein anderer Parametersatz verwendet wird.
Patch-Aufgaben abgeschlossen	Dieses Widget zeigt den Fortschritt der Patch-Aufgaben wie Erkennungs-, Bereitstellungs- und

Widget	Beschreibung
	Rollback-Aufgaben an, die derzeit auf verwalteten Geräten laufen. Wenn für Ihre Appliance die Organisationskomponente aktiviert ist, zeigt das Widget Informationen für die jeweils ausgewählte Organisation an.
Berichte	Dieses Widget enthält Links zu häufig verwendeten Patching-Berichten. Sie können damit schnell Berichte zu bestimmten Themen erstellen wie *Liste mit kritischen und aktuellen Bulletins*, *Nicht kompatible Geräte nach Patch* und andere.
SCAP-Zusammenfassung	Dieses Widget liefert Informationen zu den SCAP-Scans, die an Geräten durchgeführt wurden. Wenn für Ihre Appliance die Organisationskomponente aktiviert ist, zeigt das Widget Informationen für die jeweils ausgewählte Organisation an.
Ansichten	Dieses Widget enthält Links zu allgemeinen Patching-Seiten und -Assistenten, einschließlich benutzerdefinierten Ansichten, die Sie erstellt haben. Sie können damit schnell zu bestimmten Seiten navigieren, z. B. zum *Patch-Katalog*. Wenn Sie benutzerdefinierte Ansichten angelegt haben, werden diese alphabetisch sortiert. Wenn die benutzerdefinierten Ansichten in einer bestimmten Reihenfolge angezeigt werden sollen, können Sie ihre Namen bei Bedarf mit Nummern versehen.
Windows 10 Versionen	Dieses Widget zeigt ein Balkendiagramm an, wobei jedes Element im Diagramm eine bestimmte Windows 10-Version und die Anzahl der verwalteten Geräte darstellt, auf denen diese Version ausgeführt wird. So können Sie sich ein Bild davon machen, wie viele Geräte für veröffentlichte Windows 10-Aktualisierungen geeignet sind.

Sicherheits-Dashboard anpassen

Sie können das Dashboard anpassen und Widgets nach Bedarf ein- oder ausblenden.

1. Rufen Sie das *Dashboard* auf.
    a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.

b. Klicken Sie in der linken Navigationsleiste auf **Sicherheit** und anschließend auf **Dashboard**.

2. Fahren Sie mit dem Mauszeiger über das Widget und verwenden Sie anschließend die folgenden Schaltflächen:
   - : Die Informationen im Widget aktualisieren
   - : Die Informationen zum Widget anzeigen
   - : Das Widget ausblenden
   - : Die Größe des Widgets ändern
   - : Das Widget an eine andere Position auf der Seite ziehen.
3. Einige Widgets sind bearbeitbar, sodass Sie die angezeigten Informationen filtern können. Klicken Sie zum Bearbeiten des Widgets auf , und wählen Sie im angezeigten Dialogfeld den Patch-Herausgeber, das Betriebssystem, das Label, die Klassifizierung, den Schweregrad, die KB-Nummer oder das Verfügbarkeitsdatum aus. Sie können je nach Bedarf auch zwischen Balkendiagramm- und Ringdiagramm-Ansichten wechseln.
4. Klicken Sie auf die Schaltfläche **Anpassen** in der oberen rechten Ecke der Seite, um die verfügbaren Widgets anzuzeigen.
5. Um ein Widget anzuzeigen, das derzeit ausgeblendet ist, klicken Sie auf **Installieren**.

Informationen zur Patch-Verwaltung

Die Patch-Verwaltung umfasst das Abrufen, Testen und Installieren von Patches für Software auf Geräten. Mit der Appliance können Sie die Patch-Verwaltung automatisieren, um die Verbesserung von Softwarefunktionen und den Schutz von Geräten und Netzwerken vor Sicherheitslücken zu vereinfachen.

Mit der Patch-Verwaltung können Sie für Windows und Mac Geräte, die die Appliance nutzen, die neuesten Sicherheits-Patches und Softwareaktualisierungen ermitteln und bereitstellen.

HINWEIS: Die Komponente "Patch-Verwaltung" wird nur auf Windows und Mac Geräten unterstützt. Die Patch-Verwaltung ist für Linux Geräte nicht verfügbar.

Patch-Workflow

Der Patch-Workflow umfasst das Abonnieren von Patches, das Auswählen von Downloadeinstellungen für Patches, das Identifizieren von Patches und zu patchenden Geräten mithilfe von Labels sowie das Planen von Patch-Jobs.

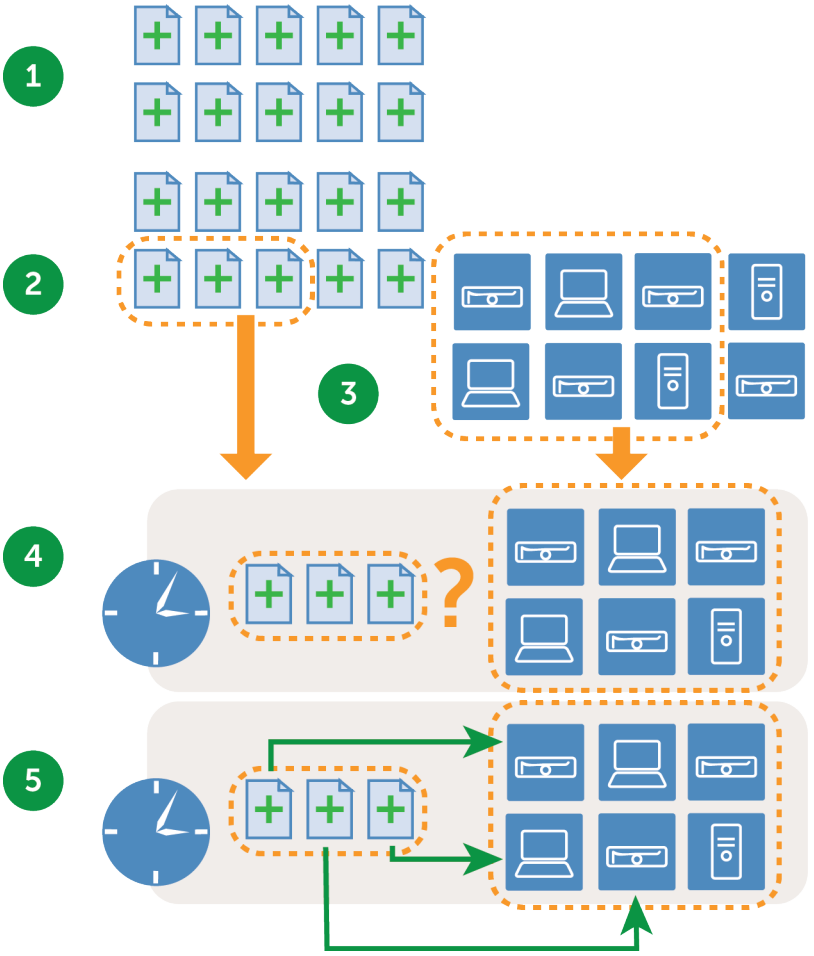
Der Patch-Workflow umfasst folgende Aufgaben:

- Die Patches abonnieren, die Sie herunterladen möchten. Wenn auf der Appliance die Organisationskomponente installiert wurde, legen Sie für jede Organisation individuelle

Abonnementeinstellungen fest. Zusätzliche Workflow-Details sind verfügbar, wenn Sie zum ersten Mal ein Patch abonnieren. Siehe Abonnieren von Patches und Konfigurieren von Downloadeinstellungen.

- Auswählen von Patch-Download-Einstellungen auf der Seite *Patch-Abonnementeinstellungen*. Siehe Download-Einstellungen für Patch- und Funktionsaktualisierungen auswählen.
- Erstellen von Smart Labels, um Geräte für das Patchen und Patches für die Bereitstellung zu gruppieren. Siehe Smart Labels für Patches verwenden.
- Patch-Zeitpläne für die Erkennung und Bereitstellung von Paketen erstellen. Wenn auf der Appliance die Organisationskomponente installiert wurde, erstellen Sie für jede Organisation individuelle Patch-Zeitpläne. Siehe Konfigurieren von Patch-Zeitplänen.

Patch-Workflow



Nummer in der Legende	Aktion
1	Signaturdateien für Patches, die Sie abonniert haben, werden von Quest auf die Appliance heruntergeladen. Patch-Pakete werden von Quest und von Softwareherstellern heruntergeladen.
2	Smart Labels gruppieren die heruntergeladenen Patches.
3	Smart Labels wählen Geräte zum Patchen aus.

Nummer in der Legende	Aktion
4	Patches, die von Geräten benötigt werden, werden nach einem Zeitplan erkannt.
5	Patches werden nach einem Zeitplan auf Geräten bereitgestellt.

Informationen zu Patch-Signaturdateien

Patch-Signaturdateien enthalten die Sicherheitsbulletins und andere Dateien, die Patches definieren. Sie enthalten nicht die Patch-Pakete, mit denen Patches installiert werden.

Patch-Signaturdateien werden nach den von Ihnen ausgewählten Abonnement- und Download-Optionen von Quest heruntergeladen. Weitere Informationen zum Herunterladen von Patch-Signaturdateien finden Sie unter Download-Einstellungen für Patch- und Funktionsaktualisierungen auswählen.

Informationen zu Patch-Paketen

Patch-Pakete sind die Dateien, die für die Installation von Patches benötigt werden.

Patch-Pakete werden nach den von Ihnen ausgewählten Abonnement- und Download-Optionen von Quest heruntergeladen. In einigen Fällen werden Patch-Pakete auch direkt von Herstellern wie Microsoft und Adobe heruntergeladen.

Es gibt zwei Optionen für das Herunterladen von Patch-Paketen:

- **Nur die benötigten Patches herunterladen**: Sie haben die Möglichkeit, nur die Pakete herunterzuladen, bei denen erkannt wurde, dass sie von den verwalteten Geräten benötigt werden. Dadurch verringern sich die Download-Zeit und der benötigte Speicherplatz. Außerdem können Sie Patches nach einem angegebenen Zeitraum automatisch entfernen lassen, wenn Erkennungsergebnisse angeben, dass die Patches nicht benötigt werden.
- **Vollständigen Cache mit Patches verwalten**: Sie können einen vollständigen Cache mit Paketen unabhängig davon verwalten, ob die Patches von den verwalteten Geräten benötigt werden. Dadurch bleiben Pakete für die schnelle Bereitstellung verfügbar. Es werden aber mehr Zeit für das Herunterladen und mehr Speicherplatz benötigt als beim Herunterladen nur der Pakete, die erforderlich sind.

Weitere Informationen über Optionen für das Herunterladen von Paketen finden Sie unter Download-Einstellungen für Patch- und Funktionsaktualisierungen auswählen.

Informationen zu Patch-Tests und Sicherheit

Quest bietet sichere, zeitnahe und qualitativ hochwertige Patch-Signaturen für Windows- und Mac-Betriebssysteme sowie viele gängige Anwendungen.

Bevor Patch-Signaturen der Appliance zur Verfügung gestellt werden, führt Quest die folgenden Sicherheitsprüfungen durch:

- Überprüfung von Patch-Metadaten, die von den jeweiligen Inhaltsentwicklungsteams erstellt werden
- Überprüfung von Installations- und Deinstallationsvorgängen für Patches
- Bestätigung, dass das Patch die Stabilität der Ziel-Betriebssysteme und -Anwendungen nicht beeinträchtigt

Informationen zur Patch-Testumgebung

Quest verwendet VMware® ESX®, VMware® vCenter™, Microsoft® Azure® und benutzerdefinierte Tests der Hardware-Umgebung.

Zu den Testmethoden gehört die Überprüfung, ob die Benennungskonventionen für Patches den Richtlinien von Quest entsprechen.

Informationen zu Bewertungstests

Mithilfe von Bewertungstests wird überprüft, ob die Komponente "Patch-Verwaltung" ordnungsgemäß funktioniert.

Durch die Tests wird sichergestellt, dass

- ein anwendbares, nicht gepatchtes Gerät als anwendbar und nicht gepatcht angezeigt wird
- ein gepatchtes Gerät als installiert und nicht anwendbar angezeigt wird
- keine falsch positiven Ergebnisse bei der Erkennung des digitalen Fingerabdrucks vorhanden sind
- der Patch-Inhalt mit den obligatorischen Grundlinien kompatibel ist
- Sicherheitslücken im Aktualisierungsserver richtig angezeigt werden
- alle Smart Label-, Sortier- und sonstigen visuellen Funktionen ordnungsgemäß funktionieren

Informationen zu Bereitstellungstests

Bereitstellungstests überprüfen die ordnungsgemäße Bereitstellung von Patches.

Durch die Tests wird sichergestellt, dass

- das Paket bereitgestellt werden kann
- die Unterdrückung der Neustartfunktion funktioniert
- die Deinstallationsfunktion funktioniert
- die bedarfsmäßige Paket-Cache-Speicherung funktioniert
- die automatische Bereitstellungsplanung funktioniert
- der Agenten-Paketdownload funktioniert
- die SHA1-Prüfsumme die Paketintegrität sicherstellt
- der Agent nach der Patch-Bereitstellung automatisch eine Bewertung durchführt
- der Agent nach dem Neustart automatisch neu gestartet wird

Informationen zum Prozess der Patch-Qualitätsprüfung

Quest stellt Kunden von Patch-Verwaltung Mehrwert durch Inhaltsentwicklungs- und Qualitätssicherungsprozesse zur Verfügung. Die Qualitätssicherungsteams überprüfen die Installations- und Deinstallationsprozesse jedes Patch sowie die vom Inhaltsentwicklungsteam produzierten Metadaten. Die Bereitstellung hochwertiger Inhalte an unsere Kunden hat bei uns höchste Priorität. Um die erfolgreiche Zustellung von Inhalten zu gewährleisten, führt Quest Testfälle an den folgenden Testkomponenten aus.

Testumgebung

Quest investiert in erheblichem Maße in die Testinfrastruktur. Die Inhaltsentwicklungs- und Qualitätssicherungsteams haben Zugriff auf eine virtuelle Unternehmensumgebung, die Knoten unterschiedlicher

Konfigurationen repräsentiert. Quest verwendet neben physischen Benchtests eine Mischung aus virtuellen Desktops und Servern, um sicherzustellen, dass unsere Testinfrastruktur stets auf dem neuesten Stand ist.

Anwendungstests

Quest führt Tests mit verschiedenen Anwendungen aus, um sicherzustellen, dass die Anforderungen des Patch erfüllt werden.

Teststrategie

Quest verwendet die folgenden Arten von Tests:

- **Allgemeine Tests** bestätigen, dass:
  - die Patch-Namenskonvention die Richtlinien von Quest erfüllt
- **Bewertungstests** bestätigen, dass:
  - ein anwendbares, nicht gepatchtes System als anwendbar und nicht gepatcht angezeigt wird
  - ein gepatchtes System als installiert und nicht anwendbar angezeigt wird
  - keine falsch positiven Ergebnisse bei der Erkennung des digitalen Fingerabdrucks vorhanden sind
  - der Inhalt mit den obligatorischen Grundlinien kompatibel ist
  - der Patch korrekt im Patch-Server angezeigt wird, einschließlich aller Filter, Sortierung und visueller Funktionen
- **Bereitstellungstests** bestätigen, dass:
  - das Paket erfolgreich bereitgestellt werden kann
  - die Unterdrückung der Neustartfunktion ordnungsgemäß funktioniert
  - die Deinstallationsfunktion ordnungsgemäß funktioniert
  - die bedarfsmäßige Paket-Cache-Speicherung ordnungsgemäß funktioniert
  - die automatische Bereitstellungsplanung ordnungsgemäß funktioniert
  - der Agenten-Paketdownload funktioniert
  - der Paket-Hash die Integrität des Pakets gewährleistet
  - der Agent nach der Patch-Bereitstellung automatisch eine Bewertung durchführt
  - der Agent nach dem Neustart automatisch neu gestartet wird

Vertrauenswürdige Zustellung und Flexibilität

Die Prozesse von Quest sind darauf ausgelegt und werden implementiert, um die globale Verfügbarkeit über ein sicheres Distributionsnetzwerk für Inhalte zu maximieren. Jede Kommunikation mit Quest erfolgt über verschlüsselte, sichere Kanäle, um die Integrität der Sicherheitsinhalte zu gewährleisten.

Dank eines Best-Practice-Ansatzes werden wichtige Sicherheits-Patches automatisch an Kundenstandorte herunterladen (abhängig von den Abonnementoptionen). Zusätzliche Sicherheits-Patches können nach Bedarf heruntergeladen werden, um eine kundenindividuelle Version des of the KACE Patch Content Repository innerhalb der sicheren Unternehmensumgebung des Kunden zu erstellen.

Best Practices für den Patch-Vorgang

Die Best Practices für den Patch-Vorgang umfassen das Testen von Patches, das Organisieren von Geräten und Patches mithilfe von Labels sowie das Benachrichtigen von Benutzern beim Patchen von Systemen.

- **Testen von Patches vor ihrer Bereitstellung**

  Testen Sie Patches auf ausgewählten Geräten, bevor Sie sie für alle Geräte bereitstellen. Diese Tests gewährleisten, dass Patches bei ihrer systemweiten Bereitstellung keine Probleme verursachen.

Achten Sie bei der Auswahl von Testgeräten auf die folgenden Merkmale:

- Geräte, deren Benutzer technisch versiert sind und Probleme effektiv kommunizieren können.
- Geräte mit Zugriff auf die Systeme und Software, die die Arbeitsumgebung widerspiegeln.

Für einen umfassenden Test sollten Geräte nach dem Patchen mindestens eine Woche lang normal funktionieren. Wenn nach einer Woche keine Probleme gemeldet werden, kann das Patch für die restlichen Geräte im Netzwerk bereitgestellt werden.

- **Verwenden von Labels zum Organisieren von Geräten und Patches**

  Mit Smart Labels können Sie Geräte automatisch nach Typ, zum Beispiel Notebook, Desktop und Server, gruppieren. Außerdem können Sie mit Smart Labels Patches automatisch nach Wichtigkeit gruppieren, zum Beispiel kritische Betriebssystem-Patches und Patches für andere Anwendungen mit niedrigerer Priorität. Anschließend können Sie Patch-Zeitpläne für die einzelnen Geräte- und Patch-Typen erstellen.

  Siehe:

  - Smart Labels für Patches verwenden
  - Erstellen und Verwalten von Patch-Zeitplänen

- **Verwenden von Windows Update oder der Appliance zum Patchen von Windows-Geräten**

  Es gibt zwei Optionen für das Patchen von Windows-Geräten:

  - **Windows Update verwenden**: Windows Update ist eine Microsoft-Funktion, mit der Updates für Windows Betriebssysteme heruntergeladen und installiert werden. Wenn Sie Windows Update auf verwalteten Geräten aktivieren, verwenden Sie die Komponente "Patch-Verwaltung" der Appliance nur zur Erkennung von Patches für Windows Betriebssysteme, nicht für ihre Bereitstellung. Patches werden von Windows Update bereitgestellt.
  - **Use the appliance (Appliance verwenden)**: Sie können mithilfe der Patch-Verwaltung Patches für Windows Betriebssysteme herunterladen und bereitstellen. Deaktivieren Sie bei Verwendung der Patch-Verwaltung auf der Appliance das Windows Update-Feature auf verwalteten Geräten, da die Patches von der Appliance bereitgestellt werden.

  TIPP: Mit der Appliance können Sie eine Richtlinie erstellen, die angibt, ob verwaltete Geräte Windows Update verwenden. Siehe Verwenden der Windows Konfigurationsrichtlinien.

- **Minimieren der Ausfallzeit während des Patch-Vorgangs**

  Planen Sie die Patch-Bereitstellung in Zeiträumen, in denen die Geräte weniger genutzt werden, um die Ausfallzeit zu minimieren. Beachten Sie, dass die Gerätenutzung je nach Gerätetyp variiert:

  - **Server**: Für sie sind sorgfältige und gut publizierte Aktualisierungen erforderlich. Beim Patchen von Servern müssen Sie möglicherweise mehrere Wochen im Voraus planen.
  - **Desktops**: Sie verfügen über flexiblere Patch-Optionen, da sie oft eingeschaltet bleiben, wenn sie nicht genutzt werden.
  - **Notebooks**: Bei ihnen ist der Patch-Vorgang am schwierigsten durchzuführen, da sie häufig nur dann für den Patch-Vorgang zur Verfügung stehen, während sie benutzt werden.

  Weitere Informationen zum Erstellen von Patch-Zeitplänen für die einzelnen Gerätetypen finden Sie unter:

  - Informationen zum Planen von kritischen Betriebssystem-Patches für Desktops und Server
  - Informationen zum Planen von kritischen Patches für Notebooks

- **Benachrichtigen von Benutzern beim Patchen von Geräten**

  Vergessen Sie nicht, Benutzer über das Patchen der von ihnen verwendeten Geräte zu benachrichtigen. Das ist besonders wichtig, wenn Geräte als Teil des Patch-Vorgangs neu gestartet werden müssen. Es gibt mehrere Möglichkeiten, Benutzer über Patch-Zeitpläne zu informieren:

  - **E-Mail senden oder andere Messaging-Systeme verwenden**: Benachrichtigen Sie Benutzer vorab per E-Mail und über andere Messaging-Systeme außerhalb der **Administratorkonsole** der

Appliance. Diese Benachrichtigung ist besonders hilfreich, wenn das Patchen für einen bestimmten Zeitraum den Zugriff auf kritische Systeme (wie etwa Server) verhindert.

- **Eine Warnmeldung von der Appliance aus senden**: Erstellen Sie mit der **Administratorkonsole** Appliance eine Warnung und senden Sie sie als Broadcast-Benachrichtigung an alle oder ausgewählte Geräte. Mit diesen Broadcast-Warnungen können Benutzer daran erinnert werden, dass in Kürze mit dem Patchen begonnen wird.

  Weitere Informationen zur Erstellung von Warnungen finden Sie unter Senden von Warnungen an verwaltete Geräte.

- **Warnungen während des Patch-Vorgangs**: Wenn Sie das Patchen planen, können Sie Benutzer vorab warnen und ihnen vor dem Neustart ihrer Geräte Aufforderungen senden. Sie können Benutzern auch die Möglichkeit geben, Neustarts bei Bedarf kurzfristig per Snooze oder langfristig zu verschieben. Siehe Konfigurieren von Patch-Zeitplänen.

Weitere Informationen zum Planen von Patches für verschiedene Geräte finden Sie unter:

- Informationen zum Planen von kritischen Betriebssystem-Patches für Desktops und Server
- Informationen zum Planen von kritischen Patches für Notebooks

- **Festlegen von Fristen für Patch-Jobs, um Auswirkungen auf Benutzer zu verringern**

  Patch-Jobs können sehr viel Bandbreite und Ressourcen erfordern. Um die Auswirkungen auf Benutzer zu verringern, können Sie Fristen für Patch-Jobs festlegen. Sie können beispielsweise konfigurieren, dass Patching-Jobs um 04:00 Uhr gestartet und um 07:00 Uhr angehalten werden. Sämtliche Patching-Jobs, die sich um 07:00 Uhr noch in Bearbeitung befinden, werden ausgesetzt. Mit Beginn des nächsten geplanten Patch-Jobs werden Jobs dort fortgesetzt, wo sie angehalten wurden. Siehe Konfigurieren von Patch-Zeitplänen.

- **Verwenden von Replikationsfreigaben zur Optimierung von Netzwerkressourcen**

  Verwenden Sie Replikationsfreigaben zur Optimierung von Netzwerkressourcenanforderungen und Download-Zeiten. Replikationsfreigaben sind Geräte, die Kopien von Dateien für die Verteilung bereithalten. Das kann für verwaltete Geräte hilfreich sein, die an mehreren geografischen Standorten bereitgestellt werden. Mit Replikationsfreigaben kann beispielsweise ein Gerät in New York Patch-Dateien von einem anderen Gerät im selben Büro herunterladen anstatt von einer Appliance in Los Angeles.

  Weitere Informationen zur Einrichtung und Verwendung von Replikationsfreigaben finden Sie unter Verwenden von Replikationsfreigaben.

- **Suchen von Informationen in der Quest KACE Knowledge Base**

  Quest Support verfügt über eine Knowledge Base mit Artikeln zur Appliance. Diese finden Sie unter https://support.quest.com/kace-systems-management-appliance/kb. Die Knowledge Base wird ständig mit Lösungen zu realen Problemen, auf die Administratoren im Zusammenhang mit der Appliance stoßen, aktualisiert. Zum Anzeigen von Artikeln zum Patchen rufen Sie die Knowledge Base auf und suchen Sie nach *Security*.

- **Verwenden von ITNinja.com, um mit anderen IT-Spezialisten Verbindung aufzunehmen**

  ITNinja.com (früher AppDeploy.com) ist eine von Quest KACE gesponserte, produktübergreifende Community-Website mit dem Schwerpunkt IT. Sie ist das führende Internet-Ziel für IT-Spezialisten zum Austausch von Informationen und für Fragen auf dem Gebiet der Systemverwaltung. Siehe http://itninja.com.

Abonnieren und Herunterladen von Patches

Zum Patchen müssen Sie Patches abonnieren und Patch-Downloads auf die Appliance planen.

Informationen zu Patch-Abonnements und -Downloads

Unter Patch-Abonnement versteht man den Vorgang, bei dem Sie die Betriebssysteme und Anwendungen auswählen, für die Sie Patches erhalten möchten.

Wenn auf der Appliance die Organisationskomponente aktiviert wurde, können Sie für jede Organisation individuelle Abonnements auswählen.

Nachdem Sie Patches abonniert haben, werden diese von der Appliance entsprechend dem festgelegten Zeitplan heruntergeladen. Sie können die Patches nach dem Herunterladen testen und bereitstellen. Sie können die Patches auch automatisch bereitstellen, dies wird jedoch nur für Patches mit niedrigem Risiko oder für zeitkritische Patches empfohlen. Siehe:

- Download-Einstellungen für Patch- und Funktionsaktualisierungen auswählen
- Smart Labels für Patches verwenden

Anwendungen, die die Appliance patchen kann

Eine Liste mit Anwendungen, die die Appliance patchen kann, finden Sie unter https://support.quest.com/kb/112030. Öffnen Sie die Anlage.

NTP-Service als Voraussetzung

Um Patches über HTTPS herunterladen zu können, muss der NTP-Dienst (Network Time Protocol) auf der Appliance ausgeführt werden. Der NTP-Dienst ist erforderlich, weil das sichere Protokoll aktuelle Datumsstempel der Appliance verwendet, um die Gültigkeit des Zertifikats sicherzustellen. Falls der NTP-Service nicht ausgeführt wird, könnte das Herunterladen der Patches fehlschlagen, was ein Hinweis auf ungültige Zertifikate sein könnte.

Websites, die für die Appliance zugänglich sein müssen

Für Patch-Downloads, den Zugriff auf Produktinformationen und die Interaktion mit dem **Quest Support** müssen die Firewall-, DNS-Server- und Proxy-Servereinstellungen der Appliance den Zugriff auf bestimmte Domains über Port 80 und Port 443 ermöglichen.

Domänen, die für die Appliance zugänglich sein müssen

Domain	Verwendungszweck
https://support.quest.com/download-product-select	Quest Updates
http://servicecdn.kace.com	SCAP (Secure Content Automation Protocol)
https://service.kace.com	Appliance- und Agenten-Aktualisierungen von Quest
https://support.quest.com	Quest Support
http://cdn01.catalog.kace.com/	Quest Updates
https://cdn01.catalog.kace.com/	Quest Updates

Domain	Verwendungszweck
https://quest.com/kace	Lokalisierte Inhalte, Softwarelizenzen von Drittanbietern und Produktinformationen
http://www.itninja.com	ITNinja-Community-Funktionen
http://appdeploy.com	Weiterleitung zu ITNinja.com
http://download.windowsupdate.com	Microsoft-Updates
http://download.microsoft.com	Microsoft-Updates
http://www.microsoft.com/en-us/default.aspx	Microsoft-Updates
https://api.dell.com	Dell Aktualisierungen
http://ftp.dell.com	Dell Aktualisierungen
http://ardownload.adobe.com/	Updates für Anwendungen von Adobe
http://armdl.adobe.com/	Updates für Anwendungen von Adobe
https://airdownload.adobe.com/	Updates für Anwendungen von Adobe
https://fpdownload.macromedia.com/	Updates für Anwendungen von Adobe
http://swcdn.apple.com/	Updates für Apple
https://swdist.apple.com	Updates für Apple
http://download.winzip.com/	Updates für Corel einschließlich WinZip
https://download.winzip.com/	Updates für Corel einschließlich WinZip
https://download.virtualbox.org/	Updates für Oracle einschließlich Java
http://download.autodesk.com/	Updates für Autodesk
http://knowledge.autodesk.com/	Updates für Autodesk
http://revit.downloads.autodesk.com/	Updates für Autodesk
http://trial2.autodesk.com/	Updates für Autodesk
http://up.autodesk.com/	Updates für Autodesk
https://knowledge.autodesk.com/	Updates für Autodesk
https://up.autodesk.com/	Updates für Autodesk

Domain	Verwendungszweck
https://cdn.sw.altova.com/	Updates für Altova
http://download.imgburn.com/	Updates für ImgBurn
https://www.realvnc.com/	Updates für RealVNC
https://www.uvnc.eu/	Updates für UltraVnc
https://download-installer.cdn.mozilla.net/	Updates für Mozilla Firefox
https://www.python.org/	Updates für Python
https://the.earth.li/	Updates für Putty
http://cdn1.evernote.com/	Updates für EverNote
https://cdn1.evernote.com/	Updates für EverNote
http://cdn01.foxitsoftware.com/	Updates für Foxit
https://download.ccleaner.com/	Updates für Piriform
https://media.inkscape.org/	Updates für inkscape
https://download.cdburnerxp.se/	Updates für Canneverbe
http://download.videolan.org/	Updates für VideoLAN
https://www.tightvnc.com/	Updates für TightVNC
http://downloadarchive.documentfoundation.org/	Updates für LibreOffice
https://download.filezilla-project.org/	Updates für FileZilla
https://e3.boxcdn.net/	Updates für Box Inc.
http://www.rarlab.com/	Updates für WinRAR GmbH
https://www.rarlab.com/	Updates für WinRAR GmbH
http://ftp.uni-kl.de/	Updates für Wireshark
https://www.wireshark.org/	Updates für Wireshark
https://notepad-plus-plus.org/	Updates für Notepad++

Übersicht über den Workflow beim ersten Patch-Abonnement

Patch-Erkennungssignaturen und Patch-Pakete werden nicht standardmäßig auf die Appliance heruntergeladen. Sie müssen die gewünschten Patches abonnieren und dann einen Zeitpunkt zum Herunterladen der Patches planen.

Zum Sparen von Netzwerkbandbreite und Speicherplatz empfiehlt Quest, zuerst Patch-Definitionssignaturen herunterzuladen, da diese wesentlich kleiner sind als Patch-Pakete. Anschließend können Sie die benötigten Patches erkennen und die für Ihr Netzwerk am besten geeigneten Download-Einstellungen auswählen.

Der folgende Workflow gilt für das erste Patch-Abonnement.

1. **Sammeln Sie Informationen**: Ermitteln Sie die Betriebssysteme, Sprachpakete und Anwendungen, die auf den verwalteten Geräten installiert sind, sodass Sie wissen, was Sie abonnieren müssen. Diese Informationen finden Sie auf der Seite *Dashboard* der Appliance sowie durch Ausführen von Berichten. Siehe Details zu Betriebssystemen und Anwendungen anzeigen.
2. **Wählen Sie anfängliche Patch-Abonnementeinstellungen aus**: Abonnieren Sie die Betriebssysteme und Sprachen, die von den verwalteten Geräten benötigt werden. Siehe Abonnieren von Patches und Konfigurieren von Downloadeinstellungen.
3. **Laden Sie Patch-Erkennungssignaturen herunter**: Patch-Erkennungssignaturen sind kleinere Dateien, die schnell heruntergeladen werden können und nicht viel Speicherplatz belegen. Laden Sie die Patch-Erkennungssignaturen der Patches herunter, die Sie abonnieren. Durch das Herunterladen dieser Signaturen können Sie verfügbare Patches anzeigen und die Patch-Pakete ermitteln, die Sie später herunterladen möchten. Siehe Download-Einstellungen für Patch- und Funktionsaktualisierungen auswählen.
4. **Führen Sie einen "Nur erkennen"-Patch-Job aus**: Planen Sie einen "Nur erkennen"-Patch-Job, um die Patches zu ermitteln, die von den verwalteten Geräten benötigt werden. Ein Patch-Job vom Typ "Nur erkennen" ist ein einmaliger Vorgang zur Ermittlung des Umfangs des ersten Patch-Jobs. Außerdem wird Ihnen die Zuteilung von Ressourcen auf Basis der Geräteverfügbarkeit für Patch-Installationen und Neustarts erleichtert. Wenn Sie einen Patch-Job vom Typ "Nur erkennen" ausführen möchten, erstellen Sie einen Patch-Zeitplan zur Erkennung von Patches auf allen Geräten. Siehe Konfigurieren von Patch-Zeitplänen.
5. **Wählen Sie Download-Einstellungen für Patch-Pakete aus**: Legen Sie nach dem Ermitteln der erforderlichen Patch-Pakete eine Uhrzeit für die Paket-Downloads fest. Siehe Download-Einstellungen für Patch- und Funktionsaktualisierungen auswählen.

Details zu Betriebssystemen und Anwendungen anzeigen

Auf der Seite *Übersichtsdetail* können Sie Informationen zu auf den verwalteten Geräten installierten Betriebssystemen und Anwendungen anzeigen.

Sammeln Sie vor dem Abonnieren von Patches Informationen zu den Betriebssystemen, Sprachpaketen und Softwareanwendungen, die auf den verwalteten Geräten installiert sind, damit Sie wissen, welche Abonnements Sie benötigen.

1. Führen Sie einen der folgenden Schritte aus:
   - **Wenn auf Ihrer Appliance die Organisationskomponente aktiviert ist und Sie Informationen zur Appliance anzeigen möchten, melden Sie sich bei der Systemverwaltungskonsole an:**

`http://appliance_hostname/system`, oder wählen Sie System aus der Dropdownliste in der oberen rechten Ecke der Seite aus.

- **Wenn für Ihre Appliance die Organisationskomponente nicht aktiviert ist oder Sie auf Informationen auf Organisationsebene zugreifen möchten, melden Sie sich bei der Administratorkonsole an: `http://appliance_hostname/admin`. Oder wählen Sie in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus, wenn die Option** *Organisationsmenü in Verwaltungskopfzeile anzeigen* **aktiviert ist.**

2. Klicken Sie auf **Startseite**, um die Seite *Dashboard* anzuzeigen.
3. Klicken Sie in der oberen rechten Ecke der Seite auf **Details anzeigen**.

   Die *Dashboard-Detailseite* wird angezeigt. Im Abschnitt *Geräte* werden die Betriebssysteme von verwalteten Geräten für die Appliance oder für die ausgewählte Organisation angezeigt.
4. Klicken Sie im Abschnitt *Software* auf **Softwaretitel**.

Die Appliance führt einen Bericht aus, der die auf verwalteten Geräten installierte Software anzeigt. Siehe Informationen zu Berichten.

Abonnieren von Patches und Konfigurieren von Downloadeinstellungen

Sie können Patches abonnieren und Einstellungen für Patch-Downloads einrichten, um einen Patch-Workflow einzurichten.

Patches abonnieren

Sie können Patches für die Betriebssysteme und Anwendungen auf Ihren verwalteten Geräten abonnieren.

Ermitteln Sie vor dem Abonnieren und Herunterladen von Patches die Betriebssysteme und Anwendungen, die auf den verwalteten Geräten installiert sind, und überprüfen Sie die Patch-Anforderungen. Siehe Details zu Betriebssystemen und Anwendungen anzeigen.

1. Rufen Sie die Seite *Patch-Abonnementeinstellungen* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Sicherheit** und anschließend auf **Patch-Verwaltung**.
   c. Klicken Sie im Fensterbereich *Patch-Verwaltung* auf **Abonnements**.
2. Im Abschnitt *Patch-Status* finden Sie Details zum letzten Patch-Download sowie zum Speicherplatz der Appliance. Hier können Sie auch bestimmen, ob neu heruntergeladene Patches standardmäßig als aktiv oder inaktiv gekennzeichnet werden sollen.

Option	Beschreibung
Neue Patches aktivieren	Kennzeichnen Sie neue Patches als Aktiv. Mit dieser Einstellung werden Patches, die Ihren Abonnementeinstellungen entsprechen, nach jedem Herunterladen aktiviert. Wenn diese Option deaktiviert ist, werden neue Patches als Inaktiv

Option	Beschreibung
	gekennzeichnet. Auf diese Weise können Sie Patches vor deren Bereitstellung prüfen.

3. Geben Sie die *Abonnementeinstellungen* an. Welche Patches heruntergeladen werden, hängt von den im Abonnement angegebenen Betriebssystemen und Gebietsschemata ab.

Option	Beschreibung
Windows Betriebssysteme	Lädt Patches für die ausgewählten Windows Betriebssysteme herunter. Klicken Sie auf die Bearbeitungsschaltfläche, um die Betriebssystemliste zu bearbeiten: . Wählen Sie **Alle Windows PCs im Inventar** aus, um die Windows Betriebssysteme auf der Grundlage verwalteter Geräte auszuwählen. Sollen Patches für Windows Betriebssysteme ignoriert werden, wählen Sie **Deaktiviert** aus. Oder: Aktivieren Sie die Kontrollkästchen neben den gewünschten Windows Betriebssystemen. Die ausgewählten Elemente werden nach dem Speichern der Einstellungen angezeigt.
Mac Betriebssysteme	Lädt Patches für die ausgewählten Mac Betriebssysteme herunter. Klicken Sie auf die Bearbeitungsschaltfläche, um die Betriebssystemliste zu bearbeiten: . Wählen Sie **Alle Macs im Inventar** aus, um die Mac Betriebssysteme auf der Grundlage verwalteter Geräte auszuwählen. Sollen Patches für Mac Betriebssysteme ignoriert werden, wählen Sie **Deaktiviert** aus. Oder: Aktivieren Sie die Kontrollkästchen neben den gewünschten Mac Betriebssystemen. Die ausgewählten Elemente werden nach dem Speichern der Einstellungen angezeigt.
Gebietsschemata	Lädt Patches für die ausgewählten Sprachen herunter. Klicken Sie auf die Bearbeitungsschaltfläche, um die Gebietsschemaliste zu bearbeiten: . Wählen Sie **Alle Gebietsschemata** aus, um Patches unabhängig vom Gebietsschema herunterzuladen, oder aktivieren Sie die Kontrollkästchen neben den gewünschten Gebietsschemata. Die ausgewählten Elemente werden nach dem Speichern der Einstellungen angezeigt.

HINWEIS: Für ein Patch-Abonnement müssen mindestens ein Betriebssystem und ein Gebietsschema ausgewählt werden.

4. Geben Sie die Einstellungen für *Anwendungs-Patches* an. Mit diesen Einstellungen wird der Patch-Status nach dem Herunterladen der Patch-Dateien bestimmt. Mögliche Werte: "Aktiv", "Inaktiv" und "Deaktiviert".

Option	Beschreibung
Herausgeber	Mit dieser Option können Sie Anwendungs-Patches auf der Grundlage des Herstellers abonnieren. Klicken Sie auf die Bearbeitungsschaltfläche, um die gewünschten Typen auszuwählen: . Wählen Sie **Alle Herausgeber** aus, um Patches von allen verfügbaren Herausgebern auszuwählen. Oder: Aktivieren Sie die Kontrollkästchen neben den gewünschten Herausgebern. Die ausgewählten Elemente werden nach dem Speichern der Einstellungen angezeigt.

5. Geben Sie *erweiterte Optionen* für das Abonnement an.

Option	Beschreibung
Klassifizierung	Klicken Sie auf diese Option, und wählen Sie einen Abonnementtyp aus. Wählen Sie entweder **Alle Klassifizierungen** aus, um sie zu **deaktivieren**, oder klicken Sie auf **Klassifizierung auswählen**, und wählen Sie nach Bedarf einen oder mehrere der vorhandenen Werte aus: **Kritische Updates**, **Definitionsupdates**, **Feature Packs**, **Vollständige Software**, **Hotfix**, **Sicherheitsupdates**, **Service Packs**, **Tools**, **Updaterollups**, **Updates** und **Upgrades**.
Schweregrad	Klicken Sie auf diese Option, und wählen Sie einen Schweregrad für dieses Abonnement aus. Sie können **Alle Schweregrade** auswählen, um sie zu **deaktivieren**, oder auf **Schweregrad auswählen** klicken und einen oder mehrere der vorhandenen Werte auswählen, sofern zutreffend: **Kritisch**, **Hoch**, **Niedrig**, **Mittel** und **Empfohlen**.
Labels	Sie können ausschließlich die Patches herunterladen, die mit den ausgewählten Labels übereinstimmen. Klicken Sie auf **Verknüpfte Labels verwalten**, um die Labels auszuwählen. Dies ist von Bedeutung, wenn nur begrenzter Speicherplatz verfügbar ist. Wenn der insgesamt für die ausgewählten Patches erforderliche Speicherplatz den auf der Appliance verfügbaren Platz übersteigt, können keine Patches heruntergeladen werden. **HINWEIS:** Informationen zum Speicherplatz der Appliance werden oben auf der Seite im Abschnitt *Patch-Status* angezeigt.
Eingebettete Windows-Patches deaktivieren	Identifizieren und deaktivieren Sie eingebettete Windows-Patches. Ist diese Option gewählt, werden Signaturen für eingebettete Patches heruntergeladen, können jedoch nicht bereitgestellt werden, es sei denn, sie erfüllen Subskriptionskriterien.

Option	Beschreibung
Aktivierung von überholten Patches aufheben	Überholte Patches nach jedem Herunterladen mit dem Status *Inaktiv* kennzeichnen. Inaktive überholte Patches werden auf der Seite *Patch-Katalog* als **Inaktiv** gekennzeichnet.
Deaktivierte Patches erkennen	Damit kann die Appliance deaktivierte Patches beim Ausführen eines Erkennungs-Jobs ermitteln. Wenn diese Option ausgewählt wird, werden die Signaturen für deaktivierte Patches nur zur Erkennung heruntergeladen. Patches können nur bereitgestellt werden, wenn sie die Abonnementkriterien erfüllen.

6. Klicken Sie auf **Speichern**.

Ausgewählte Patches werden zum nächsten geplanten Download-Zeitpunkt automatisch heruntergeladen. Wenn ein Patch nach dem Herunterladen nicht mit den Abonnementeinstellungen übereinstimmt, wird es als **Deaktiviert** angezeigt. Wenn ein Patch zwar den Abonnementeinstellungen entspricht, aber überholt ist oder manuell deaktiviert wurde, erhält er den Status **Inaktiv**.

Download-Einstellungen für Patch- und Funktionsaktualisierungen auswählen

Die von Ihnen abonnierten Patches und Windows-Funktionsaktualisierungen werden entsprechend den von Ihnen ausgewählten Einstellungen auf die Appliance heruntergeladen.

Der erste Patch-Download beansprucht möglicherweise eine große Netzwerkbandbreite.

1. Rufen Sie die Seite *Download-Einstellungen für Patch- und Funktionsaktualisierungen* auf.
   - **Wenn die Organisationskomponente auf der Appliance nicht aktiviert ist, klicken Sie auf der linken Navigationsleiste auf** *Sicherheit***.**
   - **Wenn die Organisationskomponente für die Appliance aktiviert ist, melden Sie sich bei der Systemverwaltungskonsole der Appliance an: `https://appliance_hostname/system`. Oder wählen Sie in der Dropdown-Liste rechts oben auf der Seite den Eintrag System aus, und klicken Sie dann auf Einstellungen > Systemsteuerung.**
2. Klicken Sie auf *Download-Einstellungen für Patch- und Funktionsaktualisierungen*.
3. Wählen Sie im Abschnitt *Datei-Downloads konfigurieren* folgende Optionen aus:

Option	Beschreibung
Patchen:	• **Deaktiviert**: Verhindert das Herunterladen von Patch-Paketen. Dies beinhaltet die für die Installation der Patches erforderlichen Installationsprogramme. • **Alle abonnierten Dateien** Auf Ihrer Appliance können Sie einen Vollcache abonnierter Pakete verwalten. Mit dieser Option werden alle von Ihnen abonnierten Bereitstellungspakete heruntergeladen, ohne zu prüfen, ob diese für Ihre Umgebung erforderlich sind. Für einige Umgebungen muss ein Vollcache verwaltet werden. Wenn Sie beispielsweise die Option **Offlineziel** oder

Option	Beschreibung
	Onlinequelle auswählen, ist ein Vollcache erforderlich. • **Als fehlend erkannte Dateien** Die Appliance kann ermitteln, welche Pakete basierend auf den Ergebnissen von Erkennungs-Jobs heruntergeladen werden sollen. Wenn eine Patch-Erkennungssignatur auf einem verwalteten Gerät als nicht installiert erkannt wird, wird das Patch-Paket heruntergeladen. Wenn kein verwaltetes Gerät als nicht installiert erkannt wird, werden für dieses Patch keine Pakete heruntergeladen.
Funktionsaktualisierungen	• **Deaktiviert**: Verhindert das Herunterladen von Windows-Funktionsupdates. Dies beinhaltet die für die Installation der Patches erforderlichen Installationsprogramme. • **Als fehlend erkannte Dateien** Die Appliance kann ermitteln, welche Pakete basierend auf den Ergebnissen von Erkennungs-Jobs heruntergeladen werden sollen. Wenn eine Funktionsaktualisierungssignatur auf einem verwalteten Gerät als nicht gepatcht erkannt wird, wird das Paket für die Windows-Funktionsaktualisierung heruntergeladen. Wenn kein verwaltetes Gerät als nicht aktualisiert erkannt wird, werden für diese Windows-Funktionsaktualisierungen keine Pakete heruntergeladen.
Nicht verwendete Dateien löschen nach __ Tagen	Nicht bereitgestellte Patches und Windows-Funktionsupdates werden nach Ablauf der angegebenen Anzahl von Tagen gelöscht. Als *Inaktiv* oder *Deaktiviert* gekennzeichnete Patches und Windows-Funktionsaktualisierungen werden während des Patch-Downloadvorgangs automatisch gelöscht.
Offline-Aktualisierung	Die durchzuführende Aktion, wenn die Appliance zum geplanten Startzeitpunkt der Aktualisierung offline ist. Deaktivieren Sie das Kontrollkästchen *Offline-Aktualisierung*, wenn die Appliance mit dem Internet verbunden wird und Patches oder Windows-Funktionsaktualisierungen direkt herunterladen kann.
Offlineziel	Das Offlineziel, das verwendet werden soll, wenn die Appliance nicht mit dem Internet verbunden ist und Sie die Dateien für Patches und Windows-Funktionsaktualisierungen aus einem lokalen Verzeichnis hochladen möchten. Wenn Ihre Appliance mit dem Internet verbunden ist, können Sie diese als Offlinequelle konfigurieren. Dann können Sie die Patch-Dateien manuell aus der Dateifreigabe mit Patches der Offlinequelle in das

Option	Beschreibung
	folgende Verzeichnis am Offlineziel kopieren: `\\`**appliance_host**`\patches`. Klicken Sie zum Laden von TAR-Patch-Dateien auf **Hochladen**.
Onlinequelle	Gibt an, ob die Appliance als Quelle für eine andere Appliance verwendet wird. Wenn diese Option ausgewählt wird, werden die Patch-Dateien in die Dateifreigabe für Patches und Windows-Funktionsupdates der Appliance heruntergeladen.
Aktualisieren **Beschreibung** **Aktionen**	Für jeden Aktualisierungstyp (*Signatur*, *Dateien zur Funktionsaktualisierung*, *Patch-Dateien*) wird eine Beschreibung und der Zugriff auf die verfügbaren Aktionen bereitgestellt: • **Auf Update überprüfen**: Klicken Sie auf diese Option, um Patch-Signaturdateien herunterzuladen. • **Löschen**: Klicken Sie auf diese Option, um alle Patches oder Windows-Funktionsaktualisierungen umgehend von der Appliance zu entfernen. Das kann nützlich sein, wenn Sie keine Patches mehr benötigen und den von den Patches belegten Speicherplatz rasch zurückgewinnen möchten. • **Jetzt ausführen**: Klicken Sie auf diese Option, um die Patches oder Windows-Funktionsaktualisierungen, die Sie abonniert haben, unabhängig vom Abonnementplan sofort herunterzuladen.

4. Wählen Sie im Abschnitt *Planen* die Zeitplanoptionen für die Signaturen von Patches und Windows-Funktionsaktualisierungen aus. Dateisignaturen beinhalten die Sicherheitsbulletins sowie andere Dateien, die die über Quest heruntergeladenen Patches und Windows-Funktionsupdates definieren.

Option	Beschreibung
Signaturdownload	Durch Auswahl von **Keine** wird das Herunterladen von Signaturen für Patches und Windows-Funktionsupdates verhindert.
Alle __ Stunden	Lädt Signaturen in festgelegten Intervallen herunter. Verwenden Sie kurze Intervalle (4, 8 oder 12 Stunden) mit Bedacht, da sich hierdurch die Bandbreitenanforderungen erhöhen.
Jeden Tag zum festgelegten Zeitpunkt	Wählen Sie **Tag** aus, um Erkennungssignaturen für Patches oder Windows-Funktionsupdates jeden Tag herunterzuladen, oder wählen Sie einen Wochentag aus, um Signaturen einmal pro Woche herunterzuladen. Wählen Sie die Uhrzeit für den Beginn des Downloads aus. Die Uhrzeit wird im 24-Stunden-

Option	Beschreibung
	Format angezeigt, wobei 0 Uhr Mitternacht, 1:00 a.m. 01 Uhr nachts und 11:00 p.m. 23 Uhr entspricht. **HINWEIS:** Beim Einrichten von Downloads für Patches oder Windows-Funktionsupdates ist die Uhrzeit wichtig. Das Aktivitätsprotokoll der Appliance wird um 1:30 Uhr erstellt und Wartungsaufgaben werden zwischen 01:00 und 01:30 Uhr ausgeführt. Quest empfiehlt, Patch-Downloads nach Abschluss der Protokoll- und Wartungsaufgaben, also etwa um 3:00 Uhr, zu planen.
Am n-ten jedes Monats oder eines bestimmten Monats um HH:MM	Wählen Sie den Tag des Monats aus, an dem Erkennungssignaturen für Patches oder Windows-Funktionsupdates monatlich heruntergeladen werden sollen.

5. Legen Sie die Zeitplanoptionen für Funktionsaktualisierungs- und Patch-Dateien fest:

Option	Beschreibung
Nach Signaturdownload	Pakete werden nach dem Herunterladen der Signaturen heruntergeladen. Diese Option ist nicht verfügbar, wenn **Patchen** im Bereich *Dateidownloads konfigurieren* deaktiviert wurde.
Alle __ Minuten	Legt die Häufigkeit fest, mit der Pakete heruntergeladen werden. Diese Option ist nur verfügbar, wenn die Option *Als fehlend erkannte Dateien* im Bereich *Dateidownloads konfigurieren* ausgewählt wurde.
Zeitfenster für Aussetzung von Download: Start __ Ende __	Legt einen Zeitraum fest, in dem keine Dateien heruntergeladen werden können. Beispielsweise könnten Sie eine Beendigungszeit am frühen Morgen verwenden, damit durch den Vorgang während der regulären Arbeitszeit nicht übermäßig viel Netzwerkbandbreite beansprucht wird. Wenn Sie diese Option auswählen, beendet die Appliance Dateidownloads zur angegebenen Zeit. Dateidownloads werden erst wieder zum nächsten angegebenen Zeitpunkt gestartet. Wenn der Download wieder aufgenommen wird, wird er an der Stelle fortgesetzt, an der er unterbrochen wurde. Nicht abgeschlossene Downloads werden auf der Seite *Patch-Katalog* oder *Windows Feature Update Catalog (Katalog mit Windows-Funktionsupdates)* möglicherweise nicht angezeigt.

6. Klicken Sie auf **Speichern**.

Informationen zum Planen der Patch-Erkennung und -Bereitstellung für verwaltete Geräte finden Sie unter Erstellen und Verwalten von Patch-Zeitplänen. Informationen dazu, wie Sie Erkennung und Bereitstellung von Windows-Funktionsaktualisierungen für verwaltete Windows 10 Geräte zeitlich planen, finden Sie unter Zeitpläne für Windows-Funktionsaktualisierungen konfigurieren.

Anzeigen von verfügbaren Patches und Download-Status

Sie können die verfügbaren Patches prüfen und entsprechende Filter zum Herunterladen von Patches festlegen, sodass nur die benötigten Patches heruntergeladen werden.

Sobald die Patch-Pakete heruntergeladen wurden, können Sie einen Filter festlegen, um Patches nach Kategorie anzuzeigen. Zeigen Sie beispielsweise nur Betriebssystem-Patches an.

Verfügbare Patches anzeigen

Nach dem Abonnieren und Herunterladen von Patches können Sie die verfügbaren Patches anzeigen.

Zum Anzeigen von Patches müssen Sie Signaturen für die Patch-Erkennung abonnieren und Einstellungen für den Patch-Download auswählen. Siehe:

- Patches abonnieren
- Download-Einstellungen für Patch- und Funktionsaktualisierungen auswählen

1. Rufen Sie die Liste *Patch-Katalog* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Sicherheit** und anschließend auf **Patch-Verwaltung**.
   c. Klicken Sie im Fensterbereich *Patch-Verwaltung* auf **Katalog**.
2. Suchen Sie nach Anwendungs-Patches.
   a. Klicken Sie oberhalb der Liste auf der rechten Seite auf die Registerkarte **Erweiterte Suche**, um den Bereich *Erweiterte Suche* anzuzeigen.
   b. Geben Sie Suchkriterien ein:

   ```
   Patch-Listeninformationen: Kategorie | ist | Anwendung
   ```

   c. Klicken Sie auf **Suchen**.

Patch-Download-Status anzeigen

Nachdem Sie Patches abonniert haben, können Sie den Status des Patch-Downloads anzeigen.

Sie müssen Patches abonnieren, um den Status von Patch-Downloads anzeigen zu können. Siehe Patches abonnieren.

1. Rufen Sie die Liste *Patch-Katalog* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Sicherheit** und anschließend auf **Patch-Verwaltung**.

c. Klicken Sie im Fensterbereich *Patch-Verwaltung* auf **Katalog**.

2. Führen Sie einen der folgenden Schritte aus:

   - **Wählen Sie in der Dropdown-Liste** *Anzeigen nach* **rechts über der Tabelle die Option Download-Status > Heruntergeladen oder Download-Status > Nicht heruntergeladen aus.**
   - **Klicken Sie über der Tabelle auf der rechten Seite auf die Registerkarte Erweiterte Suche und wählen Sie dann die Suchkriterien aus. Beispiel:**

     `Patch-Listeninformationen: Download-Status | ist | Heruntergeladen`

Siehe Anzeigen von Patch-Informationen.

Best Practices für die Behebung von Problemen mit Patch-Abonnements

Gelegentlich kann eine Fehlermeldung angezeigt werden, dass Ihre Patch-Abonnementlizenz abgelaufen ist:

Die Fehlermeldung

```
Ihr Patch-Abonnement ist abgelaufen. Wenden Sie sich an den Support, um
Unterstützung zu erhalten.
```

Bevor Sie den Kace Support einschalten, können Sie einige vorbereitende Schritte durchführen, um das Problem zu lösen.

Dieser Fehler könnte durch einen der folgenden Fehler bewirkt worden sein:

- In den meisten Fällen geschieht dies, wenn der dreijährige Validierungszeitraum für Ihren Lizenzschlüssel abgelaufen ist.
- Ein neuer Lizenzschlüssel wird bereitgestellt, aber das Konto wurde eventuell noch nicht mit der KACE-Datenbank synchronisiert.

Wenn ein neuer Schlüssel angefordert, aber noch nicht zugestellt wurde:

Stellen Sie sicher, dass die folgende E-Mail-Nachricht nicht durch einen Spamfilter aussortiert wurde. Dies ist das Nachrichtenformat der vom KACE Lizenzteam gesendeten neuen Lizenzschlüsselbenachrichtigung:

`Absender: license@quest.com`

`Betreff:` **KACE Systemverwaltungs-Appliance** `Lizenznummer für (PO# <Bestellnummer>) Order# <Auftragsnummer>`

Wenn ein neuer Schlüssel angewendet wurde, aber der Fehler weiterhin auftritt:

1. Überprüfen Sie Ihre Produktlizenz:
   a. Navigieren Sie zur *Systemsteuerung* der Appliance.
      - Wenn die Organisationskomponente auf der Appliance nicht aktiviert ist, klicken Sie auf **Einstellungen**.
      - Wenn die Organisationskomponente für die Appliance aktiviert ist, melden Sie sich bei der Appliance an: **Systemverwaltungskonsole**, `http://`**appliance_hostname**`/system`. Oder wählen Sie in der Dropdown-Liste rechts oben auf der Seite den Eintrag **System** aus, und klicken Sie dann auf **Einstellungen**.

   b. Klicken Sie auf der linken Navigationsleiste auf **Appliance-Aktualisierungen**, um die Seite *Appliance-Aktualisierungen* anzuzeigen.
   c. Klicken Sie auf der rechten Seite der *Lizenzinformationen* auf ?.
   d. Wählen Sie *Lizenz validieren* aus und klicken Sie dann zum Bestätigen auf **Ja**.

   TIPP: Komplette Informationen zu dieser Seite finden Sie unter Lizenzschlüssel der Appliance aktualisieren.

2. Führen Sie einen manuellen Patchsignatur-Download durch.
   a. Rufen Sie die Seite *Patch-Downloadeinstellungen* der Appliance auf:
      - Wenn die Organisationskomponente auf der Appliance nicht aktiviert ist, klicken Sie auf **Einstellungen**.
      - Wenn die Organisationskomponente für die Appliance aktiviert ist, melden Sie sich bei der Appliance an: `http://`**appliance_hostname**`/system`. Oder wählen Sie in der Dropdown-Liste rechts oben auf der Seite den Eintrag **System** aus, und klicken Sie dann auf **Einstellungen**.
      - Gehen Sie zu **SecurityPatch** > **Patch-Verwaltung** > **Download-Einstellungen für Patches**.
   b. Klicken Sie auf **Jetzt ausführen**. Nachdem der Patch-Download abgeschlossen ist, wird die Fehlermeldung ausgeblendet.

      TIPP: Komplette Informationen zu dieser Seite finden Sie unter Download-Einstellungen für Patch- und Funktionsaktualisierungen auswählen.

Wenn Sie den obigen Schritt abgeschlossen haben, aber das Problem weiterhin besteht:

1. Gehen Sie zu https://support.quest.com/create-service-request und erstellen Sie eine neue Serviceanfrage (SR).
2. Geben Sie die Antworten auf die folgenden Fragen in der Anfrage an:
   - Wann trat das Problem erstmals auf?
   - Gab es irgendeine Änderung, bevor das Problem auftrat?
   - Überprüfen und bestätigen Sie das Problem im Patch-Download-Protokoll. Dokumentieren Sie die Ergebnisse in der SA (Serviceanfrage) oder laden Sie die Protokolldateien in die SA hoch.
   - Welcher Lizenzschlüssel wird derzeit verwendet? Der vollständige Lizenzschlüssel ist erforderlich. Wenn dies nicht möglich ist, sind die letzten fünf Zeichen zulässig.
   - Was ist der alte (vorherige) Lizenzschlüssel (falls verfügbar)?
   - Was ist die statische IP-Adresse der Appliance?
   - Was ist die MAC-Adresse der Appliance?
3. Laden Sie Ihre Appliance-Protokolldateien als Anhang zur Serviceanfrage (SR) hoch.
   a. Navigieren Sie zur *Systemsteuerung* der Appliance.
      - Wenn die Organisationskomponente auf der Appliance nicht aktiviert ist, klicken Sie auf **Einstellungen**.
      - Wenn die Organisationskomponente für die Appliance aktiviert ist, melden Sie sich bei der Appliance an: **Systemverwaltungskonsole**, `http://`**appliance_hostname**`/system`. Oder wählen Sie in der Dropdown-Liste rechts oben auf der Seite den Eintrag **System** aus, und klicken Sie dann auf **Einstellungen**.
   b. Klicken Sie in der linken Navigationsleiste auf **Support**.
   c. Klicken Sie im Abschnitt *Tools zur Fehlerbehebung* auf **Appliance-Aktivitätsprotokolle abrufen**.
   d. Klicken Sie auf **Datei speichern**, um die Protokolle herunterzuladen.

HINWEIS: Löschen Sie den Cache des Browsers, nachdem Sie einen Fehler beim Herunterladen eines Patches erhalten haben. Andernfalls kann das Gerät nach dem Auftreten dieses Fehlers keine Patches herunterladen.

Erstellen und Verwalten von Patch-Zeitplänen

Sie können Patch-Zeitpläne verwalten, die abonnierte Patches erkennen, bereitstellen und zurücksetzen (Rollback).

Informationen zum Abonnieren von Patches finden Sie unter Abonnieren und Herunterladen von Patches.

Informationen zum Planen von kritischen Betriebssystem-Patches für Desktops und Server

Sie können die Appliance so konfigurieren, dass kritische Betriebssystem-Patches gemäß einem Zeitplan auf Desktops und Servern installiert werden.

Desktops sind weniger kritisch als Server und weniger mobil als Notebooks. Dadurch sind deren Patches einfacher zu planen. Normalerweise können Sie routinemäßige Aktualisierungen für den frühen Morgen einplanen, bevor die Benutzer eintreffen.

Auf Servern werden kritische Dienste ausgeführt, die Ihre Organisation benötigt. Planen Sie das Patchen der Server im Voraus und warnen Sie Benutzer bezüglich der vorübergehenden Dienstausfälle, die durch das Patchen auftreten. Führen Sie Server-Patches früh morgens oder zu einer anderen Zeit aus, in der die geringste Anzahl von Benutzern die Serverressourcen benötigt.

Workflow für kritische Betriebssystem-Patches für Desktops und Server

Der Workflow umfasst die Identifizierung von Geräten und Patches, die Planung von Aktionen sowie die Bereitstellung der Patches.

- **Desktops ermitteln**: Erstellen Sie ein Smart Label, das alle Geräte identifiziert, bei denen es sich um Desktops handelt. Damit werden Server und Notebooks ausgeschlossen. Siehe Smart Labels für Desktops hinzufügen.
- **Server ermitteln**: Erstellen Sie ein Smart Label, das alle Server identifiziert. Siehe Smart Labels für Server hinzufügen.
- **Kritische Betriebssystem-Patches ermitteln**: Erstellen Sie ein Smart Label, das alle kritischen Betriebssystem-Patches identifiziert. Siehe Smart Labels für kritische Betriebssystem-Patches hinzufügen.
- **Erkennungs- und Bereitstellungsaktionen planen**: Planen Sie einen Erkennungs- und Bereitstellungsjob, mit dem angegeben wird, ob die Geräte im Smart Label aktualisiert werden müssen, mit dem für die Geräte kritische Patches bereitgestellt werden und mit dem ggf. ein Neustart erzwungen wird. Siehe Konfigurieren von Patch-Zeitplänen.
- **Patches auf einzelnen Servern bereitstellen**: Planen Sie einen Job, mit dem Patches auf Servern nach Bedarf bereitgestellt werden. Siehe Konfigurieren von Patch-Zeitplänen.
- **Benutzer benachrichtigen**: Achten Sie darauf, dass Sie beim Planen von Patches Benutzer über den Zeitplan informieren, sodass diese wissen, wann die von ihnen verwendeten Geräte gepatcht werden. Das ist besonders wichtig, wenn Geräte neu gestartet werden müssen und im Rahmen des Patch-Vorgangs möglicherweise nicht verfügbar sind. Die Benachrichtigung der Benutzer kann per E-Mail oder über einen

anderen Nachrichtendienst außerhalb der Appliance-Administratorkonsole erfolgen. Siehe Best Practices für den Patch-Vorgang.

Informationen zum Planen von kritischen Patches für Notebooks

Da Notebooks oft ausgeschaltet oder vom Netzwerk getrennt sind, ist es schwierig, eine günstige Zeit für das Patchen zu finden. Meist werden Notebooks am Beginn des Arbeitstags oder über die Mittagszeit gepatcht.

Die meisten Kunden von Quest KACE verwenden für das Patchen ihrer Notebooks zwei Zeitpläne, einen für das Erkennen und einen für das Bereitstellen.

Workflow für kritische Patches für Notebooks

Der Workflow zum Anwenden kritischer Patches auf Notebooks umfasst die Identifizierung von Geräten und Patches, die Planung von Aktionen sowie die Bereitstellung der Patches.

Die Einrichtung von Aktionen für die automatische Erkennung und Bereitstellung umfasst folgende Schritte:

- **Kritische Patches ermitteln**: Erstellen Sie ein Smart Label für Patches, mit dem kritische Patches für Notebooks automatisch ermittelt werden. Siehe Smart Labels für Patches verwenden.
- **Erkennungsaktionen planen**: Erstellen Sie einen Zeitplan, mit dem regelmäßig kritische Patches für Notebooks erkannt werden, und führen Sie ihn aus. Siehe Konfigurieren von Patch-Zeitplänen.
- **Bereitstellungsaktionen planen**: Erstellen Sie einen Zeitplan, mit dem regelmäßig kritische Patches für Notebooks bereitgestellt werden, und führen Sie ihn aus. Siehe Konfigurieren von Patch-Zeitplänen.
- **Patch-Status überprüfen**: Überprüfen Sie regelmäßig den Patch-Status mithilfe von Berichten und dem Patch. Siehe Anzeigen von Patch-Zeitplänen, -Status und -Berichten.
- **Benutzer benachrichtigen**: Informieren Sie Benutzer über den Patch-Zeitplan. Benachrichtigen Sie Benutzer, indem Sie ihnen eine E-Mail senden oder einen anderen Nachrichtendienst außerhalb der **Administratorkonsole** der Appliance verwenden. Weitere Informationen finden Sie in Best Practices für den Patch-Vorgang unter "Benachrichtigen von Benutzern beim Patchen von Geräten".

Informationen zum Planen von nicht kritischen Patches

Sie können die Appliance so konfigurieren, dass nicht kritische Patches gemäß einem Zeitplan installiert werden.

So planen Sie nicht kritische Patches

- **Patches erkennen**: Erstellen Sie einen Patch-Zeitplan zum Erkennen von Patches auf allen Geräten, um den Umfang des Patch-Jobs festzulegen. Siehe Konfigurieren von Patch-Zeitplänen.
- **Patches deaktivieren**: Wenn Patches vorhanden sind, die nicht bereitgestellt werden sollen, kennzeichnen Sie diese als **Inaktiv**.
- **Patches testen**: Erstellen Sie einen Zeitplan, mit dem Patches für Ihre Testgeräte erkannt und bereitgestellt werden. Siehe Konfigurieren von Patch-Zeitplänen.
- **Betriebssystem-Patches für Desktops und Server ermitteln**: Erstellen Sie ein Smart Label für Patches, mit dem die Patches für Server automatisch erfasst werden. Siehe Smart Labels für Patches verwenden.
- **Patches für Desktops und Server erkennen und bereitstellen** (siehe Konfigurieren von Patch-Zeitplänen):
  - Erstellen Sie einen Zeitplan, mit dem regelmäßig Patches für Ihre Desktops erkannt und bereitgestellt werden.
  - Erstellen Sie einen Zeitplan, mit dem regelmäßig Patches für Ihre Server erkannt und bereitgestellt werden.
- **Patches für Notebooks erkennen und bereitstellen** (siehe Konfigurieren von Patch-Zeitplänen):
  - Erstellen Sie einen Zeitplan, mit dem regelmäßig Patches für Ihre Notebooks erkannt werden.
  - Erstellen Sie einen Zeitplan, mit dem regelmäßig Patches für Ihre Notebooks bereitgestellt werden.
- **Patch-Status überprüfen**: Überprüfen Sie den Patch-Status regelmäßig. Siehe Anzeigen von Patch-Zeitplänen, -Status und -Berichten.

Konfigurieren von Patch-Zeitplänen

Sie können Patch-Zeitpläne erstellen und konfigurieren sowie einen Zeitpunkt für ihre Ausführung festlegen. Patch-Zeitpläne wirken sich nicht auf verwaltete Installationen oder andere Verteilungen aus.

Felder auf den Detailseiten des Patch-Zeitplans

Über die Felder im Assistenten für *Zeitplandetails* und auf der Seite *Zeitplandetails* können Sie Patch-Aktionen konfigurieren und planen.

Allgemeine Informationen

Option	Beschreibung
Name	Ein Name, der den Zeitplan genau bezeichnet. Dieser Name wird auf der Seite *Patch-Zeitpläne* angezeigt.
Beschreibung	Eine kurze Beschreibung des Patch-Zeitplans.

Aktionsbereich

Die Aktion, die mit dem Patch-Zeitplan verknüpft ist.

Das Verhalten der Patch-Aktion hängt von der Kombination der Auswahl für Neustart, Bereitstellung und Rollback ab. Wenn bei einer Patch-Aktion sowohl eine Erkennung als auch weitere Aktionen durchgeführt werden, wie beispielsweise bei Erkennen und bereitstellen und Erkennen und Rollback durchführen, wird die Aktion regelmäßig wiederholt, bis bei der Erkennung keine Patches mehr gefunden werden, für die eine Bereitstellung oder ein Rollback erforderlich ist. Dieses Verhalten kann bei einer einzigen geplanten Ausführung mehrere

Neustartaktionen zur Folge haben. Zudem bestimmt der Typ des Geräts, das Sie patchen, den Typ der zu verwendenden Patch-Aktion.

Folgende Aktionen sind verfügbar:

- **Erkennen**: Erkennt Patches, die auf verwalteten Geräten installiert sind oder auf diesen fehlen. Aktionen vom Typ "Nur erkennen" werden empfohlen, wenn in den *Einstellungen für Patch-Download* nur das Herunterladen konfiguriert wird. Beim Ausführen einer Aktion, bei der nur eine Erkennung erfolgt, wird vor der Bereitstellung eine Liste der Patch-Dateien erstellt, die heruntergeladen werden müssen, bevor die Bereitstellung gestartet wird.
- **Erkennen und zur Verfügung stellen**: Erkennt Patches, die auf verwalteten Geräten installiert sind oder fehlen, und lädt Patch-Dateien zur späteren Bereitstellung auf das Agent-Gerät herunter.
- **Erkennen und bereitstellen**: Erkennt Patches für verwaltete Geräte und stellt sie auf diesen bereit. Diese Arten von Aktionen werden bei der Verwaltung von Desktops und Servern verwendet. Für Patch-Jobs für die Erkennung und Bereitstellung ist eine Verbindung zwischen dem Gerät und der Appliance erforderlich, da diese nicht offline ausgeführt werden können. Weitere Informationen zu Messaging-Protokoll-Verbindungen finden Sie unter Agentenkommunikation und Protokolleinstellungen konfigurieren.
- **Detect, Stage and On-demand Deploy (Erkennen, zur Verfügung stellen und bedarfsgerecht bereitstellen)**: Erkennt Patches, die auf verwalteten Geräten installiert sind oder fehlen, lädt Patch-Dateien auf das Agent-Gerät herunter. In der Windows-Taskleiste auf dem Agent-Gerät wird daraufhin eine Benachrichtigung angezeigt, dass die Patches bereit für die Bereitstellung sind. Der Benutzer kann dann den Bereitstellungsvorgang nach Belieben initiieren.
  - Diese Zeitpläne sind nur für Windows-Geräte mit Agenten der Version 11.0 oder höher verfügbar.
  - Die Option *Agentenstatussymbol auf Gerät* muss in den Kommunikationseinstellungen des Agenten aktiviert sein. Diese Einstellungen finden Sie auf der Seite *Organisationsdetails*, unter *Kommunikations- und Agenteneinstellungen* (falls eine oder mehrere Organisationskomponenten aktiviert sind) oder auf der Seite *Kommunikationseinstellungen* (falls Sie über keine Organisationskomponente verfügen). Weitere Informationen hierzu finden Sie unter Agentenkommunikation und Protokolleinstellungen konfigurieren.
- **Bereitstellen**: Stellt anwendbare Patches auf verwalteten Geräten bereit. Das ist nützlich, wenn Sie wissen, dass bestimmte Patches auf verwalteten Geräten bereitgestellt werden müssen. Ein Job vom Typ "Erkennen" wird abschließend ausgeführt, nachdem das Patch bereitgestellt wurde oder, falls ein Neustart erforderlich ist, nachdem das Gerät neu gestartet wurde und der Agent erneut eine Verbindung mit der Appliance hergestellt hat.
- **Erkennen und Rollback durchführen**: Erkennt und entfernt unerwünschte Patches von verwalteten Geräten. Für manche Patches sind möglicherweise keine Rollbacks verfügbar. Siehe Ermitteln, ob für ein Patch ein Rollback möglich ist.
- **Rollback**: Entfernt unerwünschte Patches von verwalteten Geräten. Für manche Patches sind möglicherweise keine Rollbacks verfügbar. Siehe Ermitteln, ob für ein Patch ein Rollback möglich ist.

Abschnitt "Erkennen"

Option	Beschreibung
Alle Patches	Erkennt alle verfügbaren Patches. Dieser Vorgang kann viel Zeit beanspruchen. Außerdem erkennt er möglicherweise Patches für Software, die nicht auf verwalteten Geräten installiert ist oder nicht von ihnen benötigt wird. Wenn verwaltete Geräte beispielsweise Antivirenprogramme von nur einem Hersteller verwenden, müssen Patches für alle anderen Hersteller von Antivirenprogrammen nicht erkannt werden. Mit *Alle Patches* werden jedoch alle fehlenden Patches erkannt, unabhängig davon, ob sie von verwalteten Geräten benötigt werden. Um die Patch-Erkennung zu optimieren, richten

Option	Beschreibung
	Sie Labels für die Patches ein, die erkannt werden sollen, und verwenden dann die Option *Patch-Labels*.
Patch-Labels	Die Aktion wird auf die Patches beschränkt, die das von Ihnen ausgewählte Label aufweisen. Diese Option wird am häufigsten verwendet. 1. Klicken Sie auf **Verknüpfte Labels verwalten**. 2. Ziehen Sie im daraufhin angezeigten Dialogfeld *Labels auswählen* (falls zutreffend) mindestens ein Label in den Bereich *Erkennung begrenzen auf*, und klicken Sie dann auf **OK**. Um diese Option verwenden zu können, müssen bereits Smart Labels für die entsprechenden Patches vorhanden sein. Siehe Smart Labels für Patches verwenden.
Select from suggested criteria (Aus vorgeschlagenen Kriterien auswählen)	Wählt einen Patch mit vordefinierten Kriterien aus. So können Sie sich auf eine bestimmte Art von Patch basierend auf Ihrem Betriebssystem konzentrieren. Sie können beispielsweise die kritischen Windows-Patches auswählen, die in den letzten 30 Tagen veröffentlicht wurden. 1. Klicken Sie auf **Select from suggested criteria (Aus vorgeschlagenen Kriterien auswählen)**. 2. Das Dialogfeld *Select Suggested Criteria (Vorgeschlagene Kriterien auswählen)* wird angezeigt. Klicken Sie auf **Select Suggested Criteria (Vorgeschlagene Kriterien auswählen)** und dann auf **Speichern**.
Erkennungstimeout	Die Zeitdauer bis zum Abschluss der Patching-Aktion in Stunden.

Abschnitt "Bereitstellen"

Option	Beschreibung
Alle Patches	Stellt alle Patches auf den ausgewählten Geräten bereit.
Patch-Labels	Die Aktion wird auf die Patches beschränkt, die das von Ihnen ausgewählte Label aufweisen. Diese Option wird am häufigsten verwendet. 1. Klicken Sie auf **Verknüpfte Labels verwalten**. 2. Das Dialogfeld *Labels auswählen* wird angezeigt. Ziehen Sie mindestens ein Label nach Bedarf in den Bereich *Bereitstellung begrenzen auf*, und klicken Sie dann auf **OK**.

Option	Beschreibung
	Um diese Option verwenden zu können, müssen bereits Smart Labels für die entsprechenden Patches vorhanden sein. Siehe Smart Labels für Patches verwenden.
Select from suggested criteria (Aus vorgeschlagenen Kriterien auswählen)	Wählt einen Patch mit vordefinierten Kriterien aus. So können Sie sich auf eine bestimmte Art von Patch basierend auf Ihrem Betriebssystem konzentrieren. Sie können beispielsweise die kritischen Windows-Patches auswählen, die in den letzten 30 Tagen veröffentlicht wurden. 1. Klicken Sie auf **Select from suggested criteria (Aus vorgeschlagenen Kriterien auswählen)**. 2. Das Dialogfeld *Select Suggested Criteria (Vorgeschlagene Kriterien auswählen)* wird angezeigt. Klicken Sie auf **Select Suggested Criteria (Vorgeschlagene Kriterien auswählen)** und dann auf **Speichern**.
Maximale Anzahl Bereitstellungsversuche	Die maximale Anzahl der Versuche, die das Gerät bereitstellt oder für die es ein Rollback des Patch durchführt. Geben Sie eine Zahl zwischen eins (1) und zehn (10) an. Wenn Sie Null (0) angeben, wird die Bereitstellung oder das Rollback nicht ausgeführt. Ein Wert über zehn (10) führt zu einer Fehlermeldung. In einem letzten Schritt überprüft die Appliance bei der Patch-Bereitstellung oder dem Rollback, ob das Patch erfolgreich bereitgestellt oder das Rollback erfolgreich ausgeführt wurde. Wenn bei einer Bereitstellung oder einem Rollback ein Fehler auftritt, versucht die Appliance, das Patch erneut bereitzustellen oder das Rollback für das Patch erneut auszuführen, bis eines der folgenden Ereignisse eintritt: • Die Bereitstellung oder das Rollback ist erfolgreich. • Die maximale Anzahl an Versuchen wird erreicht. • Die geplante Bereitstellungs- oder Rollback-Dauer endet und der Patch-Vorgang wird angehalten.
Bereitstellungstimeout	Die Zeitdauer bis zum Abschluss der Patching-Aktion in Stunden.

Abschnitt "Rollback"

Option	Beschreibung
Alle Patches	Führt ein Rollback für alle Patches auf den ausgewählten Geräten durch.

Option	Beschreibung
Patch-Labels	Die Aktion wird auf die Patches beschränkt, die das von Ihnen ausgewählte Label aufweisen. Diese Option wird am häufigsten verwendet. 1. Klicken Sie auf **Verknüpfte Labels verwalten**. 2. Das Dialogfeld *Labels auswählen* wird angezeigt. Ziehen Sie mindestens ein Label nach Bedarf in den Bereich *Rollback begrenzen auf*, und klicken Sie dann auf **OK**. Um diese Option verwenden zu können, müssen bereits Smart Labels für die entsprechenden Patches vorhanden sein. Siehe Smart Labels für Patches verwenden.
Select from suggested criteria (Aus vorgeschlagenen Kriterien auswählen)	Wählt einen Patch mit vordefinierten Kriterien aus. So können Sie sich auf eine bestimmte Art von Patch basierend auf Ihrem Betriebssystem konzentrieren. Sie können beispielsweise die kritischen Windows-Patches auswählen, die in den letzten 30 Tagen veröffentlicht wurden. 1. Klicken Sie auf **Select from suggested criteria (Aus vorgeschlagenen Kriterien auswählen)**. 2. Das Dialogfeld *Select Suggested Criteria (Vorgeschlagene Kriterien auswählen)* wird angezeigt. Klicken Sie auf **Select Suggested Criteria (Vorgeschlagene Kriterien auswählen)** und dann auf **Speichern**.
Maximale Anzahl Rollback-Versuche	Die maximale Anzahl der Versuche für die Bereitstellung oder das Rollback des Patches durch die Appliance (zwischen 0 und 99). Wenn Sie 0 angeben, versucht die Appliance unbegrenzt, das Patch bereitzustellen oder ein Rollback für das Patch auszuführen. In einem letzten Schritt überprüft die Appliance bei der Patch-Bereitstellung oder dem Rollback, ob das Patch erfolgreich bereitgestellt oder das Rollback erfolgreich ausgeführt wurde. Wenn bei einer Bereitstellung oder einem Rollback ein Fehler auftritt, versucht die Appliance, das Patch erneut bereitzustellen oder das Rollback für das Patch erneut auszuführen, bis eines der folgenden Ereignisse eintritt: • Die Bereitstellung oder das Rollback ist erfolgreich. • Die maximale Anzahl an Versuchen wird erreicht. • Die geplante Bereitstellungs- oder Rollback-Dauer endet und der Patch-Vorgang wird angehalten.

Option	Beschreibung
Bereitstellungstimeout	Die Zeitdauer bis zum Abschluss der Patching-Aktion in Stunden.

Abschnitt "On-demand Deployment Timeout Settings" (Timeout-Einstellungen für bedarfsgerechte Bereitstellung)

Option	Beschreibung
Automatically Deploy After (Automatische Bereitstellung nach)	Die Zeit, nach der die Bereitstellung stattfindet, wenn das Agent-Gerät keine Eingaben vom Benutzer erhält.

Abschnitt "Geräte"

Option	Beschreibung
Alle Geräte	Wählen Sie diese Optionen aus, um diesen Zeitplan auf alle verwalteten Geräte anzuwenden. Deaktivieren Sie das Kontrollkästchen, um die Bereitstellung auf bestimmte Labels oder Geräte zu beschränken.
Gerätelabels	Die Aktion wird auf die Patches beschränkt, die das von Ihnen ausgewählte Label aufweisen. Diese Option wird am häufigsten verwendet. 1. Klicken Sie auf **Verknüpfte Labels verwalten**. 2. Das Dialogfeld *Labels auswählen* wird angezeigt. Ziehen Sie mindestens ein Label nach Bedarf in den Bereich *Ausführung begrenzen auf*, und klicken Sie dann auf **OK**. Um diese Option verwenden zu können, müssen bereits Smart Labels für die entsprechenden Patches vorhanden sein. Siehe Smart Labels für Patches verwenden.
Geräte	Führt auf den von Ihnen ausgewählten Geräten Patch-Aktionen aus. • Um nach Geräten zu suchen, beginnen Sie mit einer entsprechenden Eingabe in das Feld. • Um alle angegebenen Geräte zu entfernen und erneut zu starten, klicken Sie auf **Alle entfernen**. • Benutzer mit eingeschränkten Zugriffsrechten sehen nur die Geräte, die mit ihrer Rolle verknüpft sind, wenn der Rolle ein Label zugewiesen ist. Weitere Informationen zu Benutzerrollen finden Sie unter Benutzerrollen hinzufügen oder bearbeiten.
Betriebssysteme	Wählen Sie die Betriebssysteme der Geräte aus, für die der Patch bereitgestellt werden soll. Die

Option	Beschreibung
	Standardeinstellung für diese Option sind alle Betriebssysteme. Wenn diese Option konfiguriert ist, gilt der Zeitplan nur für Geräte mit den ausgewählten Betriebssystemen. 1. Klicken Sie auf **Betriebssysteme verwalten**. 2. Wählen Sie im daraufhin angezeigten Dialogfeld **Betriebssysteme** die Betriebssystemversionen in der Navigationsstruktur aus. Sie haben die Möglichkeit, Betriebssystemversionen nach Familie, Produkt, Architektur, Versions-ID oder Build-Version auszuwählen. Je nach Bedarf können Sie eine bestimmte Build-Version oder einen übergeordneten Knoten auswählen. Wenn Sie einen übergeordneten Knoten im Baum auswählen, werden die zugehörigen untergeordneten Knoten automatisch mit ausgewählt. Aufgrund dieses Verhaltens können Sie beliebige zukünftige Betriebssystemversionen auswählen, da Geräte in Ihrer verwalteten Umgebung hinzugefügt oder aktualisiert werden. Wenn Sie beispielsweise alle aktuellen und zukünftigen Versionen auswählen möchten, die mit der Windows 10 x64-Architektur verbunden sind, wählen Sie unter Windows > **Windows 10** die Option **x64** aus.

Abschnitt "Benachrichtigen"

Option	Beschreibung
Optionen	Die Benachrichtigungen, die den Benutzern bei der Ausführung von Patch-Aktionen angezeigt werden. Wenn Sie die Aktion ohne Benachrichtigung des Benutzers ausführen möchten, lassen Sie das Feld *Optionen* leer. • **OK**: Sofort ausführen. • **Abbrechen**: Abbrechen bis zur nächsten geplanten Ausführung. • **Snooze**: Der Benutzer erhält nach Ablauf der *Snooze-Dauer* erneut eine Eingabeaufforderung.
Timeout	Die Zeitspanne in Minuten, für die das Dialogfeld angezeigt werden soll, bevor eine Aktion ausgeführt wird. Wenn diese Zeitspanne verstreicht, ohne dass der Benutzer auf eine Schaltfläche klickt, führt die Appliance die in der Dropdown-Liste *Timeout* angegebene Aktion aus.

Option	Beschreibung
Timeout-Aktion	Die Aktion, die ausgeführt werden soll, wenn die Zeitspanne für den **Timeout** abgelaufen ist, ohne dass der Benutzer eine Option ausgewählt hat.
Snooze-Dauer	Die Wartezeit in Minuten, nachdem der Benutzer auf **Snooze** geklickt hat. Nach Ablauf dieser Zeit erscheint das Dialogfeld erneut.
Limit für "Snooze bis"	Aktivieren Sie das Kontrollkästchen **Limit für "Snooze bis"**, damit der Benutzer die Patch-Aktion so oft verschieben kann wie angegeben. Geben Sie die Anzahl der **Versuche** an.
Erste Meldung	Die Nachricht, die Benutzern vor dem Ausführen der Aktion angezeigt werden soll. Informationen zum Anpassen des im Dialogfeld angezeigten Logos finden Sie unter Allgemeine Appliance-Einstellungen bei aktivierter Organisationskomponente konfigurieren.
Fortschrittsmeldung	Die Meldung, die den Benutzern während der Patch-Aktion angezeigt wird.
Abschlussmeldung	Die Meldung, die den Benutzern nach Abschluss der Patch-Aktion angezeigt wird.

Abschnitt "Neustart"

Option	Beschreibung
Optionen	Die Optionen für den Neustart des verwalteten Geräts. • **Kein Neustart**: Das Gerät wird nicht neu gestartet, obwohl möglicherweise ein Neustart erforderlich ist, damit das Patch wirksam wird. Es wird davon abgeraten, die Option "Kein Neustart" zu verwenden, da die Bereitstellung von Patches ohne einen erforderlichen Neustart die Stabilität der Systeme beeinträchtigen kann. Zudem werden Patches, die einen Neustart erfordern, erst nach dem Neustart als bereitgestellt angezeigt. • **Eingabeaufforderung für Benutzer**: Vor dem Geräteneustart wird gewartet, bis der Benutzer den Neustart akzeptiert hat. Wenn sich der Benutzer den Neustart per Snooze verschiebt oder abbricht, wird der Patch-Vorgang angehalten, bis ein Neustart durchgeführt wird. Wenn Sie im Dialogfeld "Agent", das auf dem Zielgerät angezeigt wird, eine Snooze-Dauer auswählen, wird die

Option	Beschreibung
	Neustartaufforderung für das angegebene Snooze-Intervall angehalten. • **Neustart erzwingen**: Ein Neustart wird durchgeführt, sobald ein Patch bereitgestellt wurde, der einen Neustart erfordert. Erzwungene Neustarts können nicht abgebrochen werden. Neustart erzwingen eignet sich gut für Desktops und Server. Unter Umständen ist es nicht sinnvoll, auf Notebooks einen Neustart zu erzwingen. "Neustart erzwingen" eignet sich für Server, da diese in der Regel keine speziell zugewiesenen Benutzer besitzen. Es ist jedoch wichtig, Benutzer darauf hinzuweisen, dass Dienste nicht verfügbar sind, wenn Server gepatcht und neu gestartet werden. Siehe Best Practices für den Patch-Vorgang.
Automatisch neu starten, wenn niemand angemeldet ist	Das verwaltete Gerät wird automatisch neu gestartet, wenn keine Benutzer angemeldet sind.
Meldung	Die Nachricht, die Benutzern vor dem Neustart des Geräts angezeigt werden soll. Informationen zum Hinzufügen eines benutzerdefinierten Logos zum Meldungsdialogfeld finden Sie unter Allgemeine Appliance-Einstellungen bei aktivierter Organisationskomponente konfigurieren.
Timeout	Die Zeitspanne in Minuten, für die das Dialogfeld angezeigt werden soll, bevor eine Aktion ausgeführt wird. Wenn diese Zeitspanne verstreicht, ohne dass der Benutzer auf eine Schaltfläche klickt, führt die Appliance die in der Dropdown-Liste *Timeout* angegebene Aktion aus. Wenn *Neustart erzwingen* ausgewählt ist, berücksichtigt das Timeout-Verhalten den `KUSerAlert` und globale KACE Agenten-Prozess-Timeouts. Das im Abschnitt *Agenten- und Kommunikationseinstellungen* festgelegte globale Timeout bestimmt immer, wie lange ein durch den Agenten gestarteter Prozess laufen kann, einschließlich des `KUserAlert`-Timeout. Angenommen, das `KUserAlert`-Timeout ist auf zwei Stunden eingestellt, und Sie setzen das globale Timeout auf eine Stunde, so stoppt der Agent den `KUserAlert`, weil seine Ausführung zu lange dauern würde. Das globale Timeout muss daher auf ein Timeout gesetzt werden, das länger als das `KUserAlert`-Timeout ist. Dieser Wert muss entsprechend festgelegt werden. Weitere Informationen zu diesen Agenten-Einstellungen finden Sie unter Agentenkommunikation und Protokolleinstellungen konfigurieren.

Option	Beschreibung
Timeout-Aktion	Die Aktion, die ausgeführt werden soll, wenn die Zeitspanne für den **Timeout** abgelaufen ist, ohne dass der Benutzer eine Option ausgewählt hat.
Neustartverzögerung (Countdown)	Der Neustart wird mithilfe eines Countdowns verschoben. Der Countdown wird in Minuten angegeben.
Jetzt neu starten	Das Gerät wird sofort neu gestartet.
Später neu starten	Das Gerät wird später neu gestartet.
Anzahl der Eingabeaufforderungen	Die Anzahl der Eingabeaufforderungen, die dem Benutzer angezeigt werden, bevor das Gerät neu gestartet wird. Wenn Sie beispielsweise den Wert 5 eingeben, wird das Gerät automatisch neu gestartet, wenn der Benutzer die fünfte Aufforderung zum Neustart erhält. Mit anderen Worten: Der Benutzer kann den Neustart nur viermal verzögern, wenn der Wert für **Anzahl der Eingabeaufforderungen** auf "5" festgelegt ist.
Intervall für erneute Eingabeaufforderung	Die Zeit, die verstreicht, bevor der Benutzer erneut aufgefordert wird, einen Neustart durchzuführen.

Abschnitt "Planen"

Option	Beschreibung
Kein(e)	Die Ausführung erfolgt im Zusammenhang mit einem Ereignis anstatt zu einem bestimmten Datum oder zu einem bestimmten Zeitpunkt. Diese Option ist nützlich, wenn Sie Patches manuell auf Server anwenden oder Patch-Aktionen ausführen möchten, die nicht nach einem Zeitplan ausgeführt werden sollen.
Alle _ Stunden	Der Vorgang wird im angegebenen Intervall durchgeführt.
Täglich/an einem bestimmten Tag um HH:MM	Die Erfassung wird täglich zu einem bestimmten Zeitpunkt oder an einem bestimmten Wochentag um eine bestimmte Uhrzeit ausgeführt.
Ausführen am n-ten jedes Monats/eines bestimmten Monats um HH:MM	Am **n**. Tag jedes Monats ausführen (beispielsweise am ersten oder zweiten) Tag des Monats oder in einem bestimmten Monat zu einer bestimmten Zeit.
Ausführen am n-ten Wochentag **jedes Monats/ eines bestimmten Monats um HH:MM**	Die Erfassung wird jeden Monat oder in einem bestimmten Monat an einem festgelegten Wochentag zu einer festgelegten Uhrzeit ausgeführt.

Option	Beschreibung

Benutzerdefiniert	Ausführung nach einem benutzerdefinierten Zeitplan.
	Verwenden Sie das Standard-5-Feld-Cron-Format (das erweiterte Cron-Format wird nicht unterstützt):
	`* * * * *`
	`| | | | +————————Wochentag (0-6) (Sonntag=0)`
	`| | | +————————Monat (1-12)`
	`| | +————————Monatstag (1-31)`
	`| +————————Stunde (0-23)`
	`+————————Minute (0-59)`
	Verwenden Sie bei der Angabe von Werten die folgenden Zeichen:
	• **Leerzeichen( )**: Die einzelnen Felder mit einem Leerzeichen trennen.
	• **Sternchen (*)**: Ein Sternchen repräsentiert den gesamten Wertebereich in einem Feld. Zum Beispiel repräsentiert ein Sternchen im Stundenfeld eine beliebige Stunde.
	• **Kommas (,)**: Mehrere Werte in einem Feld werden mit einem Komma getrennt. Zum Beispiel werden mit `0,6` im Feld „Wochentag“ Sonntag und Samstag angegeben.
	• **Bindestriche (-)**: Mit einem Bindestrich wird ein Wertebereich in einem Feld angegeben. Zum Beispiel entspricht `1-5` im Feld „Wochentag“ `1,2,3,4,5`, d. h. Montag bis Freitag.
	• **Schrägstriche (/)**: Die Angabe der Zeitabstände, mit denen eine Aktion wiederholt werden soll, erfolgt mit einem Schrägstrich. Zum Beispiel entspricht `*/3` im Feld Stunde `0,3,6,9,12,15,18,21`. Das Sternchen (`*`) gibt jede Stunde an, mit `/3` erfolgt aber eine Einschränkung auf durch drei teilbare Stunden.
	Beispiele:
	• `15 * * * * Jeden Tag 15 Minuten nach jeder vollen Stunde ausführen`
	• `0 22 * * * Jeden Tag um 22:00 Uhr ausführen`
	• `0 0 1 1,6 * Am 1. Januar und 1. Juni um 00:00 Uhr ausführen`
	• `30 8,12 * * 1-5 An Wochentagen um 08:30 Uhr und 12:30 Uhr ausführen`
	• `0 2 */2 * * Jeden zweiten Tag um 02:00 Uhr ausführen`

Aufgabenplan anzeigen	Klicken Sie, um den Aufgabenplan anzuzeigen. Im Dialogfeld *Taskplan* wird eine Liste der geplanten

Option	Beschreibung
	Ziele angezeigt. Klicken Sie auf eine Aufgabe, um die Aufgabendetails anzuzeigen. Weitere Informationen hierzu finden Sie unter Aufgabenpläne anzeigen.
Zeitzone	Die Zeitzone, die beim Planen der Aktion verwendet werden soll. Wählen Sie **Server** aus, um die Zeitzone der Appliance zu verwenden. Wählen Sie **Agent** aus, um die Zeitzone des verwalteten Geräts zu verwenden.
Wenn offline, bei nächster Verbindung ausführen	Wenn das Gerät derzeit offline ist, wird die Aktion ausgeführt, sobald das verwaltete Gerät das nächste Mal eine Verbindung mit der Appliance herstellt. Diese Option eignet sich für Notebooks und andere Geräte, die regelmäßig offline sind. Wenn diese Option nicht ausgewählt wird und das Gerät offline ist, wird die Aktion erst zum nächsten geplanten Zeitpunkt ausgeführt.
Ausführung nach Wiederverbinden verzögern	Der Zeitplan wird um eine angegebene Zeitspanne verzögert. Die Zeitspanne der Verzögerung beginnt zu dem Zeitpunkt, für den die Ausführung der Patch-Aktion geplant wurde.
Beenden nach	Das Zeitlimit für Patch-Aktionen. Wenn Sie beispielsweise festlegen, dass Patches um 4.00 Uhr ausgeführt werden sollen, sollten Sie möglicherweise auch festlegen, dass alle Patch-Aktionen um 7.00 Uhr beendet werden, um Probleme hinsichtlich der Bandbreite zu vermeiden, wenn Benutzer mit der Arbeit beginnen. Hierzu können Sie im Minutenfeld den Wert **180** angeben. Wenn dieses Zeitlimit erreicht wird, werden alle Patch-Aufgaben, die derzeit ausgeführt werden, angehalten und der zugehörige Status im Sicherheitsprotokoll wird mit *Angehalten* angegeben. Diese Patch-Aufgaben werden bei der nächsten Ausführung nicht fortgesetzt, sondern beginnen vielmehr bei jeder geplanten Patch-Aktion wieder von vorn.

Konfigurieren von Patch-Zeitplänen

Sie können Patch-Zeitpläne erstellen und konfigurieren sowie einen Zeitpunkt für ihre Ausführung festlegen. Patch-Zeitpläne wirken sich nicht auf verwaltete Installationen oder andere Verteilungen aus.

1. Starten Sie den Assistenten für *Zeitplandetails*:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.

b. Klicken Sie in der linken Navigationsleiste auf **Sicherheit** und anschließend auf **Patch-Verwaltung**.

c. Klicken Sie im Fensterbereich *Patch-Verwaltung* auf **Zeitpläne**.

d. Führen Sie im Dialogfeld *Patch-Zeitpläne* einen der folgenden Schritte aus:

- Um einen neuen Patch-Zeitplan zu erstellen, klicken Sie auf **Aktion auswählen** > **Neu (Assistent)**.
- Zum Bearbeiten eines vorhandenen Zeitplans klicken Sie in der Liste auf den Namen des Zeitplans, und dann auf der Seite *Patch-Zeitplanübersicht* auf **Bearbeiten**.

  Der Assistent für *Zeitplandetails* wird wie ausgewählt angezeigt. Dieselben Optionen stehen auf der Seite *Schedule Detail (Zeitplandetails)* zur Verfügung. Sie können zwischen der Seite und dem Assistenten wechseln, indem Sie in der rechten oberen Ecke auf **Klassische Ansicht** oder **Wizard View (Assistentenansicht)** klicken.

2. Geben Sie im Assistenten für *Zeitplandetails* auf der Seite *Allgemeine Informationen* allgemeine Informationen zum Zeitplan an.

   Beschreibungen der Optionen finden Sie unter Allgemeine Informationen.

3. Klicken Sie auf **Weiter**.
4. Wählen Sie auf der Seite *Aktion* die Aktion aus, die Sie dem Zeitplan zuordnen möchten.

   Beschreibungen der Optionen finden Sie unter Aktionsbereich.

5. **Nur Zeitpläne für Erkennen, Erkennen und zur Verfügung stellen, Erkennen und Bereitstellen, Erkennen, zur Verfügung stellen und bedarfsgerecht bereitstellen, Erkennen und Rollback**. Geben Sie auf der Seite *Aktion* im Abschnitt *Erkennen* die Erkennungsoptionen für den Zeitplan an.

   Beschreibungen der Optionen finden Sie unter Abschnitt "Erkennen".

6. **Nur Zeitpläne für Erkennen und bereitstellen, Erkennen, zur Verfügung stellen und bedarfsgerecht Bereitstellen und Bereitstellen**. Geben Sie im Abschnitt *Bereitstellen* die Erkennungsoptionen für den Zeitplan an.

   Beschreibungen der Optionen finden Sie unter Abschnitt "Bereitstellen".

7. **Nur Zeitpläne für "Erkennen und Rollback" und "Rollback".** Geben Sie im Abschnitt *Rollback* die Rollback-Optionen für den Zeitplan an.

   Beschreibungen der Optionen finden Sie unter Abschnitt "Rollback".

8. **Nur Zeitpläne für Erkennen, zur Verfügung stellen und bedarfsgerecht bereitstellen**. Geben Sie im Abschnitt *On-demand Deployment Timeout Settings" (Timeout-Einstellungen für bedarfsgerechte Bereitstellung)* die Bereitstellungs-Timeout-Option für Erkennung, Staging und bedarfsgerechte Bereitstellung an.

   Beschreibungen der Optionen finden Sie unter Abschnitt "On-demand Deployment Timeout Settings" (Timeout-Einstellungen für bedarfsgerechte Bereitstellung).

9. Klicken Sie auf **Weiter**.
10. Geben Sie auf der Seite *Geräte* die Geräte an, die Sie diesem Zeitplan zuordnen möchten.

    Beschreibungen der Optionen finden Sie unter Abschnitt "Geräte".

11. Klicken Sie auf **Weiter**.
12. **Nur Zeitpläne für Erkennen und bereitstellen, Bereitstellen, Erkennen und Rollback und Rollback**. Konfigurieren Sie auf der Seite *Benachrichtigung* die Benachrichtigungsoptionen für den Zeitplan.

    Beschreibungen der Optionen finden Sie unter Abschnitt "Benachrichtigen".

13. Klicken Sie auf **Weiter**.
14. Geben Sie im Abschnitt *Neustart* die Neustartoptionen für den Zeitplan an.

Beschreibungen der Optionen finden Sie unter Abschnitt "Neustart".

15. Klicken Sie auf **Weiter**.
16. Geben Sie im Abschnitt *Zeitplan* Optionen für den Zeitplan an.

    Beschreibungen der Optionen finden Sie unter Abschnitt "Planen".

17. Klicken Sie auf **Speichern**.

    Die Seite *Patch-Zeitplanübersicht* wird eingeblendet, auf der der neu erstellte oder aktualisierte Zeitplan angezeigt wird. Weitere Informationen zu dieser Seite finden Sie unter Überprüfen von Details zu Patch-Zeitplänen. Wenn Sie Geräte hinzufügen, die den Kriterien für das Smart Label entsprechen, werden sie automatisch in den Patch-Zeitplan aufgenommen.

Fehlercodes aufgrund von Patching und Skripterstellung

Die folgenden Fehlschlagen-Fehlercodes können während des Patching (Nur Erkennungs- oder Bereitstellungsphase) oder Skripting auftreten.

Beim Patching oder Skripting aufgetretene Fehlercodes

Fehlercode	Beschreibung
8001	Der an das Plug-in gesendete Befehl wurde vom `KPluginsKacePatch` nicht erkannt
8002	Fehler beim Parsen des an das Plug-In gesendeten Befehls
8003	Fehler beim Herunterladen einer Manifestdatei
8004	Fehler beim Extrahieren der heruntergeladenen Manifestdatei
8005	Allgemeiner Fehler beim Ausführen des Befehls PreDetect (z. B. ungültige Funktionseingaben)
8007	Fehler beim Generieren der PreDetect-Ergebnisse
8008	Allgemeiner Fehler beim Ausführen des Befehls Ermitteln (z. B. ungültige Funktionseingaben)
8009	Fehler beim Parsen der Ermitteln-Manifestdatei
8010	Fehler beim Generieren der Ermittlungsergebnisse
8011	Ein Neustart ist ausstehend
8012	Fehler beim Hochladen eines Ergebnisprotokolls
8013	Allgemeiner Fehler bei der Verarbeitung der Ermittlungsdatei (z. B. ungültige Funktionseingaben)
8014	Fehler beim Herunterladen einer Patch-Ermittlungsdatei

Fehlercode	Beschreibung
8015	Prüfsummenabweichung zwischen der Patch-Erkennungsdatei und dem Erkennungsmanifest-Datensatz
8016	Fehler beim Erstellen einer Prüfsummendatei für die Patch-Ermittlungsdatei
8017	Fehler beim Laden der Patch-Ermittlungsdatei
8018	Fehler beim Entschlüsseln der Patch-Ermittlungsdatei
8019	Fehler beim Entpacken der Patch-Ermittlungsdatei
8020	Fehler beim Parsen von json in der Patch-Ermittlungsdatei
8021	Erkennungstyp in der Patch-Ermittlungsdatei nicht als gültige Ermittlungsmethode erkannt
8100	Fehler beim Parsen der Manifestdatei
8101	Allgemeiner Fehler beim Ausführen des Befehls Bereitstellen (z. B. ungültige Funktionseingaben)
8102	Allgemeiner Fehler beim Ausführen des Befehls Rollback (z. B. ungültige Funktionseingaben)
8103	Ungültiger HSD-Typ (Handler Specific Data)
8150	Prüfsummenabweichung zwischen der angeforderten Datei und dem Manifestdatensatz
8151	Fehler beim Herunterladen einer angeforderten Datei
8152	Fehler beim Erstellen einer Prüfsummendatei für eine heruntergeladene Datei
8200	Ungültiger Befehl Skalarvorgang
8201	Ungültiger Befehl Stringvorgang
8202	Ungültiger Befehl
8250	Ungültiger Pfad zur Ergebnisdatei
8251	Fehler beim Erstellen einer Ergebnisdatei

Anzeigen von Patch-Zeitplänen, -Status und -Berichten

Sie können Patch-Zeitpläne sowie den Patch-Status anzeigen – sowohl allgemein als auch nach Gerät. Darüber hinaus können Sie nach einzelnen Paketen innerhalb der Patches suchen und patchbezogene Berichte anzeigen.

Liste der Patch-Zeitpläne anzeigen

Sie können zusammenfassende Informationen für die Patch-Zeitpläne anzeigen, die auf der Appliance erstellt wurden. Wenn auf der Appliance die Organisationskomponente aktiviert wurde, zeigen Sie die Patch-Zeitpläne für jede Organisation einzeln an.

1. Rufen Sie die Seite *Patch-Zeitplan* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Sicherheit** und anschließend auf **Patch-Verwaltung**.
   c. Klicken Sie im Fensterbereich *Patch-Verwaltung* auf **Zeitpläne**.

   Auf der Seite *Patch-Zeitpläne* gibt es folgende Spalten:

Option	Beschreibung
Letzte Aktualisierung	Datum und Uhrzeit, wann der Patch-Zeitplan aktualisiert wurde.
Name	Der Name des Patch-Zeitplans. Klicken Sie hier, um weitere Details auf der Seite *Patch-Zeitplanübersicht* anzuzeigen. Weitere Informationen hierzu finden Sie unter Überprüfen von Details zu Patch-Zeitplänen.
Planen	Die vorgegebene Frequenz, in der der Patch-Zeitplan ausgeführt werden soll. Ist diese Option deaktiviert, bedeutet das, dass der Patch nach keinem Zeitplan ausgeführt wird.
Aktion	Die Art der Patch-Aktion, die ausgeführt werden kann.
Neustartoption	Angabe darüber, ob der Patch-Zeitplan erfordert, dass verwaltete Geräte bei der Patch-Ausführung neu gestartet werden müssen.
Alle Geräte	Angabe darüber, ob der Patch-Zeitplan alle Geräte (Ja) oder ausgewählte Geräte (Nein) umfasst.
Ausstehend	Die Anzahl der verwalteten Geräte, auf denen der Patch nach Zeitplan ausgeführt werden soll. Patches mit diesem Status zeigen eine der folgenden

Option	Beschreibung
	Angaben im Abschnitt *Sicherheit* auf der Seite *Gerätedetail*: • *warten auf Verbindung* • *geplant* • *warten auf Zeitplanerstellung*
Download wird ausgeführt ...	Die Anzahl der Geräte, die den Patch herunterladen. Patches mit diesem Status zeigen die folgende Angabe im Abschnitt *Sicherheit* auf der Seite *Gerätedetail*: *Wird heruntergeladen*.
Wird ausgeführt ...	Die Anzahl verwalteter Geräte, auf denen der Patch installiert ist. Patches mit diesem Status zeigen eine der folgenden Angaben im Abschnitt *Sicherheit* auf der Seite *Gerätedetail*: • *Handshake* • *Erkennung wird ausgeführt* • *Rollback wird ausgeführt* • *Bereitstellung wird ausgeführt* • *Bereinigung* • *Überprüfung wird ausgeführt* • *Warnung wird ausgegeben* • *Hochladen*
Neustart wird ausgeführt ...	Die Anzahl der verwalteten Geräte, die beim Patching-Prozess neustarten. Patches mit diesem Status zeigen eine der folgenden Angaben im Abschnitt *Sicherheit* auf der Seite *Gerätedetail*: • *Neustart wird ausgeführt* • *Neustart ausstehend* • *Verbindung wird hergestellt*
Angehalten	Die Anzahl der verwalteten Geräte, für die der Patching-Prozess angehalten oder auf Snooze gesetzt wurde. Patches mit diesem Status zeigen eine der folgenden Angaben im Abschnitt *Sicherheit* auf der Seite *Gerätedetail*: • *Snooze für Neustart* • *Snooze*
Erfolgreich	Die Anzahl der verwalteten Geräte, für die der Patching-Prozess erfolgreich abgeschlossen wurde. Patches mit diesem Status zeigen die folgende Angabe im Abschnitt *Sicherheit* auf der Seite *Gerätedetail*: *abgeschlossen*.

Option	Beschreibung
Fehler	Die Anzahl der verwalteten Geräte, die beim Patching-Prozess Fehler gemeldet wurden. Patches mit diesem Status zeigen eine der folgenden Angaben im Abschnitt *Sicherheit* auf der Seite *Gerätedetail*: • *angehalten* • *abgebrochen*
Offline	Die Anzahl der verwalteten Geräte, die zum Zeitpunkt der geplanten Patching-Ausführung nicht verbunden waren. Patches mit diesem Status zeigen die folgende Angabe im Abschnitt *Sicherheit* auf der Seite *Gerätedetail*: *Nicht geplant*.
Abgeschlossen	Die Anzahl der verwalteten Geräte, auf denen der Patching-Prozess mit dem Status *Erfolgreich*, *Fehler* oder *Offline* abgeschlossen wurde.

2. (Optional) Um die angezeigten Spalten zu ändern, wählen Sie aus der Dropdown-Liste *Tabellenoptionen* rechts über der Tabelle **Spaltenanzeige** aus.

Überprüfen von Details zu Patch-Zeitplänen

Wenn Sie einen Patching-Zeitplan konfigurieren, werden auf dieser Seite Details zur Konfiguration des Zeitplans und dessen Status angezeigt.

1. Rufen Sie die Seite *Patch-Zeitplanübersicht* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Sicherheit** und anschließend auf **Patch-Verwaltung**.
   c. Klicken Sie im Fensterbereich *Patch-Verwaltung* auf **Zeitpläne**.
   d. Klicken Sie auf den Namen eines Patch-Zeitplans.
2. Überprüfen Sie den Inhalt des Abschnitts *Konfiguration*.

Option	Beschreibung
Erstellt	Das Datum und die Uhrzeit der Erstellung des Zeitplans.
Geändert	Das Datum und die Uhrzeit der letzten Änderung des Zeitplans.
Letzte Ausführung	Das Datum und die Uhrzeit der letzten Ausführung des Zeitplans.
Name	Der Name des Zeitplans.

Option	Beschreibung

Aktion	Die mit dem Zeitplan verbundene Aktion:
	• **Erkennen**: Erkennt Patches, die auf verwalteten Geräten installiert sind oder auf diesen fehlen. Aktionen vom Typ "Nur erkennen" werden empfohlen, wenn in den *Einstellungen für Patch-Download* nur das Herunterladen konfiguriert wird. Beim Ausführen einer Aktion, bei der nur eine Erkennung erfolgt, wird vor der Bereitstellung eine Liste der Patch-Dateien erstellt, die heruntergeladen werden müssen, bevor die Bereitstellung gestartet wird.
	• **Erkennen und zur Verfügung stellen**: Erkennt Patches, die auf verwalteten Geräten installiert sind oder fehlen, und lädt Patch-Dateien zur späteren Bereitstellung auf das Agent-Gerät herunter.
	• **Erkennen und bereitstellen**: Erkennt Patches für verwaltete Geräte und stellt sie auf diesen bereit. Diese Arten von Aktionen werden bei der Verwaltung von Desktops und Servern verwendet. Für Patch-Jobs für die Erkennung und Bereitstellung ist eine Verbindung zwischen dem Gerät und der Appliance erforderlich, da diese nicht offline ausgeführt werden können. Weitere Informationen zu Messaging-Protokoll-Verbindungen finden Sie unter Agentenkommunikation und Protokolleinstellungen konfigurieren.
	• **Detect, Stage and On-demand Deploy (Erkennen, zur Verfügung stellen und bedarfsgerecht bereitstellen)**: Erkennt Patches, die auf verwalteten Geräten installiert sind oder fehlen, lädt Patch-Dateien auf das Agent-Gerät herunter. In der Windows-Taskleiste auf dem Agent-Gerät wird daraufhin eine Benachrichtigung angezeigt, dass die Patches bereit für die Bereitstellung sind. Der Benutzer kann dann den Bereitstellungsvorgang nach Belieben initiieren.
	  ◦ Diese Zeitpläne sind nur für Windows-Geräte mit Agenten der Version 11.0 oder höher verfügbar.
	  ◦ Die Option *Agentenstatussymbol auf Gerät* muss in den Kommunikationseinstellungen des Agenten aktiviert sein. Diese Einstellungen finden Sie auf der Seite *Organisationsdetails*, unter *Kommunikations- und Agenteneinstellungen* (falls eine oder mehrere Organisationskomponenten

Option	Beschreibung
	aktiviert sind) oder auf der Seite *Kommunikationseinstellungen* (falls Sie über keine Organisationskomponente verfügen). Weitere Informationen hierzu finden Sie unter Agentenkommunikation und Protokolleinstellungen konfigurieren. • **Bereitstellen**: Stellt anwendbare Patches auf verwalteten Geräten bereit. Das ist nützlich, wenn Sie wissen, dass bestimmte Patches auf verwalteten Geräten bereitgestellt werden müssen. Ein Job vom Typ "Erkennen" wird abschließend ausgeführt, nachdem das Patch bereitgestellt wurde oder, falls ein Neustart erforderlich ist, nachdem das Gerät neu gestartet wurde und der Agent erneut eine Verbindung mit der Appliance hergestellt hat. • **Erkennen und Rollback durchführen**: Erkennt und entfernt unerwünschte Patches von verwalteten Geräten. Für manche Patches sind möglicherweise keine Rollbacks verfügbar. Siehe Ermitteln, ob für ein Patch ein Rollback möglich ist. • **Rollback**: Entfernt unerwünschte Patches von verwalteten Geräten. Für manche Patches sind möglicherweise keine Rollbacks verfügbar. Siehe Ermitteln, ob für ein Patch ein Rollback möglich ist.
Beschreibung	Eine kurze Beschreibung des Patch-Zeitplans.
Geräte	Dieses Feld wird nur angezeigt, wenn der Zeitplan so konfiguriert ist, dass er auf alle Geräte angewendet wird.
Label des Geräts	Mindestens ein Smart Label, das mit den Geräten verknüpft ist, für die der Zeitplan ausgeführt wird. Weitere Informationen hierzu finden Sie unter Smart Labels für Patches verwenden. Dieses Feld wird nur angezeigt, wenn der Zeitplan so konfiguriert ist, dass er auf ausgewählte Geräte angewendet wird.
Gerätename	Mindestens ein ausgewähltes Geräte, für das der Zeitplan ausgeführt wird. Dieses Feld wird nur angezeigt, wenn der Zeitplan so konfiguriert ist, dass er auf ausgewählte Geräte angewendet wird.
Zu erkennende Patches	**Detect schedules only (Nur Zeitpläne für Erkennung)**. Dieses Feld wird nur angezeigt, wenn der Zeitplan so konfiguriert ist, dass alle Patches erkannt werden.
Label finden	**Detect schedules only (Nur Zeitpläne für Erkennung)**. Mindestens ein Smart Label, das mit den geplanten Patches verknüpft ist. Weitere

Option	Beschreibung
	Informationen hierzu finden Sie unter Smart Labels für Patches verwenden. Dieses Feld wird nur angezeigt, wenn der Zeitplan so konfiguriert ist, dass ausgewählte Patches erkannt werden.
Bereitzustellende Patches	**Deploy schedules only (Nur Zeitpläne für Bereitstellung)**. Dieses Feld wird nur angezeigt, wenn der Zeitplan so konfiguriert ist, dass alle Patches bereitgestellt werden.
Label bereitstellen	**Deploy schedules only (Nur Zeitpläne für Bereitstellung)**. Mindestens ein Smart Label, das mit den geplanten Patches verknüpft ist. Weitere Informationen hierzu finden Sie unter Smart Labels für Patches verwenden. Dieses Feld wird nur angezeigt, wenn der Zeitplan für die Bereitstellung ausgewählter Patches konfiguriert ist.
Patches to Rollback (Zurückzusetzende Patches)	**Rollback schedules only (Nur Zeitpläne für Rollback)**. Dieses Feld wird nur angezeigt, wenn der Zeitplan so konfiguriert ist, dass alle Patches entfernt werden.
Rollback für Label	**Rollback schedules only (Nur Zeitpläne für Rollback)**. Mindestens ein Smart Label, das mit den geplanten Patches verknüpft ist. Weitere Informationen hierzu finden Sie unter Smart Labels für Patches verwenden. Dieses Feld wird nur angezeigt, wenn der Zeitplan so konfiguriert ist, dass ausgewählte Patches entfernt werden.
Warnungen	**Schedules without the Deploy action only (Nur Zeitpläne ohne Bereitstellungsaktion)**. Die Benachrichtigungen, die den Benutzern bei der Ausführung von Patch-Aktionen angezeigt werden: • **OK**: Sofort ausführen. • **Abbrechen**: Abbrechen bis zur nächsten geplanten Ausführung. • **Snooze**: Der Benutzer erhält nach Ablauf der *Snooze-Dauer* erneut eine Eingabeaufforderung.
Neustart	**Schedules without the Deploy action only (Nur Zeitpläne ohne Bereitstellungsaktion)**. Die Optionen für den Neustart des verwalteten Geräts: • **Kein Neustart**: Das Gerät wird nicht neu gestartet, obwohl möglicherweise ein Neustart erforderlich ist, damit das Patch wirksam wird. Es wird davon abgeraten, die Option "Kein Neustart" zu verwenden, da die Bereitstellung von Patches ohne einen erforderlichen Neustart die Stabilität der Systeme beeinträchtigen kann. Zudem werden Patches, die einen Neustart erfordern,

Option	Beschreibung
	erst nach dem Neustart als bereitgestellt angezeigt. • **Eingabeaufforderung für Benutzer**: Vor dem Geräteneustart wird gewartet, bis der Benutzer den Neustart akzeptiert hat. Wenn sich der Benutzer den Neustart per Snooze verschiebt oder abbricht, wird der Patch-Vorgang angehalten, bis ein Neustart durchgeführt wird. Wenn Sie im Dialogfeld "Agent", das auf dem Zielgerät angezeigt wird, eine Snooze-Dauer auswählen, wird die Neustartaufforderung für das angegebene Snooze-Intervall angehalten. • **Neustart erzwingen**: Ein Neustart wird durchgeführt, sobald ein Patch bereitgestellt wurde, der einen Neustart erfordert. Erzwungene Neustarts können nicht abgebrochen werden. Neustart erzwingen eignet sich gut für Desktops und Server. Unter Umständen ist es nicht sinnvoll, auf Notebooks einen Neustart zu erzwingen. "Neustart erzwingen" eignet sich für Server, da diese in der Regel keine speziell zugewiesenen Benutzer besitzen. Es ist jedoch wichtig, Benutzer darauf hinzuweisen, dass Dienste nicht verfügbar sind, wenn Server gepatcht und neu gestartet werden. Siehe Best Practices für den Patch-Vorgang.
Planen	Die ausgewählten Zeitplandetails. Klicken Sie auf **Aufgabenplan anzeigen**, um eine detaillierte Aufgabenplanung anzuzeigen. Klicken Sie im daraufhin angezeigten Dialogfeld auf eine Aufgabe, um die Aufgabendetails zu überprüfen. Weitere Informationen hierzu finden Sie unter Aufgabenpläne anzeigen.
Wenn offline, bei nächster Verbindung ausführen	Wenn das Gerät derzeit offline ist, wird die Aktion ausgeführt, sobald das verwaltete Gerät das nächste Mal eine Verbindung mit der Appliance herstellt.
Ausführung nach Wiederverbinden verzögern	Diese Option gibt an, wie lange sich der Zeitplan verzögert. Die Zeitspanne der Verzögerung beginnt zu dem Zeitpunkt, für den die Ausführung der Patch-Aktion geplant wurde.
Beenden nach	Diese Option gibt die maximale Zeitspanne für die Ausführung des Zeitplans an. Wenn dieses Zeitlimit erreicht ist, werden alle laufenden Patching-Aufgaben angehalten.

3. Überprüfen Sie im Abschnitt *Zeitplanstatus* den Gesamtstatus des Patch-Zeitplans auf einer der folgenden Registerkarten:

Registerkarte	Inhalt
Nach Computer	Geräte, die für das Patching ausgewählt wurden. Jeder Eintrag zeigt den Gerätenamen, seine IP-Adresse, den Patchstatus (siehe Patching-Status-Definitionen), Patch-Ergebnisse und das Datum, an dem das Patching abgeschlossen wurde. Um die entsprechenden Patches anzuzeigen, erweitern Sie den Geräteknoten. Jeder Patch-Eintrag zeigt die Patch-ID, die zugehörige Knowledge Base-Artikelnummer, den Patch-Namen und den aktuellen Status an (Gepatcht, Nicht gepatcht, Bereitgestellt, Erkannt, Bereitstellen oder Bereitstellungsfehler).
Nach Patch	Patches, die für Erkennung, Staging und Bereitstellung ausgewählt wurden. Jeder Eintrag zeigt die Patch-ID, die zugehörige Knowledge Base-Artikelnummer, den Patch-Namen und die Anzahl der Geräte an, die gepatcht oder nicht gepatcht wurden, sowie die Geräte, bei denen Erkennung- oder Bereitstellungsfehler aufgetreten sind.
Gepatcht	Patches wurden erfolgreich auf Geräten installiert. Jeder Eintrag zeigt die Patch-ID, die zugehörige Knowledge Base-Artikelnummer und den Patch-Namen an. Um die Geräte anzuzeigen, auf denen der Patch installiert ist, erweitern Sie den Geräteknoten.
Nicht gepatcht	Patches, die nicht auf Geräten installiert sind. Jeder Eintrag zeigt die Patch-ID, die zugehörige Knowledge Base-Artikelnummer und den Patch-Namen an. Um die Geräte anzuzeigen, auf denen der Patch installiert werden soll, erweitern Sie den Geräteknoten.
Bereitgestellt (Staging)	Patches, die für die Installation bereitgestellt werden. Staging bezieht sich auf Patch-Dateien, die zur späteren Bereitstellung auf das Agent-Gerät kopiert werden. Jeder Eintrag zeigt die Patch-ID, die zugehörige Knowledge Base-Artikelnummer und den Patch-Namen an. Um die Geräte anzuzeigen, auf denen der Patch installiert werden soll, erweitern Sie den Geräteknoten.
Fehler bei der Erkennung	Unvollständige Patches, die zu einem Erkennungsfehler geführt haben. Jeder Eintrag zeigt die Patch-ID, die zugehörige Knowledge Base, den Patch-Namen und den zugehörigen Fehlercode an (siehe Fehlercodes aufgrund von Patching und Skripterstellung). Um die Geräte anzuzeigen, auf denen der Fehler aufgetreten ist, erweitern Sie den Geräteknoten.
Stage Failures (Staging-Fehler)	Unvollständige Patches, die zu einem Staging-Fehler geführt haben. Jeder Eintrag zeigt die Patch-ID, die zugehörige Knowledge Base-Artikelnummer, den Patch-Namen und den zugehörigen Fehlercode

Registerkarte	Inhalt
	an (siehe Fehlercodes aufgrund von Patching und Skripterstellung). Um die Geräte anzuzeigen, auf denen der Fehler aufgetreten ist, erweitern Sie den Geräteknoten.
Fehler bei der Bereitstellung	Unvollständige Patches, die zu einem Bereitstellungsfehler geführt haben. Jeder Eintrag zeigt die Patch-ID, die zugehörige Knowledge Base, den Patch-Namen und den zugehörigen Fehlercode an (siehe Fehlercodes aufgrund von Patching und Skripterstellung). Um die Geräte anzuzeigen, auf denen der Fehler aufgetreten ist, erweitern Sie den Geräteknoten.

4. **Optional**. Nach Überprüfung der Zeitplandetails können Sie eine der folgenden Aktionen durchführen:
   - Klicken Sie zum Bearbeiten des Patching-Zeitplans auf **Bearbeiten**. Weitere Informationen hierzu finden Sie unter Konfigurieren von Patch-Zeitplänen.
   - Klicken Sie zum Ausführen des Patching-Zeitplans auf **Jetzt ausführen**.
   - Um eine Kopie des Patching-Zeitplans zu erstellen, klicken Sie auf **Duplizieren**.
   - Um den Patching-Zeitplan zu löschen, klicken Sie auf **Löschen**.

Patching-Status-Definitionen

Ein Patching-Status gibt den Zustand der aktuellen Aufgabe an. Diese Informationen werden auf der Seite *Patch-Zeitplanübersicht* im Abschnitt *Schedule Status (Zeitplanstatus)* angezeigt. Weitere Informationen hierzu finden Sie unter Überprüfen von Details zu Patch-Zeitplänen.

Patching-Status-Definitionen

Patching-Status	Definition
Warnung wird ausgegeben	An Benutzer gesendeter Alarm wartet auf Bestätigung.
abgebrochen	Die Aufgabe wurde vom Benutzer abgebrochen.
Bereinigung	Payload-Dateien vom Agenten, für die in den letzten 90 Tagen kein Zugriff erfolgt ist.
abgeschlossen	Die Aufgabe wurde abgeschlossen.
Verbindung wird hergestellt	Nach dem Neustart wird Verbindung mit dem Agenten wieder hergestellt.
bereitstellen	Die Patch-Bereitstellung wird durchgeführt.
erkennen	Die Patch-Erkennung wird durchgeführt.
Download wird durchgeführt	Die Patch-Bereitstellung muss zunächst Pakete herunterladen.

Patching-Status	Definition
error	Die Aufgabe wurde aufgrund eines Timeouts oder eines anderen Fehlers nicht abgeschlossen.
nicht geplant	Die Aufgabe wurde für dieses Gerät noch nicht erstellt.
vorab erkennen	Die Voraberkennung mit dem Agenten ist in Bearbeitung.
Neustart ausstehend	Patches wurden bereitgestellt; Neustart erforderlich, um Vorgang fortzusetzen.
Snooze für Neustart	Patches wurden bereitgestellt; Neustart erforderlich, um Vorgang fortzusetzen. Nach einem konfigurierten Intervall wird der Endbenutzer an den Neustart erinnert.
Rollback wird ausgeführt	Das Patch-Rollback wird durchgeführt.
geplant	Die Aufgabe wurde geplant und wartet auf die Ausführung.
Snooze	Die Aufgabe wurde per Snooze verschoben; der Benutzer wird nach der konfigurierten Snooze-Dauer an die Aufgabe erinnert.
zur Verfügung stellen	Die Dateien werden für eine spätere Bereitstellung heruntergeladen.
angehalten	Die Aufgabe wurde vor Abschluss unterbrochen.
Protokolle werden hochgeladen ...	Protokolle zur Vorerkennung, Erkennung, Bereitstellung, Überprüfung oder Rollback werden hochgeladen.
Überprüfung wird ausgeführt	Nach der Bereitstellung wird zur Überprüfung eine Erkennung durchgeführt.
version check (Versionsprüfung)	Die Aufgabe überprüft die Patch-Version.
waiting on-demand deploy (Warten auf bedarfsgerechte Bereitstellung)	Aufgabe wartet auf die Bereitstellung des Zeitplans durch die Benutzeraktion.
warten auf Verbindung	Gerät nicht verbunden.
warten auf Zeitplanerstellung	Aufgabe wartet auf Zeitplan gemäß der Zeitzone des Agenten.

Patch-Status anzeigen

Sie können den Status von Patches sowie eine Liste der Geräte, auf denen Patches bereitgestellt wurden, anzeigen.

1. Rufen Sie die *Patch-Detailseite* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Sicherheit** und anschließend auf **Patch-Verwaltung**.
   c. Klicken Sie im Fensterbereich *Patch-Verwaltung* auf **Katalog**.
2. Scrollen Sie nach unten bis zur Tabelle *Bereitstellungsstatus*.

   In der Tabelle werden Details zum Patch sowie eine Liste mit den Geräten angezeigt, auf denen das Patch bereitgestellt wurde.

Patch-Status nach Gerät anzeigen

Sie können den Patch-Status für die einzelnen verwalteten Geräte anzeigen.

1. Rufen Sie die *Gerätedetailseite* der Organisation auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Inventar** und anschließend auf **Dashboard**.
   c. Klicken Sie auf den Namen eines Geräts.
2. Scrollen Sie nach unten zum Abschnitt *Sicherheit* und klicken Sie auf den Link **Status von Patch-Erkennung/-Bereitstellung**.

Die Liste der auf dem Gerät installierten Patches wird angezeigt.

In Patches enthaltene Dateien anzeigen

Sie können die in den einzelnen Patches enthaltenen Dateien anzeigen.

1. Rufen Sie die *Patch-Detailseite* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Sicherheit** und anschließend auf **Patch-Verwaltung**.
   c. Klicken Sie im Fensterbereich *Patch-Verwaltung* auf **Katalog**.
2. Scrollen Sie nach unten zur Tabelle *Zugehörige Dateien*.

Patch-Berichte anzeigen

Sie können Berichte zum Patchen anzeigen.

1. Rufen Sie die *Berichtsseite* für die Patch-Verwaltung auf:
    a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
    b. Klicken Sie in der linken Navigationsleiste auf **Sicherheit** und anschließend auf **Patch-Verwaltung**.
    c. Klicken Sie im Fensterbereich *Patch-Verwaltung* auf **Berichterstellung**.

    Die Seite *Berichte* wird angezeigt und in der Dropdown-Liste *Anzeigen nach* ist die Option **Patchen** ausgewählt. Diese Seite enthält Links zu Berichten über Patches.

Verwalten von Patch-Rollbacks

Sie können ein Rollback für Patches durchführen, um sie von verwalteten Geräten zu entfernen, sofern dies für den Patch unterstützt wird.

Rollbacks werden allerdings nicht von allen Herstellern und Patch-Typen unterstützt. Beispielsweise erlauben umfangreiche Software-Patches wie Service Packs kein Rollback.

Ermitteln, ob für ein Patch ein Rollback möglich ist

Auf der Seite *Patch-Katalog* können Sie ermitteln, ob für Patches ein Rollback durchgeführt werden kann, nachdem sie auf verwalteten Geräten bereitgestellt wurden.

1. Rufen Sie die *Patch-Detailseite* auf:
    a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
    b. Klicken Sie in der linken Navigationsleiste auf **Sicherheit** und anschließend auf **Patch-Verwaltung**.
    c. Klicken Sie im Fensterbereich *Patch-Verwaltung* auf **Katalog**.
    d. Klicken Sie auf den Namen eines Patches.
2. Klicken Sie oberhalb der Liste auf der rechten Seite auf die Registerkarte **Erweiterte Suche**, um den Bereich *Erweiterte Suche* anzuzeigen.
3. Geben Sie folgende Suchkriterien ein.

    ```
    Patch-Listeninformationen: Support Rollback | is | True
    ```

4. **Optional**: Geben Sie zusätzliche Suchkriterien ein.
5. Klicken Sie auf **Suchen**.

Patches mit Rollback-Unterstützung werden angezeigt.

Letzten Patch-Job rückgängig machen

Wenn der Patch-Hersteller ein Rollback unterstützt, können Sie die letzte Patch-Bereitstellung rückgängig machen, indem Sie einen Patch-Zeitplan für Rollback oder Erkennen und Rollback erstellen und ausführen.

1. Rufen Sie die *Detailseite für den Patch-Zeitplan* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Sicherheit** und anschließend auf **Patch-Verwaltung**.
   c. Klicken Sie im Fensterbereich *Patch-Verwaltung* auf **Zeitpläne**.
   d. Klicken Sie auf den Namen eines Patch-Zeitplans.
2. Wählen Sie in der Dropdown-Liste *Aktion* die Option **Rollback** oder **Erkennen und Rollback durchführen** aus.
3. Wählen Sie die Patches für das Rollback in der gleichen Weise aus, wie Sie sie im ursprünglichen Zeitplan angegeben haben. Erstellen Sie dazu ein Smart Label.

   Siehe Smart Labels für Patches verwenden.

   Diese Option unterstützt nur das Entfernen des letzten für eine Softwareanwendung installierten Patches. Siehe Verwalten von Patch-Rollbacks.
4. Legen Sie nach Bedarf weitere Einstellungen für den Patch-Zeitplan fest.

   Weitere Informationen hierzu finden Sie unter Konfigurieren von Patch-Zeitplänen.

Verwalten des Patch-Inventars

Auf die Appliance heruntergeladene Patches werden als Patch-Inventar bezeichnet. Sie können Details und Statistiken zum Patch-Inventar anzeigen und Patches als aktiv oder inaktiv kennzeichnen. Außerdem können Sie Patches mithilfe von Labels verwalten.

Voraussetzungen für die Verwaltung des Patch-Inventars

Bevor Sie das Patch-Inventar verwalten, müssen Sie Patches abonnieren und herunterladen.

Siehe:

- Abonnieren von Patches und Konfigurieren von Downloadeinstellungen
- Download-Einstellungen für Patch- und Funktionsaktualisierungen auswählen

Anzeigen von Patch-Informationen

Sie können Informationen zu Patches sowie Patch-Informationen für Geräte nach Bedarf anzeigen.

Heruntergeladene Patches anzeigen

Die Liste *Patch-Katalog* enthält die für abonnierte Patches heruntergeladenen Patch-Erkennungssignaturen.

1. Rufen Sie die Patch-Seite *Katalog* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Sicherheit** und anschließend auf **Patch-Verwaltung**.
   c. Klicken Sie im Fensterbereich *Patch-Verwaltung* auf **Katalog**.
2. Verwenden Sie diese Dropdownliste, um die Patches aufzulisten.
   - **Anzeigen nach: Steuert die Patch-Anzeige in der Liste auf der Grundlage der in der Dropdown-Liste getroffenen Auswahl.**

Spalte	Beschreibung
Alle Patches	Alle Patches anzeigen.
Label	Mit einem Label versehene Patches anzeigen. Diese Informationen werden nur angezeigt, wenn Labels erstellt wurden.
Status	Patches mit dem Status **Aktiv**, **Deaktiviert** oder **Inaktiv** anzeigen.
Download-Status	Patches anzeigen, deren Status **Heruntergeladen** oder **Nicht heruntergeladen** lautet.
Schweregrad	Die Patch-Liste nach der von Herstellern, beispielsweise Microsoft, angegebenen Bedeutung filtern. Die Schweregrade sind: **Kritisch**, **Wichtig**, **Niedrig** usw.
Aktuellste	Patches anzeigen, die zuletzt hinzugefügt wurden. Sie können die Patches anzeigen, die im **letzten Monat**, in den **letzten 6 Monaten**, im **letzten Jahr** oder in den **letzten 2 Jahren** hinzugefügt wurden.
Jahr	Die Patch-Liste nach dem Jahr filtern, in dem das Patch veröffentlicht wurde.
Betriebssystem	Die Patch-Liste nach Betriebssystem filtern.

3. Die Spalten auf der Seite *Patch-Katalog* enthalten folgende Informationen:

Spalte	Beschreibung
Status	Der Status des Patches: Aktiv, Inaktiv oder Deaktiviert. • **Aktiv**: Patches, die Sie abonniert haben, die heruntergeladen wurden und erkannt oder bereitgestellt werden können. • **Inaktiv**: Patches, die Sie abonniert haben, die aber als inaktiv markiert wurden, damit sie nicht automatisch erkannt oder bereitgestellt werden. • **Deaktiviert**: Patches, die nicht mit Ihrem Abonnement übereinstimmen. Diese Patches können nur erkannt werden, wenn die Option *Deaktivierte Patches erkennen* in Ihrem Patch-Abonnement aktiviert ist. Patches können nur bereitgestellt werden, wenn sie die Abonnementkriterien erfüllen.
Paket	Die Informationen zur Identifizierung des Patches. In dieser Spalte werden auch Labels angezeigt, die dem Patch zugewiesen wurden.
Name	Der Name des Patches.
Herausgegeben	Das Datum, an dem das Patch zur Verfügung stand.
Herausgeber	Der Name des Herausgebers des Patches.
Schweregrad	Die vom Herausgeber (beispielsweise Microsoft) festgelegte Bedeutung des Patches.
Neustart	Angabe, ob Geräte zum Abschließen des Patch-Vorgangs neu gestartet werden müssen.
Compliance	Der prozentuale Anteil installierter Patches im Vergleich zu geplanten Patches.
Installiert	Die Anzahl der Geräte, die das Patch erhalten haben.
Fehlt	Die Anzahl der erkannten Geräte, die das Patch benötigen und auf die Bereitstellung warten.
Fehler	Die Anzahl der Geräte, bei denen die Bereitstellung nach der maximalen Anzahl der Versuche fehlgeschlagen ist. Die maximale Anzahl der Versuche für die Bereitstellung wird im Patch-Zeitplan konfiguriert. Siehe Konfigurieren von Patch-Zeitplänen.

Spalte	Beschreibung
Größe	Die Größe der Patch-Datei. • **Schwarz**: Inaktive oder deaktivierte Patches. • **Rot**: Patches, die Sie abonniert haben; für das betreffende Patch wurden aber zu diesem Zeitpunkt keine dazugehörigen Pakete heruntergeladen. Um anzuzeigen, welche dazugehörigen Pakete fehlen, klicken Sie auf den Patch-Namen zur Anzeige der Seite mit den Patch-Details. • **Größe = 0**: Keines der Patch-Pakete wurde heruntergeladen. • **Tatsächliche Größe** (ungleich null): Mindestens eines der Patch-Pakete wurde heruntergeladen.
Ersetzt	Patches, die durch andere Patches ersetzt wurden und nicht mehr benötigt werden.

Patch-Details anzeigen

Zu den Patch-Details zählen Herstellerinformationen, Bereitstellungsstatus und Hinweise. Außerdem können Sie Patches in den Patch-Details mit Labels versehen.

1. Rufen Sie die *Patch-Detailseite* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Sicherheit** und anschließend auf **Patch-Verwaltung**.
   c. Klicken Sie im Fensterbereich *Patch-Verwaltung* auf **Katalog**.
   d. Klicken Sie auf einen Patch-Namen.

      Die Seite *Patch-Details* wird mit vollständigen Informationen zum Patch angezeigt.

Anzahl von Patch-Bereitstellungsversuchen zurücksetzen

Wenn bei einer Patch-Bereitstellung die maximal zulässige Anzahl von Bereitstellungsversuchen erreicht wurde, kann die Anzahl der Wiederholungen zurückgesetzt werden.

Informationen zur Konfiguration einer maximal zulässigen Anzahl von Bereitstellungsversuchen finden Sie unter Konfigurieren von Patch-Zeitplänen.

Es gibt zwei Möglichkeiten, die Anzahl von Bereitstellungsversuchen zurückzusetzen: die Liste *Katalog* und die Seite *Patch-Detail*.

- Informationen zur Zurücksetzung der Patch-Bereitstellungsversuche über den Patch-Katalog finden Sie unter Anzahl der Patch-Bereitstellungsversuche über den Patch-Katalog zurücksetzen.
- Informationen zur Zurücksetzung der Patch-Bereitstellungsversuche über die Patch-Detailseite finden Sie unter Anzahl der Patch-Bereitstellungsversuche über die Patch-Detailseite zurücksetzen.

Anzahl der Patch-Bereitstellungsversuche über den Patch-Katalog zurücksetzen

Wenn bei einer Patch-Bereitstellung die maximal zulässige Anzahl von Bereitstellungsversuchen erreicht wurde, kann die Anzahl der Wiederholungen über die Seite *Katalog* zurückgesetzt werden.

1. Rufen Sie die Patch-Seite *Katalog* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Sicherheit** und anschließend auf **Patch-Verwaltung**.
   c. Klicken Sie im Fensterbereich *Patch-Verwaltung* auf **Katalog**.
2. Aktivieren Sie das Kontrollkästchen neben mindestens einem Patch/Bulletin in der Liste und wählen Sie dann **Aktion auswählen** > **Versuche zurücksetzen**.

   Die Anzahl der Bereitstellungsversuche wird auf Null zurückgesetzt.

Anzahl der Patch-Bereitstellungsversuche über die Patch-Detailseite zurücksetzen

Wenn bei einer Patch-Bereitstellung die maximal zulässige Anzahl von Bereitstellungsversuchen erreicht wurde, kann die Anzahl der Wiederholungen über die Patch-Detailseite zurückgesetzt werden.

1. Rufen Sie die Liste *Katalog* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Sicherheit** und anschließend auf **Patch-Verwaltung**.
   c. Klicken Sie im Fensterbereich *Patch-Verwaltung* auf **Katalog**.
2. Führen Sie einen der folgenden Schritte aus, um die Seite *Patch-Detail* aufzurufen:
   - Ist in der Dropdown-Liste **Anzeigen** die Option **Anwendbare Pakete** oder **Alle Pakete** ausgewählt, klicken Sie auf den Namen des Pakets und anschließend auf den Namen eines Patches innerhalb des Pakets.
   - Ist in der Dropdown-Liste **Anzeigen** die Option **Einzelne Patches** ausgewählt, klicken Sie auf den Namen eines Patches.
3. Scrollen Sie nach unten zum Abschnitt *Bereitstellungsstatus* und klicken Sie auf die Schaltfläche **Versuche zurücksetzen**.

   Die Anzahl der Bereitstellungsversuche wird auf Null zurückgesetzt.

Patch-Informationen für Geräte im Inventar anzeigen

Der Abschnitt *Inventar* enthält detaillierte Patch-Informationen zu verwalteten Geräten.

Diese Informationen umfassen Folgendes:

- Liste der auf dem Gerät bereitgestellten Patches
- Details der Patch-Zeitpläne, die für das Gerät gelten
- Informationen zu erfolgreichen und nicht erfolgreichen Patch- und Rollback-Versuchen

1. Rufen Sie die *Gerätedetailseite* der Organisation auf.
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Inventar** und anschließend auf **Dashboard**.
   c. Klicken Sie auf den Namen eines Geräts.
2. Scrollen Sie nach unten zum Abschnitt *Sicherheit*.
3. Klicken Sie auf **Status von Patch-Erkennung/-Bereitstellung**, um die Details zu *Status von Patch-Erkennung/-Bereitstellung* anzuzeigen.
4. Weitere Informationen erhalten Sie durch Klicken auf die Schaltfläche **Hilfe** neben *Geplante Aufgabe – Status* bzw. neben *Bereitstellungsstatus:*. ?.

Geräte mit fehlenden Patches anzeigen

Sie können die Geräte mit fehlenden Patches anzeigen, um zu ermitteln, warum sie nicht aktualisiert wurden.

1. Rufen Sie die Liste *Patch-Katalog* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Sicherheit** und anschließend auf **Patch-Verwaltung**.
   c. Klicken Sie im Fensterbereich *Patch-Verwaltung* auf **Katalog**.
2. Klicken Sie über der Katalogliste auf die Zahl nach dem Text *Geräte mit fehlenden Patches*.

   Die Liste *Geräte* erscheint und zeigt alle Geräte mit fehlenden Patches.

Anzeigen von statistischen Daten und Protokollen zu Patches

Statistische Daten und Protokolle zu Patches bieten eine Übersicht über die Patching-Aufgaben der Appliance.

Statistische Daten zu Patches anzeigen

Im Bereich *Patch-Verwaltung* können Sie Statistiken zu Patches anzeigen.

1. Rufen Sie den Bereich *Patch-Verwaltung* auf.
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.

b. Klicken Sie in der linken Navigationsleiste auf **Sicherheit** und anschließend auf **Patch-Verwaltung**.

Der Bereich *Patch-Verwaltung* wird mit statistischen Daten zu Patches angezeigt.

Patch-Protokoll anzeigen

Im Patch-Protokoll können Sie nach Fehlern beim Patch-Downloadvorgang suchen.

1. Navigieren Sie zur *Systemsteuerung* der Appliance:
   - **Wenn die Organisationskomponente nicht für die Appliance aktiviert ist, melden Sie sich bei der Administratorkonsole an: `https://appliance_hostname/admin`, und wählen Sie dann Einstellungen > Systemsteuerung aus.**
   - **Wenn die Organisationskomponente für die Appliance aktiviert ist, melden Sie sich bei der Systemverwaltungskonsole der Appliance an: `https://appliance_hostname/system`. Oder wählen Sie in der Dropdown-Liste rechts oben auf der Seite den Eintrag System aus, und klicken Sie dann auf Einstellungen > Systemsteuerung.**
2. Klicken Sie in der linken Navigationsleiste auf **Protokolle**, um die Seite *Protokolle* anzuzeigen.
3. Wählen Sie in der Dropdown-Liste *Protokoll* die Option **Patch-Download-Protokoll** aus.

Das Patch-Protokoll wird angezeigt.

Patches als inaktiv markieren

Sie können abonnierte Patches als inaktiv kennzeichnen, um zu verhindern, dass diese automatisch erkannt oder bereitgestellt werden.

1. Rufen Sie die Liste *Patch-Katalog* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Sicherheit** und anschließend auf **Patch-Verwaltung**.
   c. Klicken Sie im Fensterbereich *Patch-Verwaltung* auf **Katalog**.
2. Aktivieren Sie das Kontrollkästchen neben einem Patch.
3. Wählen Sie **Aktion auswählen** > **Status ändern in** > **Inaktiv**.

Ist in der Dropdown-Liste **Anzeigen** die Option **Anwendbare Pakete** oder **Alle Pakete** ausgewählt, werden alle Patches des ausgewählten Bulletins als inaktiv gekennzeichnet. Ist in der Dropdown-Liste **Anzeigen** die Option **Einzelne Patches** ausgewählt, werden alle ausgewählten Patches als inaktiv gekennzeichnet. Als inaktiv gekennzeichnete Patches werden beim nächsten geplanten Patch-Download automatisch aus dem Cache entfernt.

Patchen von Mac OS X Geräten

Sie können bei Bedarf Patches auf Mac OS X Geräte anwenden.

1. Rufen Sie die Liste *Patch-Katalog* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.

b. Klicken Sie in der linken Navigationsleiste auf **Sicherheit** und anschließend auf **Patch-Verwaltung**.

c. Klicken Sie im Fensterbereich *Patch-Verwaltung* auf **Katalog**.

2. Führen Sie einen der folgenden Schritte aus:

   - **Wählen Sie aus der Dropdown-Liste** *Anzeigen nach* **die Option Betriebssystem > Mac <OS X> aus.**
   - **Klicken Sie über der Tabelle auf die Registerkarte Erweiterte Suche und suchen Sie hier nach Mac OS X Patches.**
   - **Verwenden Sie die Funktion Smart Label, um die Patch-Liste automatisch anhand von vordefinierten Suchkriterien zu durchsuchen.**

3. Damit die Appliance Apple Sicherheitsaktualisierungen für Mac herunterladen kann, müssen Sie das entsprechende Betriebssystem auf der Seite *Patch-Abonnementeinstellungen* aus der Liste *Plattform: Mac* auswählen.

   Sie können mehrere Mac Betriebssysteme auswählen. Siehe Patches abonnieren

Windows-Funktionsaktualisierungen verwalten

Windows-Funktionsaktualisierungen sind neue Versionen von Microsoft Windows 10, die mehrmals jährlich veröffentlicht werden. Die Appliance ermöglicht es Ihnen, den Installationsprozess zu automatisieren, um die Leistung verwalteter Windows 10-Geräte zu verbessern und sie vor potenziellen Schwachstellen im Betriebssystem zu schützen.

Verwenden Sie die Appliance, um die neuesten Windows-Funktionsupdates für Ihre von der Appliance verwalteten Windows 10-Geräte zu erkennen und bereitzustellen.

HINWEIS: Diese Funktion wird nur auf Windows 10-Geräten mit einem halbjährlichen Kanalabonnement unterstützt. Sie ist nicht für Mac-, Linux- oder Windows-Geräte mit einer anderen Betriebssystemversion als 10 verfügbar.

Windows-Funktionsaktualisierungen abonnieren

Sie können Windows-Funktionsaktualisierungen für Ihre verwalteten Microsoft Windows 10-Geräte abonnieren.

Ermitteln Sie vor dem Abonnieren und Herunterladen von Windows-Funktionsaktualisierungen die Betriebssysteme, die auf den verwalteten Geräten installiert sind, und überprüfen Sie die Aktualisierungsanforderungen. Sie können nur Aktualisierungen für Ihre verwalteten Windows 10-Geräte herunterladen.

1. Rufen Sie die Seite *Abonnements für Windows-Funktionsaktualisierungen* auf:

   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.

   b. Klicken Sie in der linken Navigationsleiste auf **Sicherheit** und anschließend auf **Windows-Funktionsaktualisierungen**.

c. Klicken Sie im Fensterbereich *Windows-Funktionsaktualisierungen* auf **Abonnements**.

2. Geben Sie die *Abonnementeinstellungen* an. Welche Patches heruntergeladen werden, hängt von den im Abonnement angegebenen Betriebssystemen und Gebietsschemata ab.

Option	Beschreibung
Versionen der Windows-Funktionsaktualisierung	Laden Sie ausgewählten Windows-Funktionsaktualisierungen herunter. Klicken Sie auf die Bearbeitungsschaltfläche, um die Betriebssystemliste zu bearbeiten: . Klicken Sie auf **Versionen auswählen** und wählen Sie die Aktualisierungsversionen aus, die Sie auf Ihren verwalteten Windows 10-Geräten installieren möchten. Sollen Windows-Funktionsaktualisierungen ignoriert werden, wählen Sie **Deaktiviert** aus. Die ausgewählten Elemente werden nach dem Speichern der Einstellungen angezeigt.
Gebietsschemata	Lädt Patches für die ausgewählten Sprachen herunter. Klicken Sie auf die Bearbeitungsschaltfläche, um die Gebietsschemaliste zu bearbeiten: . Wählen Sie **Alle Gebietsschemata** aus, um Patches unabhängig vom Gebietsschema herunterzuladen, oder aktivieren Sie die Kontrollkästchen neben den gewünschten Gebietsschemata. Die ausgewählten Elemente werden nach dem Speichern der Einstellungen angezeigt.

HINWEIS: Um Windows-Funktionsaktualisierungen zu abonnieren, müssen mindestens eine Version und ein Gebietsschema ausgewählt werden.

3. Klicken Sie auf **Speichern**.

Ausgewählte Windows-Funktionsaktualisierungen werden zum nächsten geplanten Download-Zeitpunkt automatisch heruntergeladen.

Als Nächstes können Sie die Download-Einstellungen für Windows-Funktionsupdates konfigurieren. Siehe Download-Einstellungen für Patch- und Funktionsaktualisierungen auswählen.

Zeitpläne für Windows-Funktionsaktualisierungen konfigurieren

Sie können Zeitpläne für Windows-Funktionsaktualisierungen erstellen und konfigurieren sowie einen Zeitpunkt für ihre Ausführung festlegen. Zeitpläne für Windows-Funktionsaktualisierungen wirken sich nicht auf verwaltete Installationen oder andere Verteilungen aus.

1. Rufen Sie den Assistenten *Windows Feature Update Schedule Detail (Zeitplandetails für Windows-Funktionsupdates)* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.

b. Klicken Sie in der linken Navigationsleiste auf **Sicherheit** und anschließend auf **Windows-Funktionsaktualisierungen**.

c. Klicken Sie im Fensterbereich *Windows-Funktionsaktualisierungen* auf **Zeitpläne**.

d. Führen Sie eine der folgenden Aktionen aus, um die Seite *Windows Feature Update Schedules (Zeitplan für Windows-Funktionsupdates)* anzuzeigen:

- Um einen neuen Zeitplan für Windows-Funktionsupdates mithilfe des Assistenten zu erstellen, klicken Sie auf *Schedule Detail (Details zum Zeitplan)* auf **Aktion wählen > Neu (Assistent)**.
- Klicken Sie zum Erstellen eines neuen Zeitplans für Windows-Funktionsupdates auf der Seite *Schedule Detail (Details zum Zeitplan)* auf **Aktion wählen > New (Classic) (Neu (Klassisch))**.
- Zum Bearbeiten eines vorhandenen Zeitplans klicken Sie in der Liste auf den Namen des Zeitplans und dann auf der Seite *Windows Feature Update Schedule Summary (Zeitplan für Windows-Funktionsupdates - Übersicht)* auf **Bearbeiten**.

  Die Seite *Schedule Detail (Details zum Zeitplan)* oder der Assistent wird wie ausgewählt angezeigt. Für jede Auswahloption sind die gleichen Einstellungen verfügbar: Sie können zwischen der Seite und dem Assistenten wechseln, indem Sie in der rechten oberen Ecke auf **Klassische Ansicht** oder **Wizard View (Assistentenansicht)** klicken.

2. Konfigurieren Sie allgemeine Informationen zum Zeitplan:

Option	Beschreibung
Name	Ein Name, der den Zeitplan genau bezeichnet. Dieser Name wird auf der Listenseite *Zeitpläne für Windows-Funktionsaktualisierungen* angezeigt.
Beschreibung	Eine kurze Beschreibung des Zeitplans für Windows-Funktionsupdates.

3. Konfigurieren Sie im Abschnitt *Windows-Funktionsaktualisierung auswählen* die folgenden Optionen:

Option	Beschreibung
Build auswählen	Wählen Sie eine Version der Windows-Funktionsaktualisierung aus, die erkannt, zur Verfügung gestellt oder bereitgestellt werden soll. In diesem Abschnitt werden die in Ihrem Abonnement ausgewählten Aktualisierungen aufgeführt.
Editionen auswählen	Wählen Sie mindestens ein Edition der ausgewählten Version aus. In diesem Abschnitt werden alle Editionen für die ausgewählte Version aufgeführt, z. B. Business- und Consumer-Editionen für die verschiedenen Plattformen (32- und 64-Bit).

4. Wählen Sie eine der folgenden Aktionen aus.

   Diese Aktionen sind identisch mit den Aktionen für die Patch-Zeitpläne. Siehe Konfigurieren von Patch-Zeitplänen.

Aktion	Beschreibung
Erkennen	Sucht nach kompatiblen Windows-Funktionsaktualisierungen.
Erkennen und zur Verfügung stellen	Sucht nach kompatiblen Windows-Funktionsaktualisierungen und lädt die

Aktion	Beschreibung
	entsprechenden Dateien zur späteren Bereitstellung auf das Agentengerät herunter.
Detect, Stage and On-demand Deploy (Erkennen, zur Verfügung stellen und bedarfsgerecht bereitstellen)	Erkennt Windows-Funktionsupdates, die auf verwalteten Geräten installiert sind oder fehlen, lädt die entsprechenden Dateien auf das Agent-Gerät herunter und zeigt ein Benachrichtigungssymbol auf der Windows-Taskleiste an. • Diese Zeitpläne sind nur für Windows-Geräte mit Agenten der Version 11.0 oder höher verfügbar. • Die Option *Agentenstatussymbol auf Gerät* muss in den Kommunikationseinstellungen des Agenten aktiviert sein. Diese Einstellungen finden Sie auf der Seite *Organisationsdetails*, unter *Kommunikations- und Agenteneinstellungen* (falls eine oder mehrere Organisationskomponenten aktiviert sind) oder auf der Seite *Kommunikationseinstellungen* (falls Sie über keine Organisationskomponente verfügen). Weitere Informationen hierzu finden Sie unter Agentenkommunikation und Protokolleinstellungen konfigurieren.
Erkennen und bereitstellen	Sucht nach kompatiblen Windows-Funktionsaktualisierungen, lädt die entsprechenden Dateien auf das Agentengerät herunter und stellt das Update auf den ausgewählten Geräten bereit.

5. Wählen Sie die Zielgeräte mithilfe der folgenden Optionen aus.

   Diese Optionen sind identisch mit denen, die in den Aktionen für Patch-Zeitpläne angezeigt werden. Siehe Konfigurieren von Patch-Zeitplänen.

Aktion	Beschreibung
Alle Geräte	Wählen Sie diese Optionen aus, um diesen Zeitplan auf alle verwalteten Geräte anzuwenden. Deaktivieren Sie das Kontrollkästchen, um die Patch-Aktion auf bestimmte Labels oder Geräte zu beschränken.
Gerätelabels	Die Aktion wird auf Funktionsaktualisierungen beschränkt, die das von Ihnen ausgewählte Label aufweisen. Diese Option wird am häufigsten verwendet. a. Klicken Sie auf **Verknüpfte Labels verwalten**. b. Das Dialogfeld *Labels auswählen* wird angezeigt. Ziehen Sie mindestens ein Label nach Bedarf in den Bereich *Ausführung begrenzen auf*, und klicken Sie dann auf **OK**. Um diese Option verwenden zu können, müssen Smart Labels für die Funktionsaktualisierungen

Aktion	Beschreibung
	vorhanden sein. Siehe Smart Labels für Patches verwenden.
Geräte	Führt auf den von Ihnen ausgewählten Geräten Patch-Aktionen aus. • Um nach Geräten zu suchen, beginnen Sie mit einer entsprechenden Eingabe in das Feld. • Um alle angegebenen Geräte zu entfernen und erneut zu starten, klicken Sie auf **Alle entfernen**. • Benutzer mit eingeschränkten Zugriffsrechten sehen nur die Geräte, die mit ihrer Rolle verknüpft sind, wenn der Rolle ein Label zugewiesen ist. Weitere Informationen zu Benutzerrollen finden Sie unter Benutzerrollen hinzufügen oder bearbeiten.

6. Geben Sie im Abschnitt *Zeitplan* die entsprechenden Optionen für den Zeitplan an.

   Diese Optionen sind identisch mit denen, die in den Aktionen für Patch-Zeitpläne angezeigt werden. Siehe Konfigurieren von Patch-Zeitplänen.

Option	Beschreibung
Kein(e)	Die Ausführung erfolgt im Zusammenhang mit einem Ereignis anstatt zu einem bestimmten Datum oder zu einem bestimmten Zeitpunkt. Diese Option ist nützlich, wenn Sie Patches manuell auf Server anwenden oder Patch-Aktionen ausführen möchten, die nicht nach einem Zeitplan ausgeführt werden sollen.
Alle _ Stunden	Der Vorgang wird im angegebenen Intervall durchgeführt.
Täglich/an einem bestimmten Tag um HH:MM	Die Erfassung wird täglich zu einem bestimmten Zeitpunkt oder an einem bestimmten Wochentag um eine bestimmte Uhrzeit ausgeführt.
Ausführen am n-ten jedes Monats/eines bestimmten Monats um HH:MM	Am **n**. Tag jedes Monats ausführen (beispielsweise am ersten oder zweiten) Tag des Monats oder in einem bestimmten Monat zu einer bestimmten Zeit.
Ausführen am n-ten Wochentag **jedes Monats/ eines bestimmten Monats um HH:MM**	Die Erfassung wird jeden Monat oder in einem bestimmten Monat an einem festgelegten Wochentag zu einer festgelegten Uhrzeit ausgeführt.

Benutzerdefiniert	Ausführung nach einem benutzerdefinierten Zeitplan.
	Verwenden Sie das Standard-5-Feld-Cron-Format (das erweiterte Cron-Format wird nicht unterstützt):
	`* * * * *`
	`| | | | +————Wochentag (0-6) (Sonntag=0)`

Option	Beschreibung

	`| | | +————————Monat (1-12)`
	`| | +————————Monatstag (1-31)`
	`| +————————Stunde (0-23)`
	`+————————Minute (0-59)`
	
	Verwenden Sie bei der Angabe von Werten die folgenden Zeichen:
	
	• **Leerzeichen( )**: Die einzelnen Felder mit einem Leerzeichen trennen.
	• **Sternchen (*)**: Ein Sternchen repräsentiert den gesamten Wertebereich in einem Feld. Zum Beispiel repräsentiert ein Sternchen im Stundenfeld eine beliebige Stunde.
	• **Kommas (,)**: Mehrere Werte in einem Feld werden mit einem Komma getrennt. Zum Beispiel werden mit `0,6` im Feld „Wochentag“ Sonntag und Samstag angegeben.
	• **Bindestriche (-)**: Mit einem Bindestrich wird ein Wertebereich in einem Feld angegeben. Zum Beispiel entspricht `1-5` im Feld „Wochentag“ `1,2,3,4,5`, d. h. Montag bis Freitag.
	• **Schrägstriche (/)**: Die Angabe der Zeitabstände, mit denen eine Aktion wiederholt werden soll, erfolgt mit einem Schrägstrich. Zum Beispiel entspricht `*/3` im Feld Stunde `0,3,6,9,12,15,18,21`. Das Sternchen (`*`) gibt jede Stunde an, mit `/3` erfolgt aber eine Einschränkung auf durch drei teilbare Stunden.
	
	Beispiele:
	
	• `15 * * * * Jeden Tag 15 Minuten nach jeder vollen Stunde ausführen`
	• `0 22 * * * Jeden Tag um 22:00 Uhr ausführen`
	• `0 0 1 1,6 * Am 1. Januar und 1. Juni um 00:00 Uhr ausführen`
	• `30 8,12 * * 1-5 An Wochentagen um 08:30 Uhr und 12:30 Uhr ausführen`
	• `0 2 */2 * * Jeden zweiten Tag um 02:00 Uhr ausführen`

Aufgabenplan anzeigen	Klicken Sie, um den Aufgabenplan anzuzeigen. Im Dialogfeld *Taskplan* wird eine Liste der geplanten Ziele angezeigt. Klicken Sie auf eine Aufgabe, um die Aufgabendetails anzuzeigen. Weitere Informationen hierzu finden Sie unter Aufgabenpläne anzeigen.
Zeitzone	Die Zeitzone, die beim Planen der Aktion verwendet werden soll. Wählen Sie **Server** aus, um die

Option	Beschreibung
	Zeitzone der Appliance zu verwenden. Wählen Sie **Agent** aus, um die Zeitzone des verwalteten Geräts zu verwenden.
Wenn offline, bei nächster Verbindung ausführen	Wenn das Gerät derzeit offline ist, wird die Aktion ausgeführt, sobald das verwaltete Gerät das nächste Mal eine Verbindung mit der Appliance herstellt. Diese Option eignet sich für Notebooks und andere Geräte, die regelmäßig offline sind. Wenn diese Option nicht ausgewählt wird und das Gerät offline ist, wird die Aktion erst zum nächsten geplanten Zeitpunkt ausgeführt.
Ausführung nach Wiederverbinden verzögern	Der Zeitplan wird um eine angegebene Zeitspanne verzögert. Die Zeitspanne der Verzögerung beginnt zu dem Zeitpunkt, für den die Ausführung der Patch-Aktion geplant wurde.
Beenden nach	Das Zeitlimit für Patch-Aktionen. Wenn Sie beispielsweise festlegen, dass Patches um 4.00 Uhr ausgeführt werden sollen, sollten Sie möglicherweise auch festlegen, dass alle Patch-Aktionen um 7.00 Uhr beendet werden, um Probleme hinsichtlich der Bandbreite zu vermeiden, wenn Benutzer mit der Arbeit beginnen. Hierzu können Sie im Minutenfeld den Wert **180** angeben. Wenn dieses Zeitlimit erreicht wird, werden alle Patch-Aufgaben, die derzeit ausgeführt werden, angehalten und der zugehörige Status im Sicherheitsprotokoll wird mit *Angehalten* angegeben. Diese Patch-Aufgaben werden bei der nächsten Ausführung nicht fortgesetzt, sondern beginnen vielmehr bei jeder geplanten Patch-Aktion wieder von vorn.

7. Klicken Sie auf **Speichern**.

   Die Seite *Windows Feature Update Schedule Summary (Zeitplan für Windows-Funktionsupdates - Übersicht)* wird eingeblendet, auf der der neu erstellte oder aktualisierte Zeitplan angezeigt wird. Weitere Informationen zu dieser Seite finden Sie unter Status von Windows-Funktionsupdates anzeigen.

   - Wenn Sie Geräte hinzufügen, die den Kriterien für das Smart Label entsprechen, werden sie automatisch in den Aktualisierungszeitplan aufgenommen.
   - Wenn die Aktualisierungen auf das Agent-Gerät heruntergeladen wurden und bereitgestellt werden können, wird das KACE Agent-Symbol in der Windows-Taskleiste und im Menü aktualisiert, um darauf hinzuweisen, dass Aktionen für den Agenten verfügbar sind. Klicken Sie zum Installieren der Aktualisierungen auf dem Agent-Gerät in der Windows-Taskleiste auf den KACE Agent, und wählen Sie **Deploy staged patches (Bereitgestellte Patches bereitstellen)**. Weitere Informationen zu den KACE Agent-Symbolen finden Sie unter Verwalten des KACE Agent auf Windows-Geräten über die Windows-Taskleiste.

Zeitpläne für Windows-Funktionsaktualisierung anzeigen

Sie können zusammenfassende Informationen für die Zeitpläne für Windows-Funktionsaktualisierungen anzeigen, die auf der Appliance vorhanden sind. Wenn die Organisationskomponente für Ihre Appliance aktiviert ist, können Sie die Zeitpläne für Windows-Funktionsupdates für jede Organisation separat anzeigen.

1. Rufen Sie die Seite *Zeitpläne für Windows-Funktionsaktualisierung* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Sicherheit** und anschließend auf **Windows-Funktionsaktualisierungen**.
2. Klicken Sie im Fensterbereich *Windows-Funktionsaktualisierungen* auf **Zeitpläne**.

   Die auf der Seite *Zeitpläne für die Windows-Funktionsaktualisierungen* verfügbaren Spalten sind identisch mit denen auf der Seite *Patch-Zeitpläne*. Weitere Informationen zu den Feldern auf der Seite *Patch-Zeitpläne* finden Sie unter Liste der Patch-Zeitpläne anzeigen.
3. (Optional) Um die angezeigten Spalten zu ändern, wählen Sie aus der Dropdown-Liste *Tabellenoptionen* rechts über der Tabelle **Spaltenanzeige** aus.

Details zu Windows-Funktionsupdate-Zeitplänen prüfen

Wenn Sie einen Zeitplan für Windows-Funktionsupdates konfigurieren, werden auf dieser Seite Details zur Konfiguration des Zeitplans und dessen Status angezeigt.

1. Rufen Sie die Seite *Windows Feature Update Schedule Summary (Zeitplan für Windows-Funktionsupdates - Übersicht)* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Sicherheit** und anschließend auf **Windows-Funktionsaktualisierungen**.
   c. Klicken Sie im Fensterbereich *Windows-Funktionsaktualisierungen* auf **Zeitpläne**.
   d. Klicken Sie auf den Namen eines Zeitplans für Windows-Funktionsaktualisierungen.
2. Überprüfen Sie den Inhalt des Abschnitts *Konfiguration*.

Option	Beschreibung
Erstellt	Das Datum und die Uhrzeit der Erstellung des Zeitplans.
Geändert	Das Datum und die Uhrzeit der letzten Änderung des Zeitplans.

Option	Beschreibung
Letzte Ausführung	Das Datum und die Uhrzeit der letzten Ausführung des Zeitplans.
Name	Ein Name, der den Zeitplan genau bezeichnet. Dieser Name wird auf der Listenseite *Zeitpläne für Windows-Funktionsaktualisierungen* angezeigt.
Aktion	Die mit dem Zeitplan verbundene Aktion: • **Erkennen**: Sucht nach kompatiblen Windows-Funktionsaktualisierungen. • **Erkennen und zur Verfügung stellen**: Sucht nach kompatiblen Windows-Funktionsaktualisierungen und lädt die entsprechenden Dateien zur späteren Bereitstellung auf das Agentengerät herunter. • **Detect, Stage and On-demand Deploy (Erkennen, zur Verfügung stellen und bedarfsgerecht bereitstellen)**: Erkennt Windows-Funktionsupdates, die auf verwalteten Geräten installiert sind oder fehlen, lädt die entsprechenden Dateien auf das Agent-Gerät herunter und zeigt auf der Windows-Taskleiste des Agent-Geräts eine Benachrichtigung an, dass die Updates bereit für die Bereitstellung sind. Der Benutzer kann dann den Bereitstellungsvorgang nach Belieben initiieren. ◦ Diese Zeitpläne sind nur für Windows-Geräte mit Agenten der Version 11.0 oder höher verfügbar. ◦ Die Option *Agentenstatussymbol auf Gerät* muss in den Kommunikationseinstellungen des Agenten aktiviert sein. Diese Einstellungen finden Sie auf der Seite *Organisationsdetails*, unter *Kommunikations- und Agenteneinstellungen* (falls eine oder mehrere Organisationskomponenten aktiviert sind) oder auf der Seite *Kommunikationseinstellungen* (falls Sie über keine Organisationskomponente verfügen). Weitere Informationen hierzu finden Sie unter Agentenkommunikation und Protokolleinstellungen konfigurieren. • **Erkennen und bereitstellen:** Sucht nach kompatiblen Windows-Funktionsaktualisierungen, lädt die entsprechenden Dateien auf das Agentengerät herunter und stellt das Update auf den ausgewählten Geräten bereit.

Option	Beschreibung
Beschreibung	Eine kurze Beschreibung des Zeitplans für Windows-Funktionsupdates.
Geräte	Dieses Feld wird nur angezeigt, wenn der Zeitplan so konfiguriert ist, dass er auf alle Geräte angewendet wird.
Windows-Funktionsaktualisierung	Der Name und die Version des Windows-Funktionsupdates.
Label des Geräts	Mindestens ein Smart Label, das mit den Geräten verknüpft ist, für die der Zeitplan ausgeführt wird. Weitere Informationen hierzu finden Sie unter Smart Labels für Patches verwenden. Dieses Feld wird nur angezeigt, wenn der Zeitplan so konfiguriert ist, dass er auf ausgewählte Geräte angewendet wird.
Gerätename	Mindestens ein ausgewähltes Geräte, für das der Zeitplan ausgeführt wird. Dieses Feld wird nur angezeigt, wenn der Zeitplan so konfiguriert ist, dass er auf ausgewählte Geräte angewendet wird.
Label finden	Mindestens ein Smart Label, das mit den geplanten Aktualisierungen verknüpft ist. Weitere Informationen hierzu finden Sie unter Smart Labels für Patches verwenden. Dieses Feld wird nur angezeigt, wenn der Zeitplan so konfiguriert ist, dass ausgewählte Aktualisierungen erkannt werden.
Warnungen	**Detect and Deploy schedules only (Nur Zeitpläne für Erkennen und Bereitstellen)**. Die Benachrichtigungen, die Benutzern bei der Ausführung von Aktualisierungsaktionen angezeigt werden. • **OK**: Sofort ausführen. • **Abbrechen**: Abbrechen bis zur nächsten geplanten Ausführung. • **Snooze**: Der Benutzer erhält nach Ablauf der *Snooze-Dauer* erneut eine Eingabeaufforderung. **HINWEIS:** Benachrichtigungen sind in den Zeitplänen für Erkennen sowie Erkennen und zur Verfügung stellen nicht verfügbar.
Neustart	**Detect and Deploy schedules only (Nur Zeitpläne für Erkennen und Bereitstellen)**. Die Optionen für den Neustart des verwalteten Geräts. • **Kein Neustart**: Das Gerät wird nicht neu gestartet, obwohl möglicherweise ein Neustart erforderlich ist, damit die Aktualisierung wirksam wird. Es wird davon abgeraten, diese Option zu verwenden,

Option	Beschreibung
	da die Bereitstellung von Aktualisierungen ohne einen erforderlichen Neustart die Stabilität der Systeme beeinträchtigen kann. Zudem werden Aktualisierungen, die einen Neustart erfordern, erst nach dem Neustart als bereitgestellt angezeigt. • **Eingabeaufforderung für Benutzer**: Vor dem Geräteneustart wird gewartet, bis der Benutzer den Neustart akzeptiert hat. Wenn der Benutzer den Neustart per Snooze verschiebt oder abbricht, wird der Aktualisierungsvorgang angehalten, bis ein Neustart durchgeführt wird. Wenn Sie im Dialogfeld "Agent", das auf dem Zielgerät angezeigt wird, eine Snooze-Dauer auswählen, wird die Neustartaufforderung für das angegebene Snooze-Intervall angehalten. • **Neustart erzwingen**: Ein Neustart wird durchgeführt, sobald eine Aktualisierung bereitgestellt wurde, die einen Neustart erfordert. Erzwungene Neustarts können nicht abgebrochen werden. Neustart erzwingen eignet sich gut für Desktops und Server. Unter Umständen ist es nicht sinnvoll, auf Notebooks einen Neustart zu erzwingen. "Neustart erzwingen" eignet sich für Server, da diese in der Regel keine speziell zugewiesenen Benutzer besitzen. Es ist jedoch wichtig, Benutzer darauf hinzuweisen, dass Dienste nicht verfügbar sind, wenn Server aktualisiert und neu gestartet werden. Siehe Best Practices für den Patch-Vorgang.
Planen	Der ausgewählte Aktualisierungszeitplan. Klicken Sie auf **Aufgabenplan anzeigen**, um eine detaillierte Aufgabenplanung anzuzeigen. Klicken Sie im daraufhin angezeigten Dialogfeld auf eine Aufgabe, um die Aufgabendetails zu überprüfen. Weitere Informationen hierzu finden Sie unter Aufgabenpläne anzeigen.
Wenn offline, bei nächster Verbindung ausführen	Wenn das Gerät derzeit offline ist, wird die Aktion ausgeführt, sobald das verwaltete Gerät das nächste Mal eine Verbindung mit der Appliance herstellt.
Ausführung nach Wiederverbinden verzögern	Diese Option gibt an, wie lange sich der Zeitplan verzögert. Die Zeitspanne der Verzögerung beginnt zu dem Zeitpunkt, für den die Ausführung der Aktualisierungsaktion geplant wurde.
Beenden nach	Diese Option gibt die maximale Zeitspanne für die Ausführung des Zeitplans an. Wenn dieses

Option	Beschreibung
	Zeitlimit erreicht ist, werden alle laufenden Aktualisierungsaufgaben angehalten.

3. Überprüfen Sie im Abschnitt *Zeitplanstatus* den Gesamtstatus des Zeitplans auf einer der folgenden Registerkarten:

Registerkarte	Inhalt
Nach Computer	Geräte, die für die Aktualisierung ausgewählt wurden. Jeder Eintrag zeigt den Namen und die IP-Adresse des Geräts, den Aktualisierungsstatus (siehe Felder auf den Detailseiten des Patch-Zeitplans), die Aktualisierungsergebnisse und das Datum an, an dem die Aktualisierung abgeschlossen wurde. Sie können Geräteknoten erweitern, um die entsprechenden Aktualisierungen anzuzeigen. Jeder Eintrag zeigt die Aktualisierungs-ID, die zugehörige Knowledge Base-Artikelnummer, den Aktualisierungsnamen und den aktuellen Status an (Installiert, Nicht installiert, Bereitgestellt und Fehler bei Erkennung, Staging oder Bereitstellung).
By Feature Update (Nach Funktionsaktualisierung)	Aktualisierungen, die für Erkennung, Staging und Bereitstellung ausgewählt wurden. Jeder Eintrag zeigt die Aktualisierungs-ID, die zugehörige Knowledge Base-Artikelnummer, den Aktualisierungsnamen und die Anzahl der aktualisierten und nicht aktualisierten Geräte an, sowie die Geräte, bei denen Fehler bei der Erkennung oder Bereitstellung aufgetreten sind.
Installiert	Updates wurden erfolgreich auf Geräten installiert. Jeder Eintrag zeigt die Aktualisierungs-ID, die zugehörige Knowledge Base-Artikelnummer und den Namen der Aktualisierung an. Sie können einen Aktualisierungsknoten erweitern, um die Geräte anzuzeigen, auf denen die Aktualisierung installiert ist.
Nicht installiert	Aktualisierungen, die nicht auf Geräten installiert wurden. Jeder Eintrag zeigt die Aktualisierungs-ID, die zugehörige Knowledge Base-Artikelnummer und den Namen der Aktualisierung an. Sie können einen Aktualisierungsknoten erweitern, um die Geräte anzuzeigen, auf denen die Aktualisierung installiert werden soll.
Bereitgestellt (Staging)	Aktualisierungen, die für die Installation bereitgestellt werden (Staging). Staging bezieht sich auf Aktualisierungsdateien, die zur späteren Bereitstellung auf das Agent-Gerät kopiert werden. Jeder Eintrag zeigt die Aktualisierungs-ID, die zugehörige Knowledge Base-Artikelnummer und den Namen der Aktualisierung an. Sie können einen Aktualisierungsknoten erweitern, um die Geräte anzuzeigen, auf denen die Aktualisierung installiert werden soll.

Registerkarte	Inhalt
Fehler bei der Erkennung	Unvollständige Aktualisierungen, die zu einem Erkennungsfehler geführt haben. Jeder Eintrag zeigt die Aktualisierungs-ID, die zugehörige Knowledge Base, den Aktualisierungsnamen und den zugehörigen Fehlercode an (siehe Fehlercodes aufgrund von Patching und Skripterstellung). Sie können Aktualisierungsknoten erweitern, um die Geräte anzuzeigen, auf denen der Fehler aufgetreten ist.
Stage Failures (Staging-Fehler)	Unvollständige Aktualisierungen, die zu einem Staging-Fehler geführt haben. Jeder Eintrag zeigt die Aktualisierungs-ID, die zugehörige Knowledge Base-Artikelnummer, den Aktualisierungsnamen und den zugehörigen Fehlercode an (siehe Fehlercodes aufgrund von Patching und Skripterstellung). Sie können Aktualisierungsknoten erweitern, um die Geräte anzuzeigen, auf denen der Fehler aufgetreten ist.
Fehler bei der Bereitstellung	Unvollständige Aktualisierungen, die zu einem Bereitstellungsfehler geführt haben. Jeder Eintrag zeigt die Aktualisierungs-ID, die zugehörige Knowledge Base, den Aktualisierungsnamen und den zugehörigen Fehlercode an (siehe Fehlercodes aufgrund von Patching und Skripterstellung). Sie können Aktualisierungsknoten erweitern, um die Geräte anzuzeigen, auf denen der Fehler aufgetreten ist.

4. **Optional**. Nach Überprüfung der Zeitplandetails können Sie eine der folgenden Aktionen durchführen:
   - Klicken Sie zum Bearbeiten des Aktualisierungszeitplans auf **Bearbeiten**. Weitere Informationen hierzu finden Sie unter Zeitpläne für Windows-Funktionsaktualisierungen konfigurieren.
   - Klicken Sie zum Ausführen des Aktualisierungszeitplans auf **Jetzt ausführen**.
   - Um eine Kopie des Aktualisierungszeitplans zu erstellen, klicken Sie auf **Duplizieren**.
   - Um den Aktualisierungszeitplan zu löschen, klicken Sie auf **Löschen**.

Verfügbare Windows-Funktionsaktualisierungen anzeigen

Nachdem Sie Windows-Funktionsaktualisierungen abonniert und die Updates heruntergeladen haben, können Sie die verfügbaren Updates anzeigen.

Sie müssen Windows-Funktionsaktualisierungsversionen abonnieren und zugehörige Download-Einstellungen auswählen, um zugehörige Aktualisierungen anzuzeigen. Siehe:

- Windows-Funktionsaktualisierungen abonnieren
- Download-Einstellungen für Patch- und Funktionsaktualisierungen auswählen

1. Rufen Sie die Seite *Windows-Funktionsaktualisierung* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen

Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.

b. Klicken Sie in der linken Navigationsleiste auf **Sicherheit** und anschließend auf **Windows-Funktionsaktualisierungen**.

c. Klicken Sie im Fensterbereich *Windows-Funktionsaktualisierungen* auf **Katalog**.

2. Suchen Sie nach Windows-Funktionsaktualisierungen.

a. Geben Sie die Suchkriterien in das Suchfeld ein.

Beispiel: `1909`.

b. Drücken Sie die **Eingabetaste**.

Die Listenseite wird aktualisiert und zeigt nur die Windows-Funktionsaktualisierungen mit Version 1909 an.

Status von Windows-Funktionsupdates anzeigen

Die Details zu Windows-Funktionsupdates umfassen Informationen zum Anbieter und Bereitstellungsstatus.

1. Rufen Sie die Seite *Details zu Windows-Funktionsupdates* auf:

a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.

b. Klicken Sie in der linken Navigationsleiste auf **Sicherheit** und anschließend auf **Windows-Funktionsaktualisierungen**.

c. Klicken Sie im Fensterbereich *Windows-Funktionsaktualisierungen* auf **Katalog**.

d. Klicken Sie auf den Namen eines Windows-Funktionsupdates.

Die Seite *Details zu Windows-Funktionsupdates* wird mit vollständigen Informationen zum ausgewählten Windows-Funktionsupdate angezeigt.

Verwalten von Dell Geräten und Aktualisierungen

Mit der Appliance können Sie Geräteaktualisierungen von Dell verwalten.

Zu diesen Aktualisierungen zählen:

- Software und Firmware für Server.
- Software und Firmware für Client-Geräte.
- Einige von Dell gelieferte Anwendungen

HINWEIS: Server- und Client-Geräte beziehen sich auf Dell Server- und Client-Hardware, nicht auf ihr Server- oder Client-Betriebssystem.

Auf allen Dell Geräten, die aktualisiert werden müssen, muss der Dell Open Manage Inventory Agent installiert sein, entweder als Client- oder Serverversion. Diese Komponente ist standardmäßig in allen Dell Aktualisierungen enthalten und muss nicht manuell hinzugefügt werden. Wenn der Dell Open Manage Inventory Client nicht auf einem Zielgerät vorhanden ist, wird er während des ersten Bereitstellungsprozesses installiert.

HINWEIS: Dell Hardware-Aktualisierungen funktionieren nur mit dem KACE Agent 11.1 oder höher. Ältere Agentenversionen unterstützen diese Funktion nicht.

Führen Sie den Bericht *Unterstützte Dell Modelle* aus, um anzuzeigen, für welche Dell Computer Dell Client-Aktualisierungen unterstützt werden. Siehe Ausführen von Berichten für Einzelorganisationen sowie von konsolidierten Berichten.

Unterschiede zwischen Patchen und Dell Aktualisierungen

Das Patchen unterscheidet sich von Dell Aktualisierungen unter anderem beim Abonnementprozess, bei den Aktionsnamen und bei dem Ort, an dem sich die Verwaltungsprozesse befinden.

Unterschiede zwischen Patchen und Dell Aktualisierungen:

- Auf allen Dell Geräten, die aktualisiert werden müssen, muss der Dell Open Manage Inventory Agent installiert sein, entweder als Client- oder Serverversion.
- Der Abonnementvorgang für Dell Aktualisierungen unterscheidet sich vom Abonnementvorgang für Patches der Appliance. Anweisungen zum Abonnieren von Dell Aktualisierungen finden Sie unter Download-Einstellungen für Dell Aktualisierung auswählen.
- Die für Patch-Aktionen verwendeten Namen unterscheiden sich:

Aktion	Begriff beim Patchen	Begriff bei Dell Aktualisierungen	Begriff verwendet in:
Installieren Sie das Patch oder die Aktualisierung auf den von Ihnen verwalteten Geräten.	Bereitstellung	Aktualisieren	Verwalten von Dell Geräten und Aktualisierungen

- Patches und Dell Aktualisierungen werden in der **Administratorkonsole** über verschiedene Optionen verwaltet und ausgeführt:

Aktion	Wo zu finden
Dell Aktualisierungen ausführen	**Sicherheit > Dell Aktualisierungen**
Dell Aktualisierungen verwalten	Wenn die Organisationskomponente für Ihre Appliance **nicht aktiviert** ist: **Administratorkonsole > Einstellungen > Dell Update Download Settings (Download-Einstellungen für Dell Aktualisierung)** Wenn die Organisationskomponente für Ihre Appliance **aktiviert** ist: **Systemverwaltungskonsole > System > Einstellungen > Dell Update Download Settings (Download-Einstellungen für Dell Aktualisierung)**
Patch-Zeitpläne ausführen	**Sicherheit > Zeitpläne**
Patches verwalten	**Sicherheit > Abonnements**

Download-Einstellungen für Dell Aktualisierung auswählen

Vor dem Erstellen von Zeitplänen für die Aktualisierung von Geräten müssen Sie zunächst Katalogaktualisierungen konfigurieren und planen.

Dell Aktualisierungspakete werden in Form von **Katalogen** zur Verfügung gestellt. Es gibt einen Katalog für Server und einen für Clients.

1. Rufen Sie die Seite *Dell Update Download Settings (Download-Einstellungen für Dell Aktualisierung)* auf:
   - **Ist die Organisationskomponente auf Ihrer Appliance nicht aktiviert, klicken Sie auf** *Sicherheit* **und anschließend auf** *Dell Aktualisierungen***.**
   - **Wenn die Organisationskomponente für die Appliance aktiviert ist, melden Sie sich bei der Systemverwaltungskonsole der Appliance an: `https://appliance_hostname/system`. Oder wählen Sie in der Dropdown-Liste rechts oben auf der Seite den Eintrag System aus, und klicken Sie dann auf Einstellungen > Systemsteuerung.**
2. Klicken Sie auf **Dell Update Download Settings (Download-Einstellungen für Dell Aktualisierung)**.

   Der aktuelle Status des Dell Katalogs wird angezeigt.
3. Wählen Sie im Abschnitt *Datei-Downloads konfigurieren* folgende Optionen aus:

Option	Beschreibung
Deaktiviert	Verhindert das Herunterladen von Dell Aktualisierungspaketen. Dies beinhaltet die für die Installation der Aktualisierungen erforderlichen Installationsprogramme.
Alle Dateien	Auf Ihrer Appliance können Sie einen Vollcache abonnierter Pakete verwalten. Mit dieser Option werden alle Bereitstellungspakete heruntergeladen, ohne zu prüfen, ob diese für Ihre Umgebung erforderlich sind.
Als fehlend erkannte Dateien	Die Appliance kann ermitteln, welche Pakete basierend auf den Ergebnissen von Erkennungs-Jobs heruntergeladen werden sollen. Wenn eine Erkennungssignatur für Dell Aktualisierungen auf einem verwalteten Gerät als nicht installiert erkannt wird, wird das Paket heruntergeladen. Wenn kein verwaltetes Gerät als nicht installiert erkannt wird, werden für diese Aktualisierung keine Pakete heruntergeladen.
Nicht verwendete Dateien löschen nach __ Tagen	Nicht bereitgestellte Dell Aktualisierungspakete werden nach Ablauf der angegebenen Anzahl von Tagen gelöscht. Als *Inaktiv* oder *Deaktiviert* gekennzeichnete Dell Aktualisierungen werden während des Downloadvorgangs automatisch gelöscht.

Option	Beschreibung
Aktualisieren **Beschreibung** **Aktionen**	Für jeden Aktualisierungstyp (*Signatur*, *Dateien aktualisieren*) wird eine Beschreibung und der Zugriff auf die verfügbaren Aktionen bereitgestellt: • **Auf Update überprüfen**: Klicken Sie auf diese Option, um Signaturdateien für Dell Aktualisierungen herunterzuladen. • **Löschen**: Klicken Sie auf diese Option, um alle Dell Aktualisierungen umgehend von der Appliance zu entfernen. Das kann nützlich sein, wenn Sie keine Aktualisierungen mehr benötigen und den von den Aktualisierungen belegten Speicherplatz rasch freigeben möchten. • **Jetzt ausführen**: Klicken Sie auf diese Option, um die Dell Aktualisierungen, die Sie abonniert haben, unabhängig vom Abonnementplan sofort herunterzuladen.

4. Wählen Sie im Abschnitt *Planen* die Zeitplanoptionen für Dell Aktualisierungssignaturen aus. Dateisignaturen umfassen die Sicherheitsbulletins und andere Dateien, die über Quest heruntergeladene Dell Aktualisierungen definieren.

Option	Beschreibung
Signaturdownload	Durch Auswahl von **Keine** wird das Herunterladen von Dell Aktualisierungssignaturen verhindert.
Jeden Tag zum festgelegten Zeitpunkt	Wählen Sie **Tag** aus, um Dell Aktualisierungssignaturen jeden Tag herunterzuladen, oder wählen Sie einen Wochentag aus, um Signaturen einmal pro Woche herunterzuladen. Wählen Sie die Uhrzeit für den Beginn des Downloads aus. Die Uhrzeit wird im 24-Stunden-Format angezeigt, wobei 0 Uhr Mitternacht, 1:00 a.m. 01 Uhr nachts und 11:00 p.m. 23 Uhr entspricht. **HINWEIS:** Beim Einrichten von Dell Aktualisierungs-Downloads ist die Uhrzeit wichtig. Das Aktivitätsprotokoll der Appliance wird um 1:30 Uhr erstellt und Wartungsaufgaben werden zwischen 01:00 und 01:30 Uhr ausgeführt. Quest empfiehlt, Dell Aktualisierungs-Downloads nach Abschluss der Protokoll- und Wartungsaufgaben, also etwa um 3:00 Uhr zu planen.
Am n-ten jedes Monats oder eines bestimmten Monats um HH:MM	Wählen Sie den Tag des Monats aus, an dem Erkennungssignaturen für Dell Aktualisierungen monatlich heruntergeladen werden sollen.

5. Legen Sie die Zeitplanoptionen für Dell Aktualisierungen fest.

Option	Beschreibung
Nach Signaturdownload	Pakete werden nach dem Herunterladen der Signaturen heruntergeladen. Diese Option ist nicht verfügbar, wenn **Deaktiviert** im Bereich *Dateidownloads konfigurieren* deaktiviert wurde.
Alle __ Minuten	Legt die Häufigkeit fest, mit der Pakete heruntergeladen werden. Diese Option ist nur verfügbar, wenn die Option *Als fehlend erkannte Dateien* im Bereich *Dateidownloads konfigurieren* ausgewählt wurde.
Zeitfenster für Aussetzung von Download: Start __ Ende __	Legt einen Zeitraum fest, in dem keine Dateien heruntergeladen werden können. Beispielsweise könnten Sie eine Beendigungszeit am frühen Morgen verwenden, damit durch den Vorgang während der regulären Arbeitszeit nicht übermäßig viel Netzwerkbandbreite beansprucht wird. Wenn Sie diese Option auswählen, beendet die Appliance Dateidownloads zur angegebenen Zeit. Dateidownloads werden erst wieder zum nächsten angegebenen Zeitpunkt gestartet. Wenn der Download wieder aufgenommen wird, wird er an der Stelle fortgesetzt, an der er unterbrochen wurde. Nicht abgeschlossene Downloads werden auf der Seite *Dell Aktualisierungskatalog* möglicherweise nicht angezeigt.

6. Klicken Sie auf **Speichern**.

Dell Aktualisierungszeitpläne konfigurieren

Die Appliance kann die Firmware- und Treiberaktualisierungen für Ihre Dell Clients und Server gemäß dem von Ihnen eingerichteten Zeitplan automatisch identifizieren und installieren. Wenn die Organisationskomponente für Ihre Appliance aktiviert ist, erstellen Sie Dell Aktualisierungszeitpläne für jede Organisation separat.

Erstellen Sie gegebenenfalls Labels, um Dell Aktualisierungen und Geräte in Gruppen zusammenzufassen. Sie können diese Labels dann zum Erstellen von Dell Aktualisierungszeitplänen verwenden. Beispielsweise können Sie ein Label erstellen, um Aktualisierungen nach Anwendungsfamilien wie Treibern oder Firmware zu gruppieren. Sie können auch alle Dell Server, auf denen Microsoft Windows 7 ausgeführt wird, in einem Label erfassen und einen Dell Aktualisierungszeitplan ausführen, um diese zu aktualisieren. Weitere Informationen zur Erstellung von Labels für Aktualisierungen und Geräte finden Sie unter Smart Labels für Patches verwenden.

1. Rufen Sie die Seite *Dell Aktualisierungen* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Sicherheit** und anschließend auf **Dell Aktualisierungen**.
2. **Optional**: Überprüfen Sie die verfügbaren Aktualisierungen und deaktivieren Sie alle Aktualisierungen, die nicht installiert werden sollen.

   Aktualisierungen sind nur verfügbar, wenn die Appliance-Einstellungen so konfiguriert sind, dass Dell Katalogaktualisierungen heruntergeladen werden.

So prüfen und deaktivieren Sie Aktualisierungen

a. Klicken Sie im Fensterbereich *Dell Aktualisierungen* auf **Katalog**.
b. Aktivieren Sie das Kontrollkästchen neben einer Aktualisierung.
c. Wählen Sie **Aktion auswählen** > **Status ändern in** > **Inaktiv**.

3. Planen Sie Inventarisierungen und Aktualisierungen.

Das funktioniert ähnlich wie die Erstellung von Patch-Zeitplänen im Abschnitt *Patch-Verwaltung*. Sie können Inventarisierungen unabhängig oder im Rahmen eines Zeitplans für Inventarisierungen und Aktualisierungen durchführen, bei dem gleichzeitig auch die Aktualisierungen installiert werden. Normalerweise wird die Inventarisierung automatisch im Rahmen eines Aktualisierungszeitplans durchgeführt.

So planen Sie Inventarisierungen und Aktualisierungen

a. Klicken Sie in der linken Navigationsleiste auf **Sicherheit** und anschließend auf **Dell Aktualisierungen**.
b. Klicken Sie im Fensterbereich *Dell Aktualisierungen* auf **Zeitpläne**.
c. Wählen Sie **Aktion auswählen** > **Neu**.
d. Führen Sie auf der Listenseite *Dell Aktualisierungszeitplan* einen der folgenden Schritte aus:

- Klicken Sie zum Erstellen eines neuen Dell Aktualisierungszeitplans mithilfe des Assistenten für *Schedule Detail (Details zum Zeitplan)* auf **Aktion wählen** > **Neu (Assistent)**.
- Klicken Sie zum Erstellen eines neuen Dell Aktualisierungszeitplans auf der Seite *Schedule Detail (Details zum Zeitplan)* auf **Aktion wählen** > **New (Classic) (Neu (Klassisch))**.
- Zum Bearbeiten eines vorhandenen Zeitplans klicken Sie in der Liste auf den Namen des Zeitplans, und dann auf der Seite *Dell Update Schedule Summary (Dell Aktualisierungszeitplan - Übersicht)* auf **Bearbeiten**.

  Die Seite *Schedule Detail (Details zum Zeitplan)* oder der Assistent wird wie ausgewählt angezeigt. Für jede Auswahloption sind die gleichen Einstellungen verfügbar: Sie können zwischen der Seite und dem Assistenten wechseln, indem Sie in der rechten oberen Ecke auf **Klassische Ansicht** oder **Wizard View (Assistentenansicht)** klicken.

e. Konfigurieren Sie allgemeine Informationen zum Zeitplan:

Option	Beschreibung
Name	Ein Name, der den Zeitplan genau bezeichnet. Dieser Name wird auf der Listenseite *Dell Aktualisierungszeitpläne* angezeigt.
Beschreibung	Eine kurze Beschreibung des Dell Aktualisierungszeitplans.

f. Wählen Sie eine der folgenden Aktionen aus.

Diese Aktionen sind identisch mit den Aktionen für die Patch-Zeitpläne. Siehe Konfigurieren von Patch-Zeitplänen.

Aktion	Beschreibung
Erkennen	Sucht nach kompatiblen Dell Aktualisierungen.
Erkennen und bereitstellen	Sucht nach kompatiblen Dell Aktualisierungen, lädt die entsprechenden Dateien auf das Agentengerät herunter und stellt das Update auf den ausgewählten Geräten bereit.

Aktion	Beschreibung
Bereitstellung	Stellt die Aktualisierung auf den ausgewählten Geräten bereit.

> **HINWEIS:** Die Bereitstellungsaktionen für Dell Aktualisierungen erfordern einen Neustart der entsprechenden verwalteten Geräte.

g. Wählen Sie die Zielgeräte mithilfe der folgenden Optionen aus.

Diese Optionen sind identisch mit denen, die in den Aktionen für Patch-Zeitpläne angezeigt werden. Siehe Konfigurieren von Patch-Zeitplänen.

In der Regel werden für Laptops, Workstations und Server unterschiedliche Zeitpläne erstellt, da diese drei Arten von Geräten sehr unterschiedliche Nutzungscharakteristiken aufweisen.

Aktion	Beschreibung
Alle Geräte	Wählen Sie diese Optionen aus, um diesen Zeitplan auf alle verwalteten Geräte anzuwenden. Deaktivieren Sie das Kontrollkästchen, um die Aktualisierungsaktion auf bestimmte Labels oder Geräte zu beschränken.
Gerätelabels	Die Aktion wird auf die Dell Aktualisierungen beschränkt, die das von Ihnen ausgewählte Label aufweisen. Diese Option wird am häufigsten verwendet. a. Klicken Sie auf **Verknüpfte Labels verwalten**. b. Ziehen Sie im daraufhin angezeigten Dialogfeld *Labels auswählen* (falls zutreffend) mindestens ein Label in den Bereich *Ausführung begrenzen auf*, und klicken Sie dann auf **OK**. Um diese Option verwenden zu können, müssen Smart Labels für die Funktionsaktualisierungen vorhanden sein. Siehe Smart Labels für Patches verwenden.
Geräte	Führen Sie Dell Aktualisierungen auf den ausgewählten Geräten aus. In der Liste werden nur kompatible Dell Geräte angezeigt. • Um nach Geräten zu suchen, beginnen Sie mit einer entsprechenden Eingabe in das Feld. • Um alle angegebenen Geräte zu entfernen und erneut zu starten, klicken Sie auf **Alle entfernen**. • Benutzer mit eingeschränkten Zugriffsrechten sehen nur die Geräte, die mit ihrer Rolle verknüpft sind, wenn der Rolle ein Label zugewiesen ist. Weitere Informationen zu Benutzerrollen finden Sie unter Benutzerrollen hinzufügen oder bearbeiten.

Aktion	Beschreibung
Betriebssysteme	Wählen Sie die Betriebssysteme der Geräte aus, die aktualisiert werden sollen. Die Standardeinstellung für diese Option sind alle Betriebssysteme. Wenn diese Option konfiguriert ist, gilt der Zeitplan nur für Geräte mit den ausgewählten Betriebssystemen. a. Klicken Sie auf **Betriebssysteme verwalten**. b. Wählen Sie im daraufhin angezeigten Dialogfeld **Betriebssysteme** die Betriebssystemversionen in der Navigationsstruktur aus. Sie haben die Möglichkeit, Betriebssystemversionen nach Familie, Produkt, Architektur, Versions-ID oder Build-Version auszuwählen. Je nach Bedarf können Sie eine bestimmte Build-Version oder einen übergeordneten Knoten auswählen. Wenn Sie einen übergeordneten Knoten im Baum auswählen, werden die zugehörigen untergeordneten Knoten automatisch mit ausgewählt. Aufgrund dieses Verhaltens können Sie beliebige zukünftige Betriebssystemversionen auswählen, da Geräte in Ihrer verwalteten Umgebung hinzugefügt oder aktualisiert werden. Wenn Sie beispielsweise alle aktuellen und zukünftigen Versionen auswählen möchten, die mit der Windows 10 x64-Architektur verbunden sind, wählen Sie unter Windows > **Windows 10** die Option **x64** aus.

h. Geben Sie im Abschnitt *Zeitplan* die entsprechenden Optionen für den Zeitplan an.

Diese Optionen sind identisch mit denen, die in den Aktionen für Patch-Zeitpläne angezeigt werden. Siehe Konfigurieren von Patch-Zeitplänen.

Option	Beschreibung
Kein(e)	Die Ausführung erfolgt im Zusammenhang mit einem Ereignis anstatt zu einem bestimmten Datum oder zu einem bestimmten Zeitpunkt. Diese Option ist nützlich, wenn Sie Patches manuell auf Server anwenden oder Patch-Aktionen ausführen möchten, die nicht nach einem Zeitplan ausgeführt werden sollen.
Alle _ Stunden	Der Vorgang wird im angegebenen Intervall durchgeführt.
Täglich/an einem bestimmten Tag um HH:MM	Die Erfassung wird täglich zu einem bestimmten Zeitpunkt oder an einem bestimmten Wochentag um eine bestimmte Uhrzeit ausgeführt.
Ausführen am n-ten jedes Monats/eines bestimmten Monats um HH:MM	Am **n**. Tag jedes Monats ausführen (beispielsweise am ersten oder zweiten) Tag des Monats oder in einem bestimmten Monat zu einer bestimmten Zeit.

Option	Beschreibung
Ausführen am n-ten Wochentag **jedes Monats/ eines bestimmten Monats um HH:MM**	Die Erfassung wird jeden Monat oder in einem bestimmten Monat an einem festgelegten Wochentag zu einer festgelegten Uhrzeit ausgeführt.

Benutzerdefiniert	Ausführung nach einem benutzerdefinierten Zeitplan.
	Verwenden Sie das Standard-5-Feld-Cron-Format (das erweiterte Cron-Format wird nicht unterstützt):
	`* * * * *`
	`| | | | +————Wochentag (0-6) (Sonntag=0)`
	`| | | +————Monat (1-12)`
	`| | +————Monatstag (1-31)`
	`| +————Stunde (0-23)`
	`+————Minute (0-59)`
	Verwenden Sie bei der Angabe von Werten die folgenden Zeichen:
	• **Leerzeichen( )**: Die einzelnen Felder mit einem Leerzeichen trennen.
	• **Sternchen (*)**: Ein Sternchen repräsentiert den gesamten Wertebereich in einem Feld. Zum Beispiel repräsentiert ein Sternchen im Stundenfeld eine beliebige Stunde.
	• **Kommas (,)**: Mehrere Werte in einem Feld werden mit einem Komma getrennt. Zum Beispiel werden mit `0,6` im Feld „Wochentag“ Sonntag und Samstag angegeben.
	• **Bindestriche (-)**: Mit einem Bindestrich wird ein Wertebereich in einem Feld angegeben. Zum Beispiel entspricht `1-5` im Feld „Wochentag“ `1,2,3,4,5`, d. h. Montag bis Freitag.
	• **Schrägstriche (/)**: Die Angabe der Zeitabstände, mit denen eine Aktion wiederholt werden soll, erfolgt mit einem Schrägstrich. Zum Beispiel entspricht `*/3` im Feld Stunde `0,3,6,9,12,15,18,21`. Das Sternchen (`*`) gibt jede Stunde an, mit `/3` erfolgt aber eine Einschränkung auf durch drei teilbare Stunden.

Option	Beschreibung
	Beispiele: • `15 * * * * Jeden Tag 15 Minuten nach jeder vollen Stunde ausführen` • `0 22 * * * Jeden Tag um 22:00 Uhr ausführen` • `0 0 1 1,6 * Am 1. Januar und 1. Juni um 00:00 Uhr ausführen` • `30 8,12 * * 1-5 An Wochentagen um 08:30 Uhr und 12:30 Uhr ausführen` • `0 2 */2 * * Jeden zweiten Tag um 02:00 Uhr ausführen`
Aufgabenplan anzeigen	Klicken Sie, um den Aufgabenplan anzuzeigen. Im Dialogfeld *Taskplan* wird eine Liste der geplanten Ziele angezeigt. Klicken Sie auf eine Aufgabe, um die Aufgabendetails anzuzeigen. Weitere Informationen hierzu finden Sie unter Aufgabenpläne anzeigen.
Zeitzone	Die Zeitzone, die beim Planen der Aktion verwendet werden soll. Wählen Sie **Server** aus, um die Zeitzone der Appliance zu verwenden. Wählen Sie **Agent** aus, um die Zeitzone des verwalteten Geräts zu verwenden.
Wenn offline, bei nächster Verbindung ausführen	Wenn das Gerät derzeit offline ist, wird die Aktion ausgeführt, sobald das verwaltete Gerät das nächste Mal eine Verbindung mit der Appliance herstellt. Diese Option eignet sich für Notebooks und andere Geräte, die regelmäßig offline sind. Wenn diese Option nicht ausgewählt wird und das Gerät offline ist, wird die Aktion erst zum nächsten geplanten Zeitpunkt ausgeführt.
Ausführung nach Wiederverbinden verzögern	Der Zeitplan wird um eine angegebene Zeitspanne verzögert. Die Zeitspanne der Verzögerung beginnt zu dem Zeitpunkt, für den die Ausführung der Patch-Aktion geplant wurde.
Beenden nach	Das Zeitlimit für Patch-Aktionen. Wenn Sie beispielsweise festlegen, dass Patches um 4.00 Uhr ausgeführt werden sollen, sollten Sie möglicherweise auch festlegen, dass alle Patch-Aktionen um 7.00 Uhr beendet werden, um Probleme hinsichtlich der Bandbreite zu vermeiden, wenn Benutzer mit der Arbeit beginnen. Hierzu können Sie im Minutenfeld den Wert **180** angeben. Wenn dieses Zeitlimit erreicht wird, werden alle Patch-Aufgaben, die derzeit ausgeführt werden, angehalten und der zugehörige Status im Sicherheitsprotokoll wird mit *Angehalten* angegeben.

Option	Beschreibung
	Diese Patch-Aufgaben werden bei der nächsten Ausführung nicht fortgesetzt, sondern beginnen vielmehr bei jeder geplanten Patch-Aktion wieder von vorn.

HINWEIS: Die Zeitzone des Agenten ist nur verfügbar, wenn das Inventar ein Dell Gerät enthält, von dem die Zeitzoneninformationen abgerufen werden können.

i. Klicken Sie auf **Speichern**.

Der Zeitplan wird auf der Seite *Dell Aktualisierungszeitpläne* angezeigt. Der Zeitplan ist standardmäßig deaktiviert.

TIPP: Bevor Sie einen Zeitplan aktivieren, sollten Sie ihn auf einem kleinen Teil Ihrer Geräte testen, um sicherzustellen, dass alles wie erwartet funktioniert.

j. Aktivieren Sie das Kontrollkästchen neben dem Namen des Zeitplans und wählen Sie anschließend **Aktion auswählen** > **Aktivieren**, um den Zeitplan zu aktivieren.

Die Inventarisierung und Aktualisierung wird gemäß dem angegebenen Zeitplan ausgeführt.

Dell Aktualisierungszeitpläne anzeigen

Sie können zusammenfassende Informationen für die Dell Aktualisierungszeitpläne anzeigen, die auf der Appliance vorhanden sind. Wenn die Organisationskomponente für Ihre Appliance aktiviert ist, können Sie Dell Aktualisierungszeitpläne für jede Organisation separat anzeigen.

1. Rufen Sie die Seite *Dell Aktualisierungszeitpläne* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Sicherheit** und anschließend auf **Dell Aktualisierungen**.
2. Klicken Sie im Fensterbereich *Dell Aktualisierungen* auf **Zeitpläne**.

   Die auf der Seite *Dell Update Update Schedules (Aktualisierungszeitpläne für Dell Aktualisierungen)* verfügbaren Spalten sind identisch mit denen auf der Seite *Patch-Zeitpläne*. Weitere Informationen zu den Feldern auf der Seite *Patch-Zeitpläne* finden Sie unter Liste der Patch-Zeitpläne anzeigen.
3. (Optional) Um die angezeigten Spalten zu ändern, wählen Sie aus der Dropdown-Liste *Tabellenoptionen* rechts über der Tabelle **Spaltenanzeige** aus.

Details zum Dell Aktualisierungszeitplan prüfen

Wenn Sie einen Dell Aktualisierungszeitplan konfigurieren, werden auf dieser Seite Details zur Konfiguration des Zeitplans und dessen Status angezeigt.

1. Rufen Sie die Seite *Update Schedule Summary (Aktualisierungszeitplan - Übersicht)* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Sicherheit** und anschließend auf **Dell Aktualisierungen**.

c. Klicken Sie im Fensterbereich *Dell Aktualisierungen* auf **Zeitpläne**.
d. Klicken Sie auf den Namen eines Zeitplans.

2. Überprüfen Sie den Inhalt des Abschnitts *Konfiguration*.

Option	Beschreibung
Erstellt	Das Datum und die Uhrzeit der Erstellung des Zeitplans.
Geändert	Das Datum und die Uhrzeit der letzten Änderung des Zeitplans.
Letzte Ausführung	Das Datum und die Uhrzeit der letzten Ausführung des Zeitplans.
Name	Ein Name, der den Zeitplan genau bezeichnet. Dieser Name wird auf der Listenseite *Dell Aktualisierungszeitpläne* angezeigt.
Aktion	Die mit dem Zeitplan verbundene Aktion: • **Erkennen**: Sucht nach kompatiblen Dell Aktualisierungen. • **Erkennen und bereitstellen**: Sucht nach kompatiblen Dell Aktualisierungen und lädt die entsprechenden Dateien zur späteren Bereitstellung auf das Agentengerät herunter. • **Bereitstellen**: Stellt die Aktualisierung auf den ausgewählten Geräten bereit.
Beschreibung	Eine kurze Beschreibung des Dell Aktualisierungszeitplans.
Geräte	Dieses Feld wird nur angezeigt, wenn der Zeitplan so konfiguriert ist, dass er auf alle Geräte angewendet wird.
Label des Geräts	Mindestens ein Smart Label, das mit den Geräten verknüpft ist, für die der Zeitplan ausgeführt wird. Weitere Informationen hierzu finden Sie unter Smart Labels für Patches verwenden. Dieses Feld wird nur angezeigt, wenn der Zeitplan so konfiguriert ist, dass er auf ausgewählte Geräte angewendet wird.
Gerätename	Mindestens ein ausgewähltes Geräte, für das der Zeitplan ausgeführt wird. Dieses Feld wird nur angezeigt, wenn der Zeitplan so konfiguriert ist, dass er auf ausgewählte Geräte angewendet wird.
Label finden	Mindestens ein Smart Label, das mit den geplanten Aktualisierungen verknüpft ist. Weitere Informationen hierzu finden Sie unter Smart Labels für Patches verwenden. Dieses Feld wird nur angezeigt, wenn der Zeitplan so konfiguriert ist, dass ausgewählte Aktualisierungen erkannt werden.

Option	Beschreibung
Warnungen	**Detect and Deploy schedules only (Nur Zeitpläne für Erkennen und Bereitstellen)**. Die Warnungen, die Benutzern bei der Ausführung von Aktualisierungsaktionen angezeigt werden. • **OK**: Sofort ausführen. • **Abbrechen**: Abbrechen bis zur nächsten geplanten Ausführung. • **Snooze**: Der Benutzer erhält nach Ablauf der *Snooze-Dauer* erneut eine Eingabeaufforderung.
Neustart	**Detect and Deploy schedules only (Nur Zeitpläne für Erkennen und Bereitstellen)**. Die Optionen für den Neustart des verwalteten Geräts. • **Kein Neustart**: Das Gerät wird nicht neu gestartet, obwohl möglicherweise ein Neustart erforderlich ist, damit die Aktualisierung wirksam wird. Es wird davon abgeraten, diese Option zu verwenden, da die Bereitstellung von Aktualisierungen ohne einen erforderlichen Neustart die Stabilität der Systeme beeinträchtigen kann. Zudem werden Aktualisierungen, die einen Neustart erfordern, erst nach dem Neustart als bereitgestellt angezeigt. • **Eingabeaufforderung für Benutzer**: Vor dem Geräteneustart wird gewartet, bis der Benutzer den Neustart akzeptiert hat. Wenn der Benutzer den Neustart per Snooze verschiebt oder abbricht, wird der Aktualisierungsvorgang angehalten, bis ein Neustart durchgeführt wird. Wenn Sie im Dialogfeld "Agent", das auf dem Zielgerät angezeigt wird, eine Snooze-Dauer auswählen, wird die Neustartaufforderung für das angegebene Snooze-Intervall angehalten. • **Neustart erzwingen**: Ein Neustart wird durchgeführt, sobald eine Aktualisierung bereitgestellt wurde, die einen Neustart erfordert. Erzwungene Neustarts können nicht abgebrochen werden. Neustart erzwingen eignet sich gut für Desktops und Server. Unter Umständen ist es nicht sinnvoll, auf Notebooks einen Neustart zu erzwingen. "Neustart erzwingen" eignet sich für Server, da diese in der Regel keine speziell zugewiesenen Benutzer besitzen. Es ist jedoch wichtig, Benutzer darauf hinzuweisen, dass Dienste nicht verfügbar sind, wenn Server aktualisiert und neu gestartet werden. Siehe Best Practices für den Patch-Vorgang.

Option	Beschreibung
Planen	Der ausgewählte Aktualisierungszeitplan. Klicken Sie auf **Aufgabenplan anzeigen**, um eine detaillierte Aufgabenplanung anzuzeigen. Klicken Sie im daraufhin angezeigten Dialogfeld auf eine Aufgabe, um die Aufgabendetails zu überprüfen. Weitere Informationen hierzu finden Sie unter Aufgabenpläne anzeigen.
Wenn offline, bei nächster Verbindung ausführen	Wenn das Gerät derzeit offline ist, wird die Aktion ausgeführt, sobald das verwaltete Gerät das nächste Mal eine Verbindung mit der Appliance herstellt.
Zeitzone	Diese Option gibt die Zeitzone an, die bei der Planung der entsprechenden Aktion verwendet werden soll. Bei der Einstellung "Server" wird die Zeitzone der Appliance für den Zeitplan verwendet. Bei der Einstellung "Agent" wird die Zeitzone des verwalteten Geräts verwendet.
Ausführung nach Wiederverbinden verzögern	Diese Option gibt an, wie lange sich der Zeitplan verzögert. Die Zeitspanne der Verzögerung beginnt zu dem Zeitpunkt, für den die Ausführung der Aktualisierungsaktion geplant wurde.
Beenden nach	Diese Option gibt die maximale Zeitspanne für die Ausführung des Zeitplans an. Wenn dieses Zeitlimit erreicht ist, werden alle laufenden Aktualisierungsaufgaben angehalten.

3. Überprüfen Sie im Abschnitt *Zeitplanstatus* den Gesamtstatus des Zeitplans auf einer der folgenden Registerkarten:

Registerkarte	Inhalt
Nach Computer	Geräte, die für die Aktualisierung ausgewählt wurden. Jeder Eintrag zeigt den Namen und die IP-Adresse des Geräts, den Aktualisierungsstatus (siehe Felder auf den Detailseiten des Patch-Zeitplans), die Aktualisierungsergebnisse und das Datum an, an dem die Aktualisierung abgeschlossen ist. Sie können Geräteknoten erweitern, um die entsprechenden Aktualisierungen anzuzeigen. Jeder Eintrag enthält die Aktualisierungs-ID, die zugehörige Knowledge Base-Artikelnummer, den Namen der Aktualisierung, den aktuellen Status (installiert, nicht installiert oder Bereitstellungsfehler) und das Datum, an dem die Aktualisierung erkannt wurde.
By Update (Nach Aktualisierung)	Aktualisierungen, die für die Erkennung und Bereitstellung ausgewählt wurden. Jeder Eintrag zeigt die Aktualisierungs-ID, die zugehörige Knowledge Base-Artikelnummer, den Aktualisierungsnamen und die Anzahl der aktualisierten und nicht aktualisierten Geräte

Registerkarte	Inhalt
	an, sowie die Geräte, bei denen Fehler bei der Erkennung oder Bereitstellung aufgetreten sind.
Installiert	Updates wurden erfolgreich auf Geräten installiert. Jeder Eintrag zeigt die Aktualisierungs-ID, die zugehörige Knowledge Base-Artikelnummer und den Namen der Aktualisierung an. Sie können einen Aktualisierungsknoten erweitern, um die Geräte anzuzeigen, auf denen die Aktualisierung installiert ist.
Nicht installiert	Aktualisierungen, die nicht auf Geräten installiert wurden. Jeder Eintrag zeigt die Aktualisierungs-ID, die zugehörige Knowledge Base-Artikelnummer und den Namen der Aktualisierung an. Sie können einen Aktualisierungsknoten erweitern, um die Geräte anzuzeigen, auf denen die Aktualisierung installiert werden soll.
Fehler bei der Erkennung	Unvollständige Aktualisierungen, die zu einem Erkennungsfehler geführt haben. Jeder Eintrag zeigt die Aktualisierungs-ID, die zugehörige Knowledge Base, den Aktualisierungsnamen und den zugehörigen Fehlercode an (siehe Fehlercodes aufgrund von Patching und Skripterstellung). Sie können Aktualisierungsknoten erweitern, um die Geräte anzuzeigen, auf denen der Fehler aufgetreten ist.
Fehler bei der Bereitstellung	Unvollständige Aktualisierungen, die zu einem Bereitstellungsfehler geführt haben. Jeder Eintrag zeigt die Aktualisierungs-ID, die zugehörige Knowledge Base, den Aktualisierungsnamen und den zugehörigen Fehlercode an (siehe Fehlercodes aufgrund von Patching und Skripterstellung). Sie können Aktualisierungsknoten erweitern, um die Geräte anzuzeigen, auf denen der Fehler aufgetreten ist.

4. **Optional**. Nach Überprüfung der Zeitplandetails können Sie eine der folgenden Aktionen durchführen:
   - Klicken Sie zum Bearbeiten des Aktualisierungszeitplans auf **Bearbeiten**. Weitere Informationen hierzu finden Sie unter Zeitpläne für Windows-Funktionsaktualisierungen konfigurieren.
   - Klicken Sie zum Ausführen des Aktualisierungszeitplans auf **Jetzt ausführen**.
   - Um eine Kopie des Aktualisierungszeitplans zu erstellen, klicken Sie auf **Duplizieren**.
   - Um den Aktualisierungszeitplan zu löschen, klicken Sie auf **Löschen**.

Anzeigen verfügbarer Dell Aktualisierungen

Sie können die Liste der Dell Aktualisierungen im Dell Aktualisierungskatalog überprüfen.

Sie müssen die Download-Einstellungen für Dell Aktualisierungen auswählen, um zugehörige Aktualisierungen anzuzeigen. Siehe Download-Einstellungen für Dell Aktualisierung auswählen. Wenn alle Signaturdateien

für Dell Aktualisierungen heruntergeladen wurden, listet der Dell Aktualisierungskatalog die entsprechenden Aktualisierungen auf.

HINWEIS: Die Spalte *Schweregrad* auf dieser Seite verwendet die Microsoft-Sicherheitsstandards, die nicht mit den Dell Schweregraden übereinstimmen:

Angezeigte Schweregrade	Entsprechender Dell Schweregrad
Angemessen	Optional
Wichtig	Empfohlen
Kritisch	Dringend

1. Rufen Sie die Seite *Dell Aktualisierungskatalog* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Sicherheit** und anschließend auf **Dell Aktualisierungen**.
   c. Klicken Sie im Fensterbereich *Dell Aktualisierungen* auf **Katalog**.
2. Suchen Sie nach Dell Aktualisierungen.
   a. Geben Sie die Suchkriterien in das Suchfeld ein.

   Beispiel: `2021`.

   b. Drücken Sie die **Eingabetaste**.

   Die Listenseite wird aktualisiert und zeigt nur die Dell Aktualisierungen mit Version 2021 an.

Anzeigen des Dell Aktualisierungsstatus

Die Details zur Dell Aktualisierung umfassen Informationen zum Anbieter und Bereitstellungsstatus.

1. Rufen Sie die Seite *Dell Aktualisierungskatalog* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Sicherheit** und anschließend auf **Dell Aktualisierungen**.
   c. Klicken Sie im Fensterbereich *Dell Aktualisierungen* auf **Katalog**.
   d. Klicken Sie auf den Namen einer Dell Aktualisierung.

   Die Seite *Dell Update Detail (Details zur Dell Aktualisierung)* wird mit vollständigen Informationen zur ausgewählten Aktualisierung angezeigt.

Verwalten von Linux-Paket-Upgrades

Die Linux-Paket-Upgrades verbessern die Gesamtleistung Ihrer verwalteten Linux-Geräte und schützen sie vor potenziellen Schwachstellen.

Mit der Appliance können Sie den Prozess der Installation und Verwaltung von Linux-Paket-Upgrades automatisieren. Dabei wird davon ausgegangen, dass einzelne Linux-Paket-Repositorys vorhanden sind, und Ihre verwalteten Linux-Geräte auf das entsprechende Repository verweisen.

Außerdem erkennt die Appliance nur die Pakete, die Sicherheitsupdates enthalten, die in jedem Linux-Repository als solche identifiziert werden. Die Appliance versucht nicht, alle Pakete zu erkennen oder zu aktualisieren oder das gesamte Betriebssystem der verwalteten Geräte auf die neueste Version zu aktualisieren.

HINWEIS: Linux Raspbian unterscheidet nicht zwischen regelmäßigen und Sicherheitsaktualisierungen. Wenn Pakete für verwaltete Raspbian-Geräte erkannt und aktualisiert werden, werden alle aktualisierten Pakete auf diesen Geräten installiert.

HINWEIS: Der Begriff *Aktualisierung* in der KACE Systems Management Appliance geht von folgendem aus: Wenn neue Versionen der Pakete in den Repositorys der Distribution verfügbar sind, verwendet die Appliance die Standardsystembefehle, um sicherzustellen, dass das System die aktuelle Version installiert. Dies bedeutet keineswegs, dass der Begriff *Update* (oder *Upgrade*) in den zugrunde liegenden Systembefehlen genau so verwendet wird.

Zeitpläne für Linux-Paket-Upgrades anzeigen

Sie können zusammenfassende Informationen für die Zeitpläne der Linux-Paket-Upgrades anzeigen, die auf der Appliance vorhanden sind. Wenn auf der Appliance die Organisationskomponente aktiviert wurde, können Sie diese Zeitpläne für jede Organisation einzeln anzeigen.

1. Rufen Sie die Seite *Zeitpläne für Windows-Funktionsaktualisierung* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Sicherheit** und anschließend auf **Linux Package Upgrades (Linux-Paket-Upgrades)**.
2. Klicken Sie im Fensterbereich *Linux Package Upgrades (Linux-Paket-Upgrades)* auf **Zeitpläne**.

   Die auf der Seite *Linux Package Upgrade Schedules (Zeitpläne für Linux-Paket-Upgrades)* verfügbaren Spalten sind identisch mit denen auf der Seite *Patch-Zeitpläne*. Weitere Informationen zu den Feldern auf der Seite *Patch-Zeitpläne* finden Sie unter Liste der Patch-Zeitpläne anzeigen.
3. (Optional) Um die angezeigten Spalten zu ändern, wählen Sie aus der Dropdown-Liste *Tabellenoptionen* rechts über der Tabelle **Spaltenanzeige** aus.

Konfigurieren der Upgrade-Zeitpläne für Linux-Pakete

Sie können Zeitpläne für Upgrades von Linux-Paketen erstellen und konfigurieren sowie einen Zeitpunkt für ihre Ausführung festlegen.

1. Starten Sie den Assistenten für das Upgrade von Linux-Paketen:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Sicherheit** und anschließend auf **Linux Package Upgrades (Linux-Paket-Upgrades)**.

c. Klicken Sie im Fensterbereich *Linux Package Upgrades Management (Verwaltung von Linux-Paket-Upgrades)* auf **Zeitpläne**.

d. Führen Sie auf der Seite *Linux Package Upgrade Schedules (Zeitpläne für Linux-Paket-Upgrades)* eine der folgenden Aktionen aus:

- Um einen neuen Zeitplan für das Linux-Paket-Upgrade zu erstellen, klicken Sie auf **Aktion auswählen > Neu (Assistent)**.
- Zum Bearbeiten eines vorhandenen Zeitplans klicken Sie in der Liste auf den Namen des Zeitplans und dann auf der Seite *Linux Package Upgrade Summary (Linux-Paket-Upgrade - Übersicht)* auf **Bearbeiten**.

Der Assistent *Schedule Detail (Details zum Zeitplan)* wird angezeigt.

2. Konfigurieren Sie im Assistenten *Schedule Detail (Details zum Zeitplan)* auf der Seite *Allgemeine Informationen* allgemeine Informationen zum Zeitplan:

Option	Beschreibung
Name	Ein Name, der den Zeitplan genau bezeichnet. Dieser Name wird auf der Listenseite *Linux Package Upgrade Schedules (Zeitpläne für Linux-Paket-Upgrades)* angezeigt.
Beschreibung	Eine kurze Beschreibung des Upgrade-Zeitplans für das Linux-Paket.

3. Führen Sie auf der Seite *Aktion* die folgenden Schritte aus:

a. Wählen Sie unter *Aktion* eine der folgenden Optionen aus:

Die Ergebnisse der ausgewählten Aktion hängen davon ab, ob Ihre verwalteten Linux-Geräte mit dem entsprechenden Paket-Repository verknüpft sind. Um alle zutreffenden Geräte auszuwählen, stellen Sie sicher, dass jedes Ihrer verwalteten Geräte das entsprechende Paket-Repository verwendet.

HINWEIS: Die Appliance sucht nur nach Paketen, die Sicherheitsupdates enthalten und in jedem Linux-Repository, mit Ausnahme von Linux Raspbian, als solche identifiziert werden. Die Appliance versucht nicht, alle Pakete zu erkennen oder zu aktualisieren oder das gesamte Betriebssystem der verwalteten Geräte auf die neueste Version zu aktualisieren. Das Linux Raspbian-Repository unterscheidet nicht zwischen regelmäßigen und Sicherheitsaktualisierungen. Wenn Pakete für verwaltete Raspbian-Geräte erkannt und aktualisiert werden, werden alle aktualisierten Pakete auf diesen Geräten installiert.

Aktion	Beschreibung
Detect All (Alle Erkennen)	Sucht nach allen Linux-Paket-Upgrades, die Sicherheitsupdates enthalten.
Detect and Upgrade All (Alle erkennen und aktualisieren)	Sucht nach allen Linux-Paket-Upgrades, die Sicherheitsupdates enthalten, lädt die entsprechenden Dateien herunter und stellt das Upgrade auf den ausgewählten Geräten bereit.

b. Wählen Sie unter *Detect All (Alle erkennen)* den Zeitraum aus, für den die Erkennungsaktion ausgeführt werden soll.

c. **Nur Aktionen "Detect and Upgrade All" (Alle erkennen und aktualisieren).** Wählen Sie unter *Upgrade All (Alle aktualisieren)* den Zeitraum aus, für den die Aktualisierungsaktion ausgeführt werden soll.

4. Klicken Sie auf **Weiter**.
5. Geben Sie auf der Seite *Geräte* die Geräte an, die Sie diesem Zeitplan zuordnen möchten.

Diese Optionen sind identisch mit denen, die in den Aktionen für Patch-Zeitpläne angezeigt werden. Anleitungen dazu finden Sie unter Konfigurieren von Patch-Zeitplänen.

Aktion	Beschreibung
Alle Geräte	Wählen Sie diese Option aus, um diesen Zeitplan auf alle verwalteten Geräte anzuwenden. Deaktivieren Sie das Kontrollkästchen, um die Patch-Aktion auf bestimmte Labels oder Geräte zu beschränken.
Gerätelabels	Die Aktion wird auf die Funktionsaktualisierungen beschränkt, die das von Ihnen ausgewählte Label aufweisen. Diese Option wird am häufigsten verwendet. a. Klicken Sie auf **Verknüpfte Labels verwalten**. b. Ziehen Sie im daraufhin angezeigten Dialogfeld *Labels auswählen* (falls zutreffend) mindestens ein Label in den Bereich *Ausführung begrenzen auf*, und klicken Sie dann auf **OK**. Um diese Option verwenden zu können, müssen Smart Labels für die Funktionsaktualisierungen vorhanden sein. Siehe Smart Labels für Patches verwenden.
Geräte	Führt auf den von Ihnen ausgewählten Geräten Patch-Aktionen aus. In der eingeblendeten Liste werden nur zutreffende Linux-Geräte angezeigt. • Um nach Geräten zu suchen, beginnen Sie mit einer entsprechenden Eingabe in das Feld. • Um alle angegebenen Geräte zu entfernen und erneut zu starten, klicken Sie auf **Alle entfernen**. • Benutzer mit eingeschränkten Zugriffsrechten sehen nur die Geräte, die mit ihrer Rolle verknüpft sind, wenn der Rolle ein Label zugewiesen ist. Weitere Informationen zu Benutzerrollen finden Sie unter Benutzerrollen hinzufügen oder bearbeiten.
Betriebssysteme	Wählen Sie die Betriebssysteme der Geräte aus, für die das Upgrade durchgeführt werden soll. Im Dialogfeld werden nur zutreffende Linux-Betriebssysteme angezeigt. Die Standardeinstellung für diese Option sind alle Betriebssysteme. Wenn diese Option konfiguriert ist, gilt der Zeitplan nur für Geräte mit den ausgewählten Betriebssystemen. a. Klicken Sie auf **Betriebssysteme verwalten**. b. Wählen Sie im daraufhin angezeigten Dialogfeld **Betriebssysteme** die Betriebssystemversionen in der Navigationsstruktur aus.

Aktion	Beschreibung
	Sie haben die Möglichkeit, Betriebssystemversionen nach Familie, Produkt, Architektur, Versions-ID oder Build-Version auszuwählen. Je nach Bedarf können Sie eine bestimmte Build-Version oder einen übergeordneten Knoten auswählen. Wenn Sie einen übergeordneten Knoten im Baum auswählen, werden die zugehörigen untergeordneten Knoten automatisch mit ausgewählt. Aufgrund dieses Verhaltens können Sie beliebige zukünftige Betriebssystemversionen auswählen, da Geräte in Ihrer verwalteten Umgebung hinzugefügt oder aktualisiert werden. Wenn Sie beispielsweise alle aktuellen und zukünftigen Versionen auswählen möchten, die mit der Linux Ubuntu x86_64-Architektur verbunden sind, wählen Sie unter **Linux > Ubuntu** die Option **x64** aus.

6. Klicken Sie auf **Weiter**.
7. Geben Sie im Abschnitt *Zeitplan* die entsprechenden Optionen für den Zeitplan an.

   Diese Optionen sind identisch mit denen, die in den Aktionen für Patch-Zeitpläne angezeigt werden. Anleitungen dazu finden Sie unter Konfigurieren von Patch-Zeitplänen.

Aktion	Beschreibung
Kein(e)	Die Ausführung erfolgt im Zusammenhang mit einem Ereignis anstatt zu einem bestimmten Datum oder zu einem bestimmten Zeitpunkt. Diese Option ist nützlich, wenn Sie Patches manuell auf Server anwenden oder Patch-Aktionen ausführen möchten, die nicht nach einem Zeitplan ausgeführt werden sollen.
Alle _ Stunden	Der Vorgang wird im angegebenen Intervall durchgeführt.
Täglich/an einem bestimmten Tag um HH:MM	Die Erfassung wird täglich zu einem bestimmten Zeitpunkt oder an einem bestimmten Wochentag um eine bestimmte Uhrzeit ausgeführt.
Ausführen am n-ten jedes Monats/eines bestimmten Monats um HH:MM	Am **n**. Tag jedes Monats ausführen (beispielsweise am ersten oder zweiten) Tag des Monats oder in einem bestimmten Monat zu einer bestimmten Zeit.
Ausführen am n-ten Wochentag **jedes Monats/ eines bestimmten Monats um HH:MM**	Die Erfassung wird jeden Monat oder in einem bestimmten Monat an einem festgelegten Wochentag zu einer festgelegten Uhrzeit ausgeführt.

Benutzerdefiniert	Ausführung nach einem benutzerdefinierten Zeitplan.
	Verwenden Sie das Standard-5-Feld-Cron-Format (das erweiterte Cron-Format wird nicht unterstützt):
	`* * * * *`
	`| | | | +————Wochentag (0-6) (Sonntag=0)`

Aktion	Beschreibung

	`| | | +————————Monat (1-12)`
	`| | +————————Monatstag (1-31)`
	`| +————————Stunde (0-23)`
	`+————————Minute (0-59)`
	
	Verwenden Sie bei der Angabe von Werten die folgenden Zeichen:
	
	• **Leerzeichen( )**: Die einzelnen Felder mit einem Leerzeichen trennen.
	• **Sternchen (*)**: Ein Sternchen repräsentiert den gesamten Wertebereich in einem Feld. Zum Beispiel repräsentiert ein Sternchen im Stundenfeld eine beliebige Stunde.
	• **Kommas (,)**: Mehrere Werte in einem Feld werden mit einem Komma getrennt. Zum Beispiel werden mit `0,6` im Feld „Wochentag“ Sonntag und Samstag angegeben.
	• **Bindestriche (-)**: Mit einem Bindestrich wird ein Wertebereich in einem Feld angegeben. Zum Beispiel entspricht `1-5` im Feld „Wochentag“ `1,2,3,4,5`, d. h. Montag bis Freitag.
	• **Schrägstriche (/)**: Die Angabe der Zeitabstände, mit denen eine Aktion wiederholt werden soll, erfolgt mit einem Schrägstrich. Zum Beispiel entspricht `*/3` im Feld Stunde `0,3,6,9,12,15,18,21`. Das Sternchen (`*`) gibt jede Stunde an, mit `/3` erfolgt aber eine Einschränkung auf durch drei teilbare Stunden.
	
	Beispiele:
	
	• `15 * * * * Jeden Tag 15 Minuten nach jeder vollen Stunde ausführen`
	• `0 22 * * * Jeden Tag um 22:00 Uhr ausführen`
	• `0 0 1 1,6 * Am 1. Januar und 1. Juni um 00:00 Uhr ausführen`
	• `30 8,12 * * 1-5 An Wochentagen um 08:30 Uhr und 12:30 Uhr ausführen`
	• `0 2 */2 * * Jeden zweiten Tag um 02:00 Uhr ausführen`

Aufgabenplan anzeigen	Klicken Sie, um den Aufgabenplan anzuzeigen. Im Dialogfeld *Taskplan* wird eine Liste der geplanten Ziele angezeigt. Klicken Sie auf eine Aufgabe, um die Aufgabendetails anzuzeigen. Weitere Informationen hierzu finden Sie unter Aufgabenpläne anzeigen.
Wenn offline, bei nächster Verbindung ausführen	Wenn das Gerät derzeit offline ist, wird die Aktion ausgeführt, sobald das verwaltete Gerät das nächste

Aktion	Beschreibung
	Mal eine Verbindung mit der Appliance herstellt. Diese Option eignet sich für Geräte, die regelmäßig offline sind. Wenn diese Option nicht ausgewählt wird und das Gerät offline ist, wird die Aktion erst zum nächsten geplanten Zeitpunkt ausgeführt.

8. Klicken Sie auf **Speichern**.

   Die Seite *Linux Upgrade Package Schedule Summary (Zeitplan für Linux-Upgrade-Pakete - Übersicht)* wird eingeblendet, auf der der neu erstellte oder aktualisierte Zeitplan angezeigt wird. Weitere Informationen zu dieser Seite finden Sie unter Zeitplandetails der Linux-Paket-Upgrades überprüfen. Wenn Sie Geräte hinzugefügt haben, die den Kriterien für das Smart Label entsprechen, werden sie automatisch in den Patch-Zeitplan aufgenommen.

Zeitplandetails der Linux-Paket-Upgrades überprüfen

Wenn Sie einen Zeitplan für ein Linux-Paket-Upgrade konfigurieren, werden auf dieser Seite Details zur Konfiguration des Zeitplans und dessen Status angezeigt.

1. Rufen Sie die Seite *Linux Package Upgrade Schedule Summary (Zeitplan für Linux-Paket-Upgrades - Übersicht)* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Sicherheit** und anschließend auf **Linux Package Upgrades (Linux-Paket-Upgrades)**.
   c. Klicken Sie im Fensterbereich *Linux Package Upgrades Management (Verwaltung von Linux-Paket-Upgrades)* auf **Zeitpläne**.
   d. Klicken Sie auf den Namen eines Zeitplans für ein Linux-Paket-Upgrade.
2. Überprüfen Sie das Feld *Devices Targeted (Zielgeräte)*. Diese Zahl gibt die Anzahl der Linux-Geräte an, die für das Upgrade gemäß Zeitplan ausgewählt wurden.
3. Überprüfen Sie den Inhalt des Abschnitts *Konfiguration*.

Option	Beschreibung
Erstellt	Das Datum und die Uhrzeit der Erstellung des Zeitplans.
Geändert	Das Datum und die Uhrzeit der letzten Änderung des Zeitplans.
Letzte Ausführung	Das Datum und die Uhrzeit der letzten Ausführung des Zeitplans.
Name	Ein Name, der den Zeitplan genau bezeichnet. Dieser Name wird auf der Listenseite *Linux Package Upgrade Schedules (Zeitpläne für Linux-Paket-Upgrades)* angezeigt.

Option	Beschreibung
Aktion	Die mit dem Zeitplan verbundene Aktion: • **Detect All (Alle erkennen)**: Sucht nach allen Linux-Paket-Upgrades. • **Detect and Upgrade All (Alle erkennen und aktualisieren):** Sucht nach allen Linux-Paket-Upgrades, lädt die entsprechenden Dateien herunter und stellt sie auf den ausgewählten Geräten bereit.
Beschreibung	Eine kurze Beschreibung des Upgrade-Zeitplans für das Linux-Paket.
Geräte	Dieses Feld wird nur angezeigt, wenn der Zeitplan so konfiguriert ist, dass er auf alle Geräte angewendet wird.
Label des Geräts	Mindestens ein Smart Label, das mit den Geräten verknüpft ist, für die der Zeitplan ausgeführt wird. Weitere Informationen hierzu finden Sie unter Smart Labels für Patches verwenden. Dieses Feld wird nur angezeigt, wenn der Zeitplan so konfiguriert ist, dass er auf ausgewählte Geräte angewendet wird.
Gerätename	Mindestens ein ausgewähltes Geräte, für das der Zeitplan ausgeführt wird. Dieses Feld wird nur angezeigt, wenn der Zeitplan so konfiguriert ist, dass er auf ausgewählte Geräte angewendet wird.
Planen	Der ausgewählte Aktualisierungszeitplan. Klicken Sie auf **Aufgabenplan anzeigen**, um eine detaillierte Aufgabenplanung anzuzeigen. Klicken Sie im daraufhin angezeigten Dialogfeld auf eine Aufgabe, um die Aufgabendetails zu überprüfen. Weitere Informationen hierzu finden Sie unter Aufgabenpläne anzeigen.
Wenn offline, bei nächster Verbindung ausführen	Wenn das Gerät derzeit offline ist, wird die Aktion ausgeführt, sobald das verwaltete Gerät das nächste Mal eine Verbindung mit der Appliance herstellt.
Ausführung nach Wiederverbinden verzögern	Diese Option gibt an, wie lange sich der Zeitplan verzögert. Die Zeitspanne der Verzögerung beginnt zu dem Zeitpunkt, für den die Ausführung der Aktualisierungsaktion geplant wurde.
Beenden nach	Diese Option gibt die maximale Zeitspanne für die Ausführung des Zeitplans an. Wenn dieses Zeitlimit erreicht ist, werden alle laufenden Aktualisierungsaufgaben angehalten.

4. Überprüfen Sie im Abschnitt *Zeitplanstatus* den Gesamtstatus des Patch-Zeitplans auf einer der folgenden Registerkarten:

Registerkarte	Inhalt
Nach Computer	Geräte, die für das Upgrade ausgewählt wurden. Jeder Eintrag zeigt den Namen und die IP-Adresse des Geräts, den Upgrade-Status, die Upgrade-Ergebnisse und das Datum an, an dem das Upgrade abgeschlossen wird. Sie können Geräteknoten erweitern, um zusätzliche Informationen zu jedem Paket anzuzeigen, z. B. Paketname, Version, kompatibler Betriebssystemname, ob das Paket auf dem Gerät installiert ist und das Datum der Erkennung.
By Package (Nach Paket)	Upgrades, die zur Erkennung und Installation ausgewählt wurden. Jeder Eintrag zeigt den Paketnamen, seine Version, den Namen des kompatiblen Betriebssystems und die Paket-ID an und gibt an, ob das Paket installiert ist.
Erfordert ein Upgrade	Upgrades, die auf Geräten installiert werden können. Jeder Eintrag zeigt den Paketnamen, die Version und den Namen des kompatiblen Betriebssystems an. Sie können einen Aktualisierungsknoten erweitern, um die Geräte anzuzeigen, auf denen die Aktualisierung installiert werden soll.
Fehler bei der Bereitstellung	Unvollständige Aktualisierungen, die zu einem Bereitstellungsfehler geführt haben. Jeder Eintrag zeigt die Aktualisierungs-ID, die zugehörige Knowledge Base, den Aktualisierungsnamen und den zugehörigen Fehlercode an (siehe Fehlercodes aufgrund von Patching und Skripterstellung). Sie können Aktualisierungsknoten erweitern, um die Geräte anzuzeigen, auf denen der Fehler aufgetreten ist.

5. **Optional**. Nach Überprüfung der Zeitplandetails können Sie eine der folgenden Aktionen durchführen:
   - Klicken Sie zum Bearbeiten des Zeitplans auf **Bearbeiten**. Weitere Informationen hierzu finden Sie unter Zeitpläne für Windows-Funktionsaktualisierungen konfigurieren.
   - Klicken Sie auf **Jetzt ausführen**, um den Zeitplan auszuführen.
   - Um eine Kopie des Zeitplans zu erstellen, klicken Sie auf **Duplizieren**.
   - Um den Zeitplan zu löschen, klicken Sie auf **Löschen**.

Linux-Paket-Upgrades überprüfen

Während Sie die Aktion "Detect All" (Alle erkennen) ausführen, generiert die Appliance eine Liste der Pakete, die für ein Upgrade verfügbar sind.

Auf der Listenseite *Pakete* können Sie die neuesten Linux-Pakete anzeigen, die für ein Upgrade verfügbar und auf verwalteten Geräten installiert sind. Wählen Sie zunächst ein bestimmtes Linux-Betriebssystem aus, und überprüfen Sie den Inhalt der Liste, um eine Schätzung des Gerätepools zu erhalten, der eine Aktualisierung erfordert.

Die Liste zeigt für jedes Paket die Anzahl der Geräte, auf denen das Paket installiert ist oder nicht installiert ist, sowie den Prozentsatz der Geräte, auf denen die neueste Version ausgeführt wird.

1. Rufen Sie die Listenseite *Pakete* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Sicherheit** und anschließend auf **Linux Package Upgrades (Linux-Paket-Upgrades)**.
   c. Klicken Sie im Fensterbereich *Linux Package Upgrades Management (Verwaltung von Linux-Paket-Upgrades)* auf **Package Upgrade History (Paket-Upgradeverlauf)**.
2. Klicken Sie auf der Listenseite *Pakete* auf **Anzeigen nach**, und wählen Sie ein Linux-Betriebssystem aus. Zum Beispiel *RHEL* oder *Ubuntu*.

   Die Liste wird aktualisiert und zeigt die Pakete an, die für das ausgewählte Betriebssystem erkannt wurden.
3. Überprüfen Sie den Inhalt der Liste. Folgende Spalten sind verfügbar:

Spalte	Beschreibung
Paketname	Der Name des erkannten Pakets.
Version	Die aktuelle Paketversion.
Installiert	Die Anzahl der verwalteten Linux-Geräte, auf denen das ausgewählte Linux-Betriebssystem ausgeführt wird, auf dem das Paket installiert ist. Klicken Sie auf die Zahl in dieser Spalte, um eine Liste dieser Geräte auf der Listenseite *Geräte* anzuzeigen.
Erfordert ein Upgrade	Die Anzahl der verwalteten Linux-Geräte, auf denen das ausgewählte Linux-Betriebssystem ausgeführt wird und eine frühere Version dieses Pakets installiert ist und die für ein Upgrade geeignet sind. Klicken Sie auf die Zahl in dieser Spalte, um eine Liste dieser Geräte auf der Listenseite *Geräte* anzuzeigen.
Abschluss	Der Prozentsatz aller Geräte, auf denen dieses Paket installiert ist.

Aufrechterhalten der Geräte- und Appliance-Sicherheit

Mit der Appliance können Sie mithilfe standardmäßiger Sicherheitslückentests und Scans die Sicherheit von Geräten mit Agentenverwaltung testen. Prüfen Sie die täglichen Sicherheitsberichte und wenden Sie verfügbare Softwareaktualisierungen an, um die Appliance-Sicherheit zu gewährleisten.

Testen der Gerätesicherheit

Sie können die Ausführung von OVAL-Sicherheitslückentests und SCAP-Scans auf Geräten mit Agentenverwaltung planen, um die Gerätesicherheit zu testen.

Informationen zu OVAL-Sicherheitsprüfungen

OVAL (Open Vulnerability and Assessment Language) ist ein international anerkannter Standard zur Ermittlung von Sicherheitslücken und Konfigurationsproblemen auf Geräten.

OVAL-Sicherheitsprüfungen ermitteln Assets, die Compliance-Bedingungen nicht erfüllen, und ermöglichen Ihnen die Anpassung von Sicherheitsrichtlinien, um Regeln durchzusetzen, Tests für die automatische Ausführung zu planen und Berichte auf Basis der Ergebnisse auszuführen.

OVAL ist mit der CVE-Liste (Common Vulnerabilities and Exposures) bekannter Sicherheitslücken kompatibel. Der CVE-Inhalt wird von der CVE-Redaktion bestimmt, die aus Fachleuten aus der internationalen Community für Informationssicherheit besteht. Neue Informationen zu Sicherheitsrisiken, die im Forum der Community besprochen wurden, werden für eine mögliche Aufnahme in die Liste an die CVE-Initiative gesendet. Weitere Informationen zu CVE, zur MITRE Corporation und zur OVAL-Redaktion finden Sie unter http://cve.mitre.org.

Dank der Möglichkeit, Sicherheitslücken und Bedrohungen mithilfe eines gemeinsamen Standards zu beschreiben, wird die gemeinsame Nutzung von Sicherheitsdaten mit anderen CVE-kompatiblen Datenbanken und Programmen erleichtert.

HINWEIS: OVAL-Sicherheitsprüfungen können auf Geräten ausgeführt werden, auf denen ein unterstütztes Windows-, macOS- oder Linux-Betriebssystem ausgeführt wird. Java 1.7 oder höher muss auf verwalteten macOS- und Linux-Geräten installiert sein.

Informationen zu OVAL-Tests und -Definitionen

OVAL-Definitionen enthalten die für die Durchführung von OVAL-Tests benötigten Informationen. Hierzu zählen beispielsweise Prüfungen für Registrierungseinträge, Dateiversionen und WMI(Windows Management Instrumentation)-Daten.

Die OVAL-Testdefinitionen durchlaufen verschiedene Phasen, bevor sie herausgegeben werden. Je nachdem, wo sich eine Definition in diesem Prozess befindet, erhält sie einen der folgenden Statuswerte:

Status	Beschreibung
Entwurf	Gibt an, dass die Definition über eine OVAL-ID-Nummer verfügt und im Community-Forum und in der OVAL-Redaktion zur Diskussion steht.
Interim (Vorläufig)	Gibt an, dass die Definition derzeit von der OVAL-Redaktion geprüft wird und im Community-Forum zur Diskussion steht. Definitionen behalten diesen Status in der Regel zwei Wochen lang bei, sofern keine weiteren Änderungen oder Diskussionen erforderlich sind.
Accepted (Akzeptiert)	Gibt an, dass die Definition die Phase der Vorläufigkeit durchlaufen hat und auf den OVAL-Definitionsseiten veröffentlicht wird. Alle bisherigen Diskussionen in Bezug auf Definitionen mit dem Status Accepted (Akzeptiert) können über Links in der OVAL-Definition abgerufen werden.

Weitere mögliche Werte sind:

- Initial Submission (Erstsendung)
- Deprecated (Veraltet)

Weitere Informationen zu den Phasen von OVAL-Definitionen finden Sie unter http://cve.mitre.org.

Wenn OVAL-Tests aktiviert sind, werden alle verfügbaren OVAL-Tests auf den Zielgeräten ausgeführt.

Die Details zu OVAL-Tests enthalten keine Informationen zum Schweregrad der Sicherheitslücke. Beurteilen Sie selbst, ob Ihr Netzwerk auf ein bestimmtes Sicherheitsrisiko überprüft werden muss.

OVAL-Tests und -Definitionen anzeigen

OVAL-Tests und -Definitionen können Sie in der **Administratorkonsole** anzeigen.

1. Rufen Sie die Liste *OVAL-Katalog* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Sicherheit** und anschließend auf **OVAL-Scan**.
   c. Klicken Sie im Fensterbereich *OVAL-Scan* auf **Katalog**.
2. **Optional**: Schränken Sie mithilfe der Dropdown-Liste *Anzeigen nach* ein, welche Tests angezeigt werden. Sie können auch das Feld *Suchen* verwenden, um OVAL-Tests nach OVAL-ID, CVE-Nummer, Betriebssystem oder Text zu durchsuchen.
3. Klicken Sie in der Liste *OVAL-Katalog* auf den Link mit einem **Namen**.

   Die *OVAL-Definitionsdetailseite* wird mit folgenden Informationen angezeigt:

Feld	Beschreibung
OVAL-ID	Der Status der Sicherheitslücke, gefolgt von der OVAL-ID. Mögliche Werte sind "Entwurf", "Vorläufig" oder "Akzeptiert".
Klasse	Gibt die Art der Sicherheitslücke an. Folgende Werte sind möglich: Compliance, Veraltet, Patch und Sicherheitsrisiko.
Referenzkennung	Ein Link zu weiteren Details zu der Sicherheitslücke
Beschreibung	Die allgemeine Definition des Sicherheitsrisikos gemäß der CVE-Liste.
Definition	Gibt die Testschritte an, anhand derer bestimmt wird, ob die Sicherheitslücke besteht oder nicht.

   Die Tabelle am unteren Rand der Seite *OVAL-Tests: Definition* enthält die Liste mit den Geräten in Ihrem Netzwerk, die die Sicherheitslücke aufweisen. Eine druckerfreundliche Version dieser Daten ist ebenfalls verfügbar.

OVAL-Tests ausführen

Die Appliance führt auf der Grundlage des in den OVAL-Einstellungen definierten Zeitplans automatisch OVAL-Tests aus.

Die Ausführung der OVAL-Tests dauert etwa eine Stunde. Darüber hinaus beanspruchen OVAL-Tests sehr viel Arbeitsspeicher und CPU-Leistung und beeinträchtigen unter Umständen die Leistung der Zielgeräte. Daher sollten Sie OVAL-Tests wöchentlich oder monatlich zu einem Zeitpunkt ausführen, zu dem die Benutzer möglichst wenig gestört werden.

Darüber hinaus können Sie OVAL-Tests manuell ausführen, indem Sie sich bei dem Gerät als Administrator anmelden und `debug.bat` ausführen. Diese Datei befindet sich üblicherweise im Verzeichnis mit den Programmdaten. Beispiel: `C:\ProgramData\Quest\KACE\kbots_cache\packages\kbots\9`

OVAL-Tests mithilfe von Labels beschränken

Wenn Sie OVAL-Tests regelmäßig ausführen oder die OVAL-Testergebnisse nur für bestimmte Geräte abrufen möchten, können Sie diesen Geräten ein Label zuweisen. Dann haben Sie die Möglichkeit, OVAL-Tests mit der Funktion *Jetzt ausführen* nur auf diesen Geräten auszuführen.

Weitere Informationen zur Verwendung von Labels finden Sie unter Informationen zu den Labels.

Informationen zu OVAL-Aktualisierungen

Die Appliance prüft zwar jede Nacht, ob neue OVAL-Definitionen verfügbar sind, es ist jedoch nur einmal pro Monat mit neuen Definitionen zu rechnen. Sind OVAL-Tests aktiviert, lädt die Appliance unabhängig von den OVAL-Zeitplaneinstellungen neue OVAL-Definitionen bei der nächsten Skriptaktualisierung auf alle verwalteten Geräte herunter, sobald ein neues Paket verfügbar ist.

Die ZIP-Datei der OVAL-Aktualisierung kann über 30 MB groß sein und daher unter Umständen die Leistung von Geräten mit langsamer Verbindung beeinträchtigen. Die ZIP-Datei enthält 32- und 64-Bit-Versionen von OVAL Interpreter und verwendet jeweils die korrekte Version für das Gerät. OVAL Interpreter benötigt Microsoft .NET Framework und unterstützt sowohl die vollständige (erweiterte) Version als auch das Client-Profil.

OVAL-Einstellungen konfigurieren

Zur Ausführung von OVAL-Tests müssen Sie OVAL aktivieren, Zielgeräte und Betriebssysteme auswählen und einen Ausführungszeitplan festlegen.

OVAL-Tests benötigen umfangreiche Ressourcen und können die Leistung der Zielgeräte beeinträchtigen. Gehen Sie deshalb beim Konfigurieren von OVAL-Einstellungen mit Bedacht vor.

1. Rufen Sie die Seite *Detail zum OVAL-Zeitplan* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Sicherheit** und anschließend auf **OVAL-Scan**.
   c. Klicken Sie im Fensterbereich *OVAL-Scan* auf **Zeitpläne**.
2. Geben Sie im Abschnitt *Konfigurieren* folgende Einstellungen an:

Einstellung	Beschreibung
Aktiviert	Wird auf den Zielgeräten ausgeführt. Nur aktivierte Konfigurationen können ausgeführt werden. Wenn OVAL-Tests deaktiviert sind, werden Aktualisierungen auf der Appliance gespeichert, doch sie werden erst dann an die Zielgeräte übertragen, wenn OVAL-Tests aktiviert und geplant sind.
Ausführung bei abgemeldetem Benutzer zulassen	Ermöglicht die Ausführung, auch wenn kein Benutzer angemeldet ist. Deaktivieren Sie dieses Kontrollkästchen, um das Element nur

Einstellung	Beschreibung
	dann auszuführen, wenn ein Benutzer am Gerät angemeldet ist.

3. Geben Sie im Abschnitt *Bereitstellen* folgende Einstellungen an:

Einstellung	Beschreibung
Labels	Beschränken Sie die Bereitstellung auf Geräte, die zu angegebenen Labels gehören. Klicken Sie zum Auswählen von Labels auf **Bearbeiten**, ziehen Sie die Labels ins Fenster *Bereitstellung beschränken auf* und klicken Sie dann auf **Speichern**. Wenn Sie ein Label auswählen, das über eine Replikationsfreigabe oder eine alternative Download-Quelle verfügt, werden digitale Assets aus dieser Replikationsfreigabe oder aus dieser alternativen Download-Quelle kopiert und nicht direkt von der Appliance heruntergeladen. **HINWEIS:** Die Appliance nutzt eine Replikationsfreigabe, bevor sie den Alternativen KACE Speicherort verwendet.
Geräte	Beschränken Sie die Bereitstellung auf bestimmte Geräte. Wählen Sie aus der Dropdown-Liste die Geräte aus, auf denen Sie die Anwendung bereitstellen möchten. Um die Liste zu filtern, geben Sie einige Zeichen ins Feld *Geräte* ein. Die Zahl neben dem Feld zeigt die Anzahl der verfügbaren Geräte an. Benutzer mit eingeschränkten Zugriffsrechten sehen nur die Geräte, die mit ihrer Rolle verknüpft sind, wenn der Rolle ein Label zugewiesen ist. Weitere Informationen zu Benutzerrollen finden Sie unter Benutzerrollen hinzufügen oder bearbeiten.
Betriebssysteme	Wählen Sie das Betriebssystem, auf dem Sie bereitstellen möchten. a. Klicken Sie auf **Betriebssysteme verwalten**. b. Wählen Sie im daraufhin angezeigten Dialogfeld **Betriebssysteme** die Betriebssystemversionen in der Navigationsstruktur aus. Sie haben die Möglichkeit, Betriebssystemversionen nach Familie, Produkt, Architektur, Versions-ID oder Build-Version auszuwählen. Je nach Bedarf können Sie eine bestimmte Build-Version oder einen übergeordneten Knoten auswählen. Wenn Sie einen übergeordneten Knoten im Baum auswählen, werden die zugehörigen untergeordneten Knoten automatisch mit ausgewählt. Aufgrund dieses Verhaltens können Sie beliebige zukünftige Betriebssystemversionen auswählen, da Geräte in Ihrer verwalteten Umgebung hinzugefügt oder aktualisiert werden. Wenn Sie beispielsweise

Einstellung	Beschreibung
	alle aktuellen und zukünftigen Versionen auswählen möchten, die mit der Windows 10 x64-Architektur verbunden sind, wählen Sie unter **Alle** > **Windows** > **Windows 10** die Option **x64** aus.

4. Geben Sie im Abschnitt *Zeitplanung* die Zeit und Häufigkeit der OVAL-Ausführung an:

Einstellung	Beschreibung
Kein(e)	Die Ausführung erfolgt im Zusammenhang mit einem Ereignis anstatt zu einem bestimmten Datum oder zu einem bestimmten Zeitpunkt.
Alle n Minuten/Stunden	Der Vorgang wird im angegebenen Intervall durchgeführt.
Täglich/an einem bestimmten Tag um HH:MM	Die Erfassung wird täglich zu einem bestimmten Zeitpunkt oder an einem bestimmten Wochentag um eine bestimmte Uhrzeit ausgeführt.
Ausführen am n-ten jedes Monats/eines bestimmten Monats um HH:MM	Die Erfassung wird jeden Monat oder in einem bestimmten Monat an einem festgelegten Datum zu einer festgelegten Uhrzeit ausgeführt.
Ausführen am n-ten Wochentag **jedes Monats/ eines bestimmten Monats um HH:MM**	Die Erfassung wird jeden Monat oder in einem bestimmten Monat an einem festgelegten Wochentag zu einer festgelegten Uhrzeit ausgeführt.

Benutzerdefiniert	Ausführung nach einem benutzerdefinierten Zeitplan.
	Verwenden Sie das Standard-5-Feld-Cron-Format (das erweiterte Cron-Format wird nicht unterstützt):
	`* * * * *`
	`| | | | +————Wochentag (0-6) (Sonntag=0)`
	`| | | +————Monat (1-12)`
	`| | +————Monatstag (1-31)`
	`| +————Stunde (0-23)`
	`+————Minute (0-59)`
	Verwenden Sie bei der Angabe von Werten die folgenden Zeichen:
	• **Leerzeichen( )**: Die einzelnen Felder mit einem Leerzeichen trennen.
	• **Sternchen (*)**: Ein Sternchen repräsentiert den gesamten Wertebereich in einem Feld. Zum Beispiel repräsentiert ein Sternchen im Stundenfeld eine beliebige Stunde.
	• **Kommas (,)**: Mehrere Werte in einem Feld werden mit einem Komma getrennt. Zum Beispiel werden mit `0,6` im Feld „Wochentag“ Sonntag und Samstag angegeben.
	• **Bindestriche (-)**: Mit einem Bindestrich wird ein Wertebereich in einem Feld angegeben. Zum Beispiel entspricht `1-5` im Feld

Einstellung	Beschreibung
	„Wochentag“ `1,2,3,4,5`, d. h. Montag bis Freitag. • **Schrägstriche (/)**: Die Angabe der Zeitabstände, mit denen eine Aktion wiederholt werden soll, erfolgt mit einem Schrägstrich. Zum Beispiel entspricht `*/3` im Feld Stunde `0,3,6,9,12,15,18,21`. Das Sternchen (`*`) gibt jede Stunde an, mit `/3` erfolgt aber eine Einschränkung auf durch drei teilbare Stunden. Beispiele: • `15 * * * * Jeden Tag 15 Minuten nach jeder vollen Stunde ausführen` • `0 22 * * * Jeden Tag um 22:00 Uhr ausführen` • `0 0 1 1,6 * Am 1. Januar und 1. Juni um 00:00 Uhr ausführen` • `30 8,12 * * 1-5 An Wochentagen um 08:30 Uhr und 12:30 Uhr ausführen` • `0 2 */2 * * Jeden zweiten Tag um 02:00 Uhr ausführen`
Aufgabenplan anzeigen	Klicken Sie, um den Aufgabenplan anzuzeigen. Im Dialogfeld *Taskplan* wird eine Liste der geplanten Ziele angezeigt. Klicken Sie auf eine Aufgabe, um die Aufgabendetails anzuzeigen. Weitere Informationen hierzu finden Sie unter Aufgabenpläne anzeigen.

5. Klicken Sie auf **Speichern**.
6. Klicken Sie auf **Jetzt ausführen**, um das Skript sofort auszuführen.

   Tests werden auf den Geräten ausgeführt, die im Abschnitt *Bereitstellen* ausgewählt wurden.

OVAL-Sicherheitsrisikobericht anzeigen

Die Seite *OVAL-Bericht* zeigt die OVAL-Tests, die seit der letzten Aktualisierung der OVAL-Definitionen ausgeführt wurden.

Die OVAL-Ergebnisse auf dieser Seite werden gelöscht, wenn die OVAL-Definitionen aktualisiert werden. Falls Sie die Ergebnisse speichern möchten, erstellen Sie einen Zeitplan für die regelmäßige Ausführung eines OVAL-Geräteberichts. Siehe Zeitpläne für Berichte hinzufügen.

1. Rufen Sie die Seite *OVAL-Scan* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Sicherheit** und anschließend auf **OVAL-Scan**.
   c. Klicken Sie im Abschnitt *Berichterstellung* auf **Zusammenfassungsergebnisse anzeigen**.

Labels für betroffene Geräte übernehmen

In der *Testdetailansicht* werden alle Geräte angezeigt, die den OVAL-Test nicht bestanden haben. Sie können diesen Geräten ein Label zuweisen, um den Patch-Vorgang zu einem späteren Zeitpunkt durchzuführen.

1. Rufen Sie die Seite *OVAL-Scanzusammenfassung* auf:
   a. Klicken Sie in der linken Navigationsleiste auf **Sicherheit** und anschließend auf **OVAL-Scan**.
   b. Klicken Sie unter *Berichterstellung* auf **Geräte-Compliance anzeigen**.
2. Aktivieren Sie das Kontrollkästchen neben mindestens einem Test.
3. Klicken Sie auf **Aktion auswählen** und wählen Sie anschließend unter *Label für betroffene Geräte übernehmen* das entsprechende Label aus.

   Darüber hinaus können Sie nach Tests suchen, indem Sie in der Dropdown-Liste *Anzeigen nach* oberhalb der Tabelle auf der rechten Seite die entsprechende Auswahl vornehmen.

OVAL-Bericht anzeigen

Auf der Seite *OVAL-Geräte-Compliance* finden Sie eine Liste mit Geräten mit OVAL-Testergebnissen. Hier können Sie sich eine Zusammenfassung der Tests ansehen, die für bestimmte Geräte ausgeführt wurden.

Das Label in der Spalte *Gerät* auf der Seite *OVAL-Gerätebericht* ist die von der Appliance-Inventarkomponente zugewiesene Inventar-ID.

Wenn Sie weitere Informationen zu den Geräten im Bericht anzeigen möchten, klicken Sie auf den verknüpften Gerätenamen, um zur Gerätedetailseite zu gelangen.

1. Rufen Sie die Seite *OVAL-Geräte-Compliance* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Sicherheit** und anschließend auf **OVAL-Scan**.
   c. Klicken Sie unter *Berichterstellung* auf **Zusammenfassungsergebnisse anzeigen**.

      Die Seite *OVAL-Geräte-Compliance* wird mit einer OVAL-Berichtsliste angezeigt.

Informationen zu SCAP

SCAP (Secure Content Automation Protocol) ist ein offener Standard zur Angabe von Softwareschwachstellen, Überwachung sicherheitsbezogener Konfigurationen und Produktnamen sowie zur Untersuchung von Systemen im Hinblick auf Sicherheitslücken und zur Bewertung (Zahlenwert) der Auswirkungen der ermittelten Sicherheitsprobleme auf Windows-Geräten.

SCAP wird vom National Institute of Standards and Technology (NIST) verwaltet und von US-Regierungsbehörden wie dem Office of Management and Budget (US OMB) verbindlich vorgeschrieben.

SCAP verwendet die National Vulnerability Database der US-Regierung NVD, ein auf Standards basierendes Datenrepository der US-amerikanischen Regierung zur Verwaltung von Sicherheitslücken. NVD beinhaltet Datenbanken mit Sicherheitsprüflisten, sicherheitsbezogenen Softwareschwachstellen, fehlerhaften Konfigurationen, Produktnamen und Metriken für die Auswirkungen. Weitere Informationen zu SCAP sowie zur NVD finden Sie auf den Websites des NIST unter http://scap.nist.gov/index.html und http://nvd.nist.gov/.

Unterstützte SCAP-Versionen und Plattformen

Die Appliance unterstützt SCAP 1.0, 1.1 und 1.2. SCAP ist für Windows 7- (32-Bit und 64-Bit) und höhere Plattformen zertifiziert.

Die Appliance führt SCAP-Scans mithilfe der auf verwalteten Geräten installierten KACE Agent-Software durch. Für Geräte, auf denen die KACE Agent-Software nicht installiert ist, ist SCAP nicht verfügbar.

Durchführung von SCAP-Scans durch die Appliance

Im Rahmen von SCAP-Scans führt die Appliance Skripte auf ausgewählten Geräten mit Agentenverwaltung aus. Dabei verwendet sie Prüflisten für Sicherheitskonfigurationen aus dem National Checklist Repository.

Bei den SCAP-Versionen 1.0 und 1.1 überprüft das Skript den in XML-Formaten vorliegenden SCAP-Datenstrom anhand folgender SCAP-Standards: CCE, CPE, CVE, CVSS, OVAL und XCCDF. Siehe Definitionen von SCAP-Standards.

SCAP 1.2 wurde um das Konzept des Datenstroms erweitert. Hierzu werden die einzelnen Ergebnisdateien zu einer einzelnen XML-Datei zusammengefasst. Darüber hinaus kommt bei SCAP 1.2 das neue Ausgabeformat "ARF" (Asset Report Format 1.1) hinzu. Weitere Informationen hierzu finden Sie unter http://scap.nist.gov/specifications/arf/.

Die Appliance führt mithilfe der Agent-Software SCAP-Scan-Compliance-Prüfungen durch. Die Ergebnisdateien werden an die Appliance oder an die Organisationsdatenbank hochgeladen und zu einer einzelnen Datei zusammengefasst, um sie (bei Bedarf) einer Regierungsbehörde zu melden. Außerdem werden die Ergebnisse für die einzelnen Geräte auf der Seite *SCAP-Scanergebnisse* der Appliance angezeigt.

Ist auf der Appliance die Organisationskomponente aktiviert, können Sie die SCAP-Scanergebnisse für jede Organisation separat anzeigen.

SCAP verwendet die Version 5.10.1 von OVAL Interpreter und bietet Folgendes:

- Überwachung der Sicherheitskonfiguration von Geräten mit verschiedenen Betriebssystemen und Softwareanwendungen
- Sicherheitsstatus von Systemen zu jeder Zeit
- Compliance für verschiedene Sicherheitsanforderungen
- Eine standardisierte, automatisierte Methode zum Durchführen von Sicherheitsaufgaben
- Interoperabilität zwischen Sicherheitstools

Diese Funktionen verbessern die Softwaresicherheit, die Bedrohungsbewertung und die Beseitigung von Sicherheitslücken.

HINWEIS: Die Appliance unterstützt derzeit keine Anpassung.

Definitionen von SCAP-Standards

SCAP-Scans überwachen die Gerätesicherheit auf der Grundlage bestimmter Protokolle und Standards.

Standard	Definition
CCE	CCE (Common Configuration Enumeration) stellt eindeutige Bezeichner für Systemkonfigurationsprobleme bereit, um eine schnelle, präzise Korrelation von Konfigurationsdaten in mehreren Informationsquellen und Tools zu erleichtern. Die Ergebnisse der Compliance-Prüfung, die durch den SCAP-Scan der Appliance erzeugt wurden, umfassen die relevanten CCE ID-Referenzen zu XCCDF- und OVAL-Definitionen für jede überprüfte Regel, wie durch die Prüflistendefinition festgelegt.

Standard	Definition
	CCE-Informationen stehen sowohl in der XCCDF-Ergebnisdatei als auch auf der Seite *SCAP-Scanergebnisse* der Appliance zur Verfügung.
CPE	Bei CPE (Common Platform Enumeration) handelt es sich um ein strukturiertes Benennungsschema für IT-Systeme, -Plattformen und -Pakete. CPE basiert auf der generischen Syntax für Uniform Resource Identifiers (URI) und umfasst ein formales Namensformat, eine Sprache. zur Beschreibung komplexer Plattformen, eine Methode zur Prüfung von Namen anhand eines Systems sowie ein Beschreibungsformat zur Erstellung von Bindungen zwischen Text und Tests mit einem Namen. Im Wesentlichen sorgt CPE dafür, dass die Sicherheitsprüfliste auf die richtige Plattform angewendet wird. Diese Informationen stehen sowohl in der XCCDF-Ergebnisdatei als auch auf der Seite *SCAP-Scanergebnisse* der Appliance zur Verfügung.
CVE	"Common Vulnerability and Exposures" ist eine Liste (oder ein Verzeichnis) mit Standardbezeichnern (allgemeinen Namen) für öffentlich bekannte Sicherheitslücken und Softwareschwachstellen. Die Ergebnisse der Compliance-Prüfung durch den SCAP-Scan der Appliance umfassen die relevanten CCE ID-Referenzen und OVAL-Definitionen für jede überprüfte Regel aus der Prüflistendefinition. Auf der Seite *SCAP-Scanergebnisse* der Appliance stehen für jeden Patch und jede Sicherheitslücke CVE ID-Referenzen zur Verfügung. Die CVE-Informationen werden in einer durch den Scan generierten XML-Datei mit Patch-Ergebnissen gespeichert. Die Datei kann im Arbeitsverzeichnis des Agenten oder auf der Seite *SCAP-Scanergebnisse* des Servers überprüft werden.
CVSS	Das Common Vulnerability Scoring System ist ein offenes Framework für die Vermittlung von Merkmalen und Auswirkungen von IT-Sicherheitslücken. Das quantitative Modell gewährleistet wiederholbare, exakte Bewertungen und die Benutzer haben Einblick in die Merkmale der Sicherheitslücke, die den generierten Werten zugrunde liegen. CVSS eignet sich für Branchen, Organisationen und Behörden, die auf eine exakte und einheitliche Bewertung der Auswirkungen von Sicherheitslücken angewiesen sind. Das CVSS ist unter anderem hilfreich bei der Priorisierung von Aktivitäten zur Beseitigung von Sicherheitslücken sowie bei der Ermittlung des Schweregrads. Die National Vulnerability Database (NVD) stellt CVSS-

Standard	Definition
	Werte für nahezu alle bekannten Sicherheitslücken zur Verfügung.
OVAL	Bei OVAL (Open Vulnerability and Assessment Language) handelt es sich um einen internationalen Community-Informationssicherheitsstandard zur Verbreitung offener und öffentlich zugänglicher Sicherheitsinhalte. Er standardisiert die Übertragung dieser Informationen über das gesamte Spektrum an Sicherheitstools und -services hinweg. Die Ergebnisse jedes OVAL-Tests werden in mehrere Dateien auf dem Zielgerät geschrieben und dann in einer einzigen Ergebnisdatei auf der Appliance zusammengefasst und auf der Seite *SCAP-Scanergebnisse* angezeigt.
SCAP	Secure Content Automation Protocol (SCAP) ist ein offener Standard zur Angabe von Softwareschwachstellen, Überwachung sicherheitsbezogener Konfigurationen und Produktnamen sowie zur Untersuchung von Geräten im Hinblick auf Sicherheitslücken und zur Bewertung (Zahlenwert) der Auswirkungen der ermittelten Sicherheitsprobleme. Siehe Informationen zu SCAP.
XCCDF	Beim Format XCCDF (eXtensible Configuration Checklist Description) handelt es sich um eine Spezifikationssprache zum Schreiben von Sicherheitsprüflisten, Benchmarks und zugehörigen Dokumenten. Eine XCCDF-Datei enthält eine strukturierte Sammlung von Sicherheitskonfigurationsregeln für verschiedene Zielgeräte. Die Spezifikation dient zur Unterstützung von Informationsaustausch, Dokumenterstellung, organisations- und situationsbezogener Anpassung, automatisierten Compliance-Tests sowie Compliance-Bewertungen. Siehe Funktionsweise eines SCAP-Scans.

Informationen zu Benchmarks

Bei einem SCAP-Benchmark handelt es sich um eine Prüfliste für die Sicherheitskonfiguration mit einer Reihe von Regeln zur Bewertung von Sicherheitslücken eines Geräts in einer bestimmten Betriebsumgebung.

Das NIST (National Institute of Standards and Technology) verwaltet das National Checklist Repository, das verschiedene Prüflisten für Sicherheitskonfigurationen für bestimmte IT-Produkte sowie Kategorien von IT-Produkten enthält.

Der Benchmark-Standard USGCB (United States Government Configuration Baseline) hat sich aus der FDCC (Federal Desktop Core Configuration) entwickelt und gilt derzeit für Windows-Betriebssysteme.

Eine Prüfliste besteht aus einer ZIP-Datei, die verschiedene XML-Dateien enthält, die als SCAP-Datenstrom bezeichnet werden. Die erste Datei im Datenstrom ist die XCCDF-Datei. Bei der XCCDF-Datei enthält eine strukturierte Sammlung von Sicherheitskonfigurationsregeln für verschiedene Zielgeräte. Im Prinzip handelt es sich um eine Liste mit auszuführenden OVAL-Tests. Die anderen XML-Dateien enthalten die in der XCCDF-

Datei angegebenen OVAL-Tests. Ausführliche Informationen zur XCCDF-Spezifikation finden Sie unter http://scap.nist.gov/specifications/xccdf/.

Ein Benchmark kann ein oder mehrere Profile enthalten. Ein Profil gibt die Regeln an, die für bestimmte Arten von Geräten ausgeführt werden. Ein Benchmark kann beispielsweise Regeln für Desktops und andere Regeln für Server enthalten.

Funktionsweise eines SCAP-Scans

Vor dem Ausführen eines SCAP-Scans importiert und überprüft die Appliance einen Benchmark. Nach dem Import sowie der Überprüfung wird der Benchmark in die Appliance geladen und die XCCDF-Datei wird einem Prozess unterzogen, der als Auflösung bezeichnet wird.

Während der Auflösung wird die Datei `oval-command.zip` erzeugt. Diese ZIP-Datei enthält die Eingabedateien, die zum Ausführen eines bestimmten Profils erforderlich sind. Sie können die Dateien auf der Seite *Skriptdetail* anzeigen. Siehe SCAP-Zeitpläne konfigurieren.

Der SCAP-Scan wird durch ein KScript gesteuert. Beim Ausführen des Scans werden die folgenden Dateien als Skript-Abhängigkeiten auf das Zielgerät heruntergeladen:

- `benchmark.zip`: Enthält die Benchmark-Dateien, also den SCAP-Datenstrom, der auf die Appliance hochgeladen wurde. (Die XCCDF-Datei wird vom Gerät nicht verwendet.)
- `oval-command.zip`: Enthält die von der XCCDF-Datei erzeugten Eingabedateien.
- `ovalref.zip`: Enthält das OVAL-Scanmodul (`ovaldi.exe`).

Das KScript initiiert die OVAL-Scans auf dem Zielgeräte und erzeugt verschiedene Ergebnisdateien. Das OVAL-Scan-Modul wird zwei- oder dreimal ausgeführt:

- Bei der ersten Ausführung wird überprüft, ob das Zielgerät die richtige Plattform für dieses Benchmark-Profil ist. Dazu werden die im Benchmark enthaltenen CPE-Dateien verwendet.
- Bei der zweiten Ausführung werden die Sicherheitslücken des Geräts anhand der im Benchmark definierten Regeln überprüft. Außerdem wird der CCE-Standard implementiert.
- Bei der dritten Ausführung wird überprüft, dass die Sicherheits-Patches aktuell sind. Außerdem wird der CVE-Standard implementiert.

Jede Ausführung generiert eine Ergebnisdatei. Diese Dateien werden entsprechend der Ausführung benannt. So erhält beispielsweise die Datei aus der ersten Ausführung den Namen `scap-profile-10-result-1.xml` und die Datei aus der zweiten Ausführung den Namen `scap-profile-10-result-2.xml`. Diese Dateien befinden sich im folgenden Verzeichnis: `C:\Documents and Settings\All Users\Quest\KACE\kbots_cache\packages\kbots\`**<Arbeitsverzeichnis>**.

Das Arbeitsverzeichnis des KACE Agent finden Sie unter **Inventar** > **Geräte** > **Gerätedetail** > **Protokolle**.

Diese Ergebnisdateien werden auf die Appliance hochgeladen und zu einer Ergebnisdatei (`xccdf-results.xml`) zusammengefasst. Mithilfe dieser Datei können Sie die Ergebnisse einer Regierungsbehörde melden. Auf der Appliance und dem verwalteten Gerät werden nur die aktuellen Ergebnisdateien gespeichert.

Im letzten Schritt einer Ausführung wird ein Teil der Ergebnisdateien extrahiert, in der Organisationsdatenbank zur Berichterstellung gespeichert und auf der Seite *SCAP-Scanergebnisse* für jedes Gerät angezeigt.

Diese Informationen sind in den folgenden Datenbanktabellen enthalten: SCAP_RESULT, SCAP_RESULT_RULE und SCAP_RESULT_SCORE. Siehe SCAP-Scan-Ergebnisse anzeigen.

Auf SCAP-Scaninformationen zugreifen

SCAP-Scaninformationen stehen im Bereich *Sicherheit* zur Verfügung.

1. Rufen Sie die Seite *SCAP-Scan* auf:
    a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen*

aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.

b. Klicken Sie in der linken Navigationsleiste auf **Sicherheit** und anschließend auf **SCAP-Scan**.

c. Diese Seite hat drei Links:

- **Katalog**: Zeigt den Status von SCAP-Benchmarks an. Zudem können Sie über diese Seite Prüflisten importieren, löschen und im CSV-Format exportieren.
- **Zeitpläne**: Zeigt den Namen der Benchmarks sowie den geplanten Zeitpunkt für deren Ausführung an. Zudem können Sie über diese Seite Benchmarks hinzufügen und löschen, aktivieren oder deaktivieren und im CSV-Format exportieren.
- **Berichterstellung**: Zeigt die allgemeinen Ergebnisse von SCAP-Scans an.

Auf der Seite wird zudem ein Dashboard mit den Ergebnissen nach Benchmark angezeigt. Ein Gerät muss den Wert 100 % aufweisen, um einen Benchmark zu bestehen.

Benchmarks anzeigen und verwalten

Sie können SCAP-Benchmarks anzeigen und verwalten. Diese enthalten in die Appliance importierte Profile und Prüflisten.

Darüber hinaus können Sie Benchmarks auf der Seite *SCAP-Katalog* unter **Aktion auswählen** importieren, löschen und in das CSV-Format exportieren.

1. Rufen Sie die Seite *SCAP-Katalog* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Sicherheit** und anschließend auf **SCAP-Scan**.
   c. Klicken Sie im Fensterbereich *SCAP-Scan* auf **Katalog**.
2. **Optional**: Geben Sie über die Dropdown-Liste *Anzeigen nach* oder über das Feld *Suchen* an, welche Benchmarks angezeigt werden.

   Sie können im Titel oder Bezeichner nach Teilzeichenfolgen suchen.
3. **Optional**: Klicken Sie zum Sortieren der Benchmarks auf eine Spaltenüberschrift.
4. Klicken Sie auf den Namen eines Benchmarks, um Details anzuzeigen.

   Der*SCAP-Katalog* enthält allgemeine Informationen zum ausgewählten Benchmark sowie die Zeit, zu der die SCAP-Daten an die Appliance hochgeladen wurden. Siehe Benchmarks aus dem Archiv herunterladen.

Benchmarks importieren und ändern

Sie können Benchmarks aus dem National Checklist Repository nach Bedarf importieren und ändern.

Benchmarks und Prüflisten stehen im National Checklist Repository unter https://web.nvd.nist.gov/view/ncp/repository zum Download bereit.

1. Rufen Sie die Seite *SCAP-Katalog* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Sicherheit** und anschließend auf **SCAP-Scan**.
   c. Klicken Sie im Fensterbereich *SCAP-Scan* auf **Katalog**.
2. Wählen Sie **Aktion auswählen** > **Neue Prüflisten importieren**.

Auf der Seite *Scan-Einstellungen für die SCAP-Konfiguration* wird Schritt 1 des Assistenten für den Import angezeigt.

3. Klicken Sie auf **Durchsuchen** oder **Datei auswählen**, um eine Benchmark-ZIP-Datei zu importieren.
4. Klicken Sie auf **Weiter**.

   Ein Dialogfeld mit der Meldung, dass die Datei hochgeladen wird, wird angezeigt. Nach dem Hochladen der Datei wird in einer Meldung auf der Seite *Scan-Einstellungen für die SCAP-Konfiguration* angezeigt, dass der Import erfolgreich durchgeführt wurde.

   HINWEIS: Die Appliance überprüft, ob die ZIP-Datei gültige Benchmarks enthält. Wenn keine gültigen Benchmarks vorhanden sind, wird eine Fehlermeldung angezeigt und die Datei wird nicht hochgeladen.

5. Wählen Sie in der Dropdown-Liste *Wählen Sie ein Profil zum Überprüfen aus* einen Benchmark aus und klicken Sie dann auf **Weiter**.

   Schritt 2 wird angezeigt.

6. Wählen Sie in der Dropdown-Liste *Mit vorhandenem Modul überprüfen* das gewünschte OVAL-Modul aus.

   HINWEIS: Das Standardmodul ist OVAL Interpreter von MITRE (`ovaldi.exe`). Die Appliance lädt automatisch Aktualisierungen für dieses Modul herunter, wenn Quest neue Versionen des Moduls und OVAL-Definitionen zertifiziert und veröffentlicht.

7. **Optional**: Klicken Sie auf **Durchsuchen** oder **Datei auswählen**, um nach einem benutzerdefinierten Modul und den zugehörigen Konfigurationsdateien zu suchen und diese hochzuladen.

   In einem Dialogfeld wird die Meldung angezeigt, dass die Datei hochgeladen wird. Zudem wird auf der Seite *Scan-Einstellungen für die SCAP-Konfiguration* die Meldung angezeigt, dass das Modul erfolgreich importiert wurde.

   TIPP: Verwenden Sie ein benutzerdefiniertes Modul, wenn Sie das OVAL-Modul lokal steuern möchten oder nicht möchten, dass das Modul durch automatische Aktualisierungen geändert wird. Beim benutzerdefinierten Modul handelt es sich um die ZIP-Datei eines Ordners, der die benutzerdefinierte Datei `ovaldi.exe` sowie die Konfigurationsdateien enthält, die zum Ausführen des Moduls erforderlich sind. Diese ZIP-Datei ersetzt die Abhängigkeitsdatei `ovalref.zip` im SCAP-Scan-Skript. Siehe Aufgelöste XCCDF-Dateien anzeigen.

8. Klicken Sie auf **Weiter**.

Zunächst wird ein Dialogfeld mit der Meldung angezeigt, dass die Benchmark-Datei geladen wird. Anschließend wird die Seite *Skriptdetail* angezeigt. Siehe SCAP-Scanzeitpläne bearbeiten.

SCAP-Zeitpläne konfigurieren

Durch die Konfiguration von SCAP-Zeitplänen können Sie Benchmarks oder Definitionen importieren und Einstellungen für SCAP-Scans ändern.

1. Rufen Sie die Seite *SCAP-Scanzeitpläne* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Sicherheit** und anschließend auf **SCAP-Scan**.
   c. Klicken Sie im Fensterbereich *SCAP-Scan* auf **Zeitpläne**.
2. Wählen Sie unter **Aktion auswählen** eine Aktion aus, um Benchmarks hinzuzufügen, zu löschen, zu aktivieren, zu deaktivieren oder im CSV-Format zu exportieren.
3. Klicken Sie auf einen Benchmark, um dessen Zeitplan auf der *Skriptdetailseite* zu bearbeiten.
4. Scrollen Sie auf der Seite nach unten zum Abschnitt *Zeitplanung* und nehmen Sie die erforderlichen Änderungen vor.

SCAP-Scanzeitpläne bearbeiten

Sie können den Zeitplan eines Benchmarks auf der Seite *Skriptdetail* anzeigen und bearbeiten. Auf dieser Seite können Sie Skripte zum Konfigurieren, Planen und Festlegen, auf welchen Geräten der SCAP-Scan ausgeführt wird, verwalten und anpassen. Bei den Skripten für SCAP handelt es sich um standardmäßige KScripts.

HINWEIS: In diesem Abschnitt werden nicht alle auf der Seite *Skriptdetail* verfügbaren Funktionen beschrieben. Hier finden Sie lediglich grundlegende Informationen zu SCAP-Scans sowie Informationen zur Verwendung eines SCAP-Scans.

HINWEIS: Ausführlichere Informationen zur Bearbeitung eines KScript finden Sie unter Hinzufügen und Bearbeiten von Skripten.

Die Seite *Skriptdetail* können Sie über den Benchmark-Assistenten (siehe Auf SCAP-Scaninformationen zugreifen) oder über die Seite *SCAP-Scanzeitpläne* (siehe SCAP-Scan-Ergebnisse anzeigen) aufrufen.

Aufgelöste XCCDF-Dateien anzeigen

Sie können die Eingabedateien anzeigen, die vom Auflösungsprozess des SCAP-Scans generiert wurden.

Ein Benchmark wird auf dem Server geladen und die XCCDF-Datei wird einer so genannten Auflösung unterzogen. Dabei werden die Eingabedateien generiert, die zum Ausführen eines bestimmten Profils erforderlich sind.

1. Rufen Sie die *Skriptdetailseite* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Skripterstellung** und anschließend auf **Skripte**.
   c. Klicken Sie auf den Namen eines Skripts.
2. (Optional) Scrollen Sie zum Abschnitt *Abhängigkeiten*, klicken Sie auf **Neue Abhängigkeit hinzufügen** und klicken Sie anschließend auf **Durchsuchen** oder auf **Datei auswählen**, um die zusätzlichen ausführbaren Dateien hinzuzufügen, die für die Ausführung des Skripts erforderlich sind.
3. **Optional**: Um die Details dieser Dateien anzuzeigen, klicken Sie auf die ausgewählte ZIP-Datei und laden Sie diese Datei herunter.
4. Wenn Sie wissen möchten, wie diese Abhängigkeitsdateien ausgeführt werden, lesen Sie die Abschnitte *Aufgabe*.

OVAL-Zeitstempel anzeigen

Sie können den OVAL-Zeitstempel anzeigen. Dieser gibt Aufschluss darüber, wann das OVAL-Dokument kompiliert wurde.

1. Rufen Sie die *Skriptdetailseite* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Skripterstellung** und anschließend auf **Skripte**.
   c. Klicken Sie auf den Namen eines Skripts.
2. Scrollen Sie nach unten zum Abschnitt *Abhängigkeiten*, klicken Sie auf **benchmark.zip** und extrahieren die OVAL XML-Datei.

   Beispiel: `fdcc-winxp-oval.xml`.
3. Suchen Sie in der OVAL-Datei nach **<oval:timestamp>**.

Skriptaufgaben anzeigen

Sie können Aufgaben für ein bestimmtes Skript anzeigen.

1. Rufen Sie die *Skriptdetailseite* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Skripterstellung** und anschließend auf **Skripte**.
   c. Klicken Sie auf den Namen eines Skripts.
2. Scrollen Sie nach unten zu den Bereichen *Aufgabe*.

Die Aufgabenabschnitte werden auf der *Skriptdetailseite* angezeigt.

SCAP-Scan-Ergebnisse anzeigen

Auf der Seite *Scan-Ergebnisse* werden die Ergebnisse von SCAP-Scans pro Gerät angezeigt. Über diese Seite können Sie ausführliche Informationen zu den einzelnen Scans aufrufen.

1. Rufen Sie die Seite *SCAP-Scan* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Sicherheit** und anschließend auf **SCAP-Scan**.
   c. Klicken Sie im Fensterbereich *SCAP-Scan* auf **Berichterstellung**.
2. **Optional**: Um die Ergebnisse für einen bestimmten Benchmark anzuzeigen, wählen Sie in der Dropdown-Liste *Anzeigen nach*, die über der Tabelle auf der rechten Seite angezeigt wird, den gewünschten Benchmark aus.

   Die Ergebnisseite enthält die folgenden Informationen:

Abschnitt	Beschreibung
Gerätename	Das Gerät, auf dem der Scan ausgeführt wurde.
Benchmarkprofil	Das verwendete Profil in einem Benchmark.
Überprüft	Das Datum und die Uhrzeit der Ausführung des Scans.
Bestanden	Die Anzahl der Regeln, die vom Gerät eingehalten werden.
Fehler	Die Anzahl der Regeln, die vom Gerät nicht eingehalten werden.
Andere	Die Anzahl der Regeln, die einen anderen Wert aufweisen, zum Beispiel Fehler, unbekannt, nicht überprüft, nicht anwendbar oder zu Informationszwecken.

Abschnitt	Beschreibung
	Die XCCDF-Spezifikation definiert auch den Wert "nicht ausgewählt", der in den Ergebnissen jedoch nicht angezeigt wird.
Gesamtzahl	Die Gesamtzahl der Regeln, die ausgeführt wurden.
Compliance	Der Prozentsatz der Regeln, die eingehalten werden.
Punkt	Der vom Benchmark definierte Standardwert.
Ergebnis	Die Ergebnisse ("Erfolgreich" bzw. "Fehler") des Scans.

3. Klicken Sie zum Anzeigen der Details eines bestimmten Geräts in der Spalte *Gerät* auf dessen Namen.

   Eine Seite mit den Details des Scan-Ergebnisses für das ausgewählte Gerät wird angezeigt. In der folgenden Tabelle werden die einzelnen Abschnitte ausführlicher beschrieben:

Abschnitt	Beschreibung
Übersicht	Allgemeine Informationen zum Benchmark.
Testergebnisse	Testergebnisse in einer Baumstruktur, mit der die Gruppierung der Regeln dargestellt wird. Symbole zeigen den Status (erfolgreich/Fehler) einer Regel an. Sie können auf eine Regel klicken, um ein Dialogfeld mit den Details der Regel anzuzeigen.
Punkte	Compliance-Werte für die einzelnen für den Benchmark definierten Punktemodelle.
Ergebnisse nach CCE	Erfolgreich/Fehler-Ergebnisse nach CCE. Für die FDCC-Konfiguration muss die Compliance durch CCE gemeldet werden.
XML-Ergebnisdateien	Links für die XML-Dateien: • **XCCDF-Benchmark**: Die bei jeder Ausführung des OVAL-Scan-Moduls von der XCCDF-Datei verarbeitete und in einer einzigen Ergebnisdatei (`xccdf-results.xml`) formatierte Datei. • **CPE-Inventar**: Die Datei, die bei der ersten Ausführung des OVAL-Scan-Moduls ausgeführt wird, um sicherzustellen, dass der Benchmark für das geprüfte Gerät geeignet ist. • **OVAL-Compliance**: Die Datei, die bei der zweiten Ausführung des OVAL-Scan-Moduls ausgeführt wird, um sicherzustellen, dass die

Abschnitt	Beschreibung
	im Benchmark definierten Regeln vom Gerät eingehalten werden. • **OVAL-Patches**: Die Datei, die bei der dritten Ausführung des OVAL-Scan-Moduls ausgegeben wird, um sicherzustellen, dass die Sicherheits-Patches aktuell sind. Siehe Funktionsweise eines SCAP-Scans.

4. Um die Details einer Regel anzuzeigen, klicken Sie auf das Symbol der Regel.

   Die Seite *Details anzeigen* für diese Regel wird angezeigt. Auf dieser Seite wird eine Beschreibung der Regel aus der XCCDF-Definition sowie die XML-Datei für die Regel angezeigt. Zudem wird angezeigt, ob die Regel vom Gerät eingehalten wird.

Benchmarks aus dem Archiv herunterladen

Die Appliance erfasst täglich die SCAP-Scanergebnisse von Geräten und erstellt für jeden Benchmark ein Archiv. Bei dem Benchmark-Archiv handelt es sich um eine ZIP-Datei, die an die zuständige Behörde gesendet werden kann.

1. Rufen Sie die Seite *SCAP-Katalog* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Sicherheit** und anschließend auf **SCAP-Scan**.
   c. Klicken Sie im Fensterbereich *SCAP-Scan* auf **Katalog**.
2. Klicken Sie auf den Namen des herunterzuladenden Benchmarks.
3. Klicken Sie im Feld *Ergebnisarchiv herunterladen* auf die ZIP-Datei, um das Archiv herunterzuladen.

   Diese Datei enthält die Ergebnisse für alle Geräte, die mit dem ausgewählten Benchmark gescannt wurden.

Windows Sicherheitsprobleme beheben, die die Agenten-Provisionierung verhindern

Wenn Windows Sicherheitseinstellungen verhindern, dass die Appliance den Agenten für Windows Geräte bereitstellen kann, können Sie die Einstellungen über eine Eingabeaufforderung neu konfigurieren.

Zum Zulassen der Provisionierung müssen Sie die Firewall öffnen und die Sicherheitseinstellungen konfigurieren.

1. Öffnen Sie eine Eingabeaufforderung auf dem Gerät.
2. Öffnen Sie die Firewall und konfigurieren Sie die Sicherheitseinstellungen:

```
reg add HKLM\SYSTEM\CurrentControlSet\Control\Lsa /v ForceGuest /t REG_DWORD /d
0 /f
```

```
reg add HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\system /v
LocalAccountTokenFilterPolicy /t REG_DWORD /d 1 /f
```

```
reg add "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server" /v
FdenyTSConnections /t REG_DWORD /d 0 /f
```

```
netsh.exe firewall set service type=FILEANDPRINT mode=ENABLE scope=ALL
```

```
netsh.exe firewall set service type=REMOTEADMIN mode=ENABLE scope=ALL
```

Aufrechterhalten der Appliance-Sicherheit

Prüfen Sie die täglichen Sicherheitsberichte und wenden Sie verfügbare Softwareaktualisierungen an, um die Appliance-Sicherheit zu gewährleisten.

Verfügbare Softwareaktualisierungen für die Appliance werden auf dem Appliance-Dashboard angekündigt.

Security Run Output (Sicherheitsbericht)

Die E-Mail **Sicherheitsbericht** gibt Aufschluss über den Sicherheitsstatus der Appliance.

Der Sicherheitsbericht **Security Run Output** der Appliance geht dem Systemadministrator automatisch täglich um 2:00 Uhr per E-Mail zu.

Das folgende Beispiel zeigt den Inhalt des Sicherheitsberichts **Security Run Output**.

```
Checking setuid files and devices:
Checking for uids of 0:
root 0
toor 0
Checking for passwordless accounts:
MyK1 kernel log messages:
+++ /tmp/security.G1jFJvQh 2013-04-21 02:01:01.000000000 -0700
+em0: link state changed to DOWN
+em0: link state changed to UP
+em0: link state changed to DOWN
+em0: link state changed to UP
+em0: link state changed to DOWN
+em0: link state changed to UP
+em0: link state changed to DOWN
+em0: link state changed to UP
+em0: link state changed to DOWN
+em0: link state changed to UP
+em0: link state changed to DOWN
+em0: link state changed to UP
+em0: link state changed to DOWN
+em0: link state changed to UP
MyK1 login failures:
MyK1 refused connections:
-- End of security output --
```

Verwenden von Berichten und Zeitplanung für Benachrichtigungen

Sie können die Appliance so konfigurieren, dass sie Berichte ausführt und Benachrichtigungen an Administratoren sendet, wenn bestimmte Kriterien erfüllt sind.

Informationen zu Berichten und Benachrichtigungen

Mit der Appliance können Sie verschiedene Berichte und Benachrichtigungen erstellen und planen. Berichte erfassen Informationen zu Inventarelementen. Mit Benachrichtigungen kann die Appliance Sie per E-Mail informieren, wenn bestimmte Kriterien erfüllt sind.

Informationen zu Berichten

Die Appliance enthält eine Vielzahl von Standardberichten für Software, Hardware, Service Desk und andere Elemente.

Wenn auf der Appliance die Organisationskomponente aktiviert wurde, können Sie Berichte für jede Organisation und für die Systemebene getrennt erstellen und ausführen. Berichte auf Systemebene enthalten konsolidierte Berichte, die Informationen von allen Organisationen zusammenfassen, sowie Standardberichte für verschiedene Appliance-Komponenten.

Informationen zu Benachrichtigungen

Bei Benachrichtigungen handelt es sich um E-Mail-Nachrichten, die von der Appliance an Administratoren gesendet werden, wenn Geräte, Scan-Ergebnisse und Assets bestimmte Kriterien erfüllen.

Sie können zum Beispiel E-Mail-Benachrichtigungen basierend auf der Datenträgernutzung einrichten, wenn Sie Administratoren benachrichtigen möchten, sobald ein bestimmtes Speicherlimit auf einem Datenträger erreicht ist. Die Benachrichtigungen werden gesendet, wenn die Geräte die angegebenen Kriterien erfüllen.

Die Appliance überprüft das Inventar anhand der Kriterien gemäß der in den Benachrichtigungszeitplänen angegebenen Häufigkeit. Wenn ein Element den Kriterien entspricht, sendet die Appliance eine E-Mail an die angegebenen Empfänger.

Standardmäßig überprüft die Appliance das Inventar stündlich. Bearbeiten Sie den Benachrichtigungszeitplan, um die Häufigkeit zu ändern. Siehe Benachrichtigungszeitpläne bearbeiten.

HINWEIS: Benachrichtigungen und tägliche Berichte werden von der Standardadresse "Charlie Root" (`root@`**appliance_hostname**) versendet. Diese Adresse kann nicht geändert werden.

Änderungsnachverfolgung für die Berichteinstellungen

Wenn Verlaufsabonnements zur Aufbewahrung von Informationen konfiguriert wurden, können Sie Details zu den an Einstellungen, Assets und Objekten vorgenommenen Änderungen anzeigen.

Diese Informationen beinhalten auch das Datum der Änderung und den Benutzer, der diese vorgenommen hat. Dies kann bei der Fehlerbehebung nützlich sein. Siehe Informationen zu den Verlaufseinstellungen.

Erstellen und Ändern von Berichten

Sie können Berichte auf Listenseiten mithilfe von SQL-Abfragen sowie im Abschnitt *Berichterstellung* mithilfe des Berichts-Assistenten erstellen.

Erstellen von Berichten

Sie können Berichte erstellen, um Daten (etwa Inventarinformationen) zu erfassen und zu analysieren.

Es stehen verschiedene Möglichkeiten zur Verfügung, um Berichte zu erstellen:

- Verwenden Sie den Berichts-Assistenten auf der Seite Berichte. Siehe Berichte mit dem Berichts-Assistenten erstellen.
- Verwenden Sie den SQL-Bericht auf der Seite Berichte. Siehe Berichte mithilfe von SQL-Abfragen erstellen.
- Verwenden Sie die Menüoption auf Listenseiten (beispielsweise *Geräte*, *Assets* oder *Verwaltete Installationen*). Siehe Berichte über Listenseiten erstellen.

Zusätzlich können Sie Diagramme und Grafiken erstellen, indem Sie Berichte im XLS-Format (Microsoft Excel) oder CSV-Format (durch Komma getrennte Werte) erstellen und die Daten anschließend in Tools wie Microsoft Excel importieren.

HINWEIS: Beachten Sie, dass Multibytezeichen, die beispielsweise für die Unterstützung japanischer oder chinesischer Zeichensätze verwendet werden, möglicherweise als unlesbare Zeichen angezeigt werden, wenn CSV-Dateien in Excel importiert werden. Weitere Informationen erhalten Sie vom **Quest Support** unter https://support.quest.com/contact-support.

Berichte mit dem Berichts-Assistenten erstellen

Mit dem Berichts-Assistenten können Sie die zu erfassenden Datenbankinformationen ohne Erstellung von SQL-Abfragen angeben.

1. Führen Sie eine der folgenden Aktionen aus, um die Liste *Berichte* aufzurufen:
   - **Wenn für Ihre Appliance die Organisationskomponente aktiviert ist, können Sie folgendermaßen auf einen Bericht auf Systemebene zugreifen:**

     Melden Sie sich bei der Systemadministratorkonsole der Appliance an: `https://`**appliance_hostname**`/system`. Oder wählen Sie in der Dropdown-Liste rechts oben auf der Seite den Eintrag **System** aus. Klicken Sie anschließend auf **Berichterstellung**.

Berichte auf Systemebene enthalten konsolidierte Berichte, die Informationen von allen Organisationen zusammenfassen, sowie Standardberichte für verschiedene Appliance-Komponenten.

- **Wenn die Organisationskomponente nicht für die Appliance aktiviert ist oder Sie auf einen Bericht auf Organisationsebene zugreifen möchten, melden Sie sich bei der Administratorkonsole der Appliance an: `https://appliance_hostname/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option** *Organisationsmenü in Verwaltungskopfzeile anzeigen* **aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus. Klicken Sie anschließend auf Berichterstellung.**

  Berichte auf Organisationsebene enthalten Standardberichte für verschiedene Appliance-Komponenten. Wenn für Ihre Appliance die Organisationskomponente aktiviert ist, liefern diese Berichte Informationen speziell für die ausgewählte Organisation.

Die Liste *Berichte* wird angezeigt.

2. Wählen Sie **Aktion auswählen > Neu (Assistent)**, um die Seite *Titel und Thema* anzuzeigen.
3. Legen Sie die folgenden Einstellungen fest:

Option	Beschreibung
Titel	Der Anzeigename des Berichts, der in der Berichtsliste angezeigt wird. Der Titel sollte möglichst aussagekräftig sein, um diesen Bericht leichter von anderen Berichten in der Liste unterscheiden zu können.
Kategorie	Die Kategorie des Berichts. Wenn die Kategorie noch nicht vorhanden ist, wird sie der Dropdown-Liste auf der Seite *Berichte* hinzugefügt.
Beschreibung	Eine Beschreibung des Berichts
Zeilennummern anzeigen	Zeigt auf dem Bericht eine Spalte mit Zeilennummern an.
Thema	Das Thema des Berichts. Diese Einstellung legt fest, welche Felder für den Bericht verfügbar sind.
Unterthema hinzufügen	Klicken Sie auf diesen Link, um bis zu zwei verwandte Themen zum Bericht hinzuzufügen. Sie können damit Beziehungen zwischen bis zu drei Datentypen in ein und demselben Bericht anzeigen. Wenn Sie den Bericht im HTML-Format erstellen, können Sie die Zeilen erweitern oder reduzieren, um nach Bedarf Detailinformationen anzuzeigen. Wenn Sie auf **Unterthema hinzufügen** klicken, werden abhängig vom ausgewählten Thema verschiedene Optionen zur Verfügung gestellt. Wenn Sie beispielsweise **Gerät**, **Software** und

Option	Beschreibung
	Dateisynchronisierung auswählen, werden die beiden folgenden Kontrollkästchen angezeigt: • Nur Zeilen von **Gerät** anzeigen, die mindestens eine **Dateisynchronisierung**-Zeile umfassen. • Nur Zeilen von **Dateisynchronisierung** anzeigen, die mindestens eine **Software**-Zeile umfassen. Das Aktivieren dieser Kontrollkästchen schränkt den Bericht auf Geräte und Software ein, für die mindestens eine untergeordnete Zeile vorhanden ist. Zeilen für Geräte werden in dem Bericht nur angezeigt, wenn sie über mindestens eine entsprechende Zeile für Software verfügen. Zeilen für Software werden in dem Bericht nur angezeigt, wenn sie über mindestens eine entsprechende Zeile für die Dateisynchronisierung verfügen. Deaktivieren Sie diese Kontrollkästchen, um alle Zeilen für Geräte und Software anzuzeigen – unabhängig davon, ob sie über Zeilen für Software bzw. Dateisynchronisierung verfügen.

4. Klicken Sie auf **Weiter**, um die Seite *Anzuzeigende Felder* anzuzeigen.
5. Wählen Sie die Felder aus, die Sie in den Bericht aufnehmen möchten.
6. Klicken Sie auf **Weiter**, um die Seite *Spaltenreihenfolge* anzuzeigen.
7. Ziehen Sie die Spaltenüberschriften von oben nach unten in die gewünschte Reihenfolge. Bei der Berichtausgabe werden die Spalten von links nach rechts angezeigt.
8. Klicken Sie auf **Weiter**, um die Seite *Sortieren und Untergliederung* anzuzeigen.
9. Konfigurieren Sie die Anordnung der Zeilen:
   - **Sortieren nach**: Geben Sie an, wie die Ergebnisse sortiert werden sollen. Die Berichtsdaten werden nach der Auswahl im ersten Feld, dann nach der Auswahl im zweiten Feld und schließlich nach der Auswahl im dritten Feld strukturiert. Das erste Sortierfeld wird durch das Feld aufgefüllt, das zur Darstellung als erstes Feld auf der Berichtausgabeseite ausgewählt wurde.
   - **Sequenz**: Geben Sie an, ob die Ergebnisse in auf- oder absteigender Reihenfolge (alphanumerisch) angezeigt werden sollen.
   - **Untergliederungsüberschrift**: Wählen Sie aus, ob die Ergebnisse unter einer Zwischenüberschrift gruppiert werden sollen, wobei der Name des in der Spalte *Sortieren nach* ausgewählten Feldes verwendet wird.
10. Klicken Sie auf **Weiter**, um die Seite *Filter* anzuzeigen.
11. **Optional**: Fügen Sie Filterkriterien hinzu, wenn Sie in Ihrem Bericht nicht den gesamten Datensatz ausgeben möchten:
    a. Klicken Sie auf **Geben Sie Regeln zum Filtern der Daten an**.

       Ein Regelsatz mit *Trifft auf alle zu* wird angezeigt. Diese Regeln entsprechen in boolescher Logik **UND**-Anweisungen. Elemente müssen allen Regeln in diesem Abschnitt entsprechen, um in den Bericht aufgenommen zu werden.

    b. Legen Sie Filterkriterien fest und klicken Sie auf **Speichern**.
    c. Um eine Regel zum aktuellen Regelsatz hinzuzufügen, klicken Sie auf die Schaltfläche **Hinzufügen** +.
    d. Wählen Sie die Filterkriterien und klicken Sie rechts neben der Zeile auf **Speichern**.

e. Klicken Sie auf die Schaltfläche **Untergruppe hinzufügen**, um eine Untergruppe von Regeln hinzuzufügen: .

Die erste geschachtelte Untergruppe fügt einen Regelsatz vom Typ **Trifft auf eines zu** hinzu. Diese Regeln entsprechen in boolescher Logik **ODER**-Anweisungen. So können Sie **ODER**-Kriterien mit **UND**-Kriterien unter der Hauptebene schachteln. Elemente müssen allen Regeln im Regelsatz **Trifft auf alle zu** und mindestens einem Kriterium im Regelsatz **Trifft auf eines zu** entsprechen, um in den Bericht aufgenommen zu werden.

f. Klicken Sie neben dem Regelsatz auf **Speichern**.

g. Fügen Sie nach Bedarf weitere Regeln und Regeluntergruppen hinzu.

12. Klicken Sie auf **Speichern**.

Die Seite *Berichte* wird mit dem neuen Bericht angezeigt. Die rechts über der Tabelle angezeigte Liste *Anzeigen nach* wird automatisch auf die Kategorie des neuen Berichts eingestellt.

13. Klicken Sie auf ein Format in der Spalte *Bericht generieren*, um den Bericht auszuführen.

Die Ausgabe wird generiert. Bei HTML-Berichten wird die erste Datenspalte automatisch mit der Detailseite für dieses Element auf der **Administratorkonsole** verknüpft.

TIPP: Diagramme und Grafiken können nicht direkt aus dem Berichterstellungstool der Appliance erstellt werden. Um Diagramme und Grafiken zu erstellen, erstellen Sie einen Bericht im **XLS**-Format (Microsoft Excel) oder **CSV**-Format und importieren anschließend die Daten in ein Tool, das die Erstellung von Diagrammen und Grafiken unterstützt, beispielsweise Microsoft Excel.

Berichte mithilfe von SQL-Abfragen erstellen

Sie können Berichte erstellen, indem Sie SQL-Abfragen auf den Berichtsformular eingeben.

Wenn Sie nicht wissen, welche SQL-Abfragen Sie verwenden sollen, ist es sinnvoll, den Berichts-Assistenten zu verwenden. Siehe Berichte mit dem Berichts-Assistenten erstellen.

1. Führen Sie eine der folgenden Aktionen aus, um die Liste *Berichte* aufzurufen:

- **Wenn für Ihre Appliance die Organisationskomponente aktiviert ist, können Sie folgendermaßen auf einen Bericht auf Systemebene zugreifen:**

  Melden Sie sich bei der Systemadministratorkonsole der Appliance an: `https://`**appliance_hostname**`/system`. Oder wählen Sie in der Dropdown-Liste rechts oben auf der Seite den Eintrag **System** aus. Klicken Sie anschließend auf **Berichterstellung**.
  Berichte auf Systemebene enthalten konsolidierte Berichte, die Informationen von allen Organisationen zusammenfassen, sowie Standardberichte für verschiedene Appliance-Komponenten.

- **Wenn die Organisationskomponente nicht für die Appliance aktiviert ist oder Sie auf einen Bericht auf Organisationsebene zugreifen möchten, melden Sie sich bei der Administratorkonsole der Appliance an: `https://appliance_hostname/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option** *Organisationsmenü in Verwaltungskopfzeile anzeigen* **aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus. Klicken Sie anschließend auf Berichterstellung.**

  Berichte auf Organisationsebene enthalten Standardberichte für verschiedene Appliance-Komponenten. Wenn für Ihre Appliance die Organisationskomponente aktiviert ist, liefern diese Berichte Informationen speziell für die ausgewählte Organisation.

Die Liste *Berichte* wird angezeigt.

2. Wählen Sie **Aktion auswählen** > **Neu (SQL)**, um die *Berichtsdetailseite* anzuzeigen.
3. Geben Sie die Berichteinstellungen an:

Option	Beschreibung
Titel	Der Anzeigename des Berichts, der in der Berichtsliste angezeigt wird. Der Titel sollte möglichst aussagekräftig sein, um diesen Bericht leichter von anderen Berichten in der Liste unterscheiden zu können.
Beschreibung	Eine Beschreibung des Berichts
Kategorie	Die Kategorie des Berichts. Wenn die Kategorie noch nicht vorhanden ist, wird sie der Dropdown-Liste auf der Seite *Berichte* hinzugefügt.
Untergliederung bei Spalten	Eine durch Komma getrennte Liste mit SQL-Spaltennamen. Im Bericht werden Untergliederungsüberschriften und Zwischensummen für diese Spalten generiert.
Zeilennummern anzeigen	Zeigt auf dem Bericht eine Spalte mit Zeilennummern an.
SQL	Die Abfrageanweisung, mit der die Berichtsdaten generiert werden. Weitere Informationen finden Sie in der MySQL-Dokumentation unter http://dev.mysql.com/doc/refman/5.0/en/. Wenn Sie einen Bericht oder eine Abfrage der HD_TICKET-Tabelle des Service Desk verfassen, achten Sie darauf, dass das benutzerdefinierte Feld *Benutzer* die Benutzer-ID aus der Tabelle 'USER' in der HD_TICKET-Tabelle speichert. Letztere ist die Tabelle, die den Ticket-Datensatz enthält. Wenn Sie im Bericht den Benutzernamen anstelle der Benutzer-ID anzeigen möchten, müssen Sie der Tabelle USER beitreten. Siehe Namen von Datenbanktabellen.
Organisationseinstellungen	Diese Einstellungen sind nur auf Systemebene für Appliances mit aktivierter Organisationskomponente verfügbar. Zur Auswahl stehen folgende Optionen: • **Alle Organisationen**: Die SQL-SELECT-Anweisung wird so geändert, dass sie alle Organisationen durchläuft und der Bericht Informationen für alle Organisationen enthält. • **Ergebnisse zusammenfassen**: Die SQL-SELECT-Anweisung wird so geändert, dass sie die Datensätze aller Organisationen kombiniert und der Bericht zusammenfassende Informationen für alle Organisationen enthält. Die Standardberichte dieses Typs werden als konsolidierte Berichte kategorisiert.

4. Klicken Sie auf **Speichern**.

Die Appliance überprüft die Berichtsyntax und zeigt ggf. Fehler an.

5. Klicken Sie auf ein Format in der Spalte *Bericht generieren*, um den neuen Bericht auszuführen.

> **TIPP:** Diagramme und Grafiken können nicht direkt aus dem Berichterstellungstool der Appliance erstellt werden. Um Diagramme und Grafiken zu erstellen, erstellen Sie einen Bericht im **XLS**-Format (Microsoft Excel) oder **CSV**-Format und importieren anschließend die Daten in ein Tool, das die Erstellung von Diagrammen und Grafiken unterstützt, beispielsweise Microsoft Excel.

Berichte über Listenseiten erstellen

Sie können Berichte erstellen, während Sie Listenseiten anzeigen, wie zum Beispiel die Seite *Geräte*.

1. Rufen Sie eine Listenseite auf. Gehen Sie folgendermaßen vor, um beispielsweise die Seite *Geräte* aufzurufen:
   a. Wählen Sie ggf. rechts oben auf der Seite eine Organisation aus der Dropdown-Liste aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Inventar** und anschließend auf **Dashboard**.
2. Wählen Sie **Aktion auswählen** > **Bericht erstellen**, um die *Berichtsdetailseite* anzuzeigen.
3. Geben Sie die Berichteinstellungen an:

Option	Beschreibung
Titel	Der Anzeigename des Berichts, der in der Berichtsliste angezeigt wird. Der Titel sollte möglichst aussagekräftig sein, um diesen Bericht leichter von anderen Berichten in der Liste unterscheiden zu können.
Beschreibung	Eine Beschreibung des Berichts
Kategorie	Die Kategorie des Berichts. Wenn die Kategorie noch nicht vorhanden ist, wird sie der Dropdown-Liste auf der Seite *Berichte* hinzugefügt.
Untergliederung bei Spalten	Eine durch Komma getrennte Liste mit SQL-Spaltennamen. Im Bericht werden Untergliederungsüberschriften und Zwischensummen für diese Spalten generiert.
Zeilennummern anzeigen	Zeigt auf dem Bericht eine Spalte mit Zeilennummern an.
SQL	Die Abfrageanweisung, mit der die Berichtsdaten generiert werden. Weitere Informationen finden Sie in der MySQL-Dokumentation unter http://dev.mysql.com/doc/refman/5.0/en/. Wenn Sie einen Bericht oder eine Abfrage der HD_TICKET-Tabelle des Service Desk verfassen, achten Sie darauf, dass das benutzerdefinierte Feld *Benutzer* die Benutzer-ID aus der Tabelle 'USER' in der HD_TICKET-Tabelle speichert. Letztere ist die Tabelle, die den Ticket-Datensatz enthält. Wenn Sie im Bericht den Benutzernamen anstelle der Benutzer-ID anzeigen möchten, müssen Sie der Tabelle USER beitreten.

4. Klicken Sie auf **Speichern**.

Der Bericht wird auf der Seite *Berichte* angezeigt.

Berichte duplizieren

Sie können beliebige Berichte duplizieren, einschließlich der Standardberichte, die im Lieferumfang der Appliance enthalten sind. Wenn Sie einen Bericht erstellen, der einem vorhandenen Bericht ähnelt, kann es schneller sein, den vorhandenen Bericht zu duplizieren, als den Bericht von Grund auf neu zu erstellen.

1. Führen Sie eine der folgenden Aktionen aus, um die Liste *Berichte* aufzurufen:

   - **Wenn für Ihre Appliance die Organisationskomponente aktiviert ist, können Sie folgendermaßen auf einen Bericht auf Systemebene zugreifen:**

     Melden Sie sich bei der Systemadministratorkonsole der Appliance an: `https://`**appliance_hostname**`/system`. Oder wählen Sie in der Dropdown-Liste rechts oben auf der Seite den Eintrag **System** aus. Klicken Sie anschließend auf **Berichterstellung**.
     Berichte auf Systemebene enthalten konsolidierte Berichte, die Informationen von allen Organisationen zusammenfassen, sowie Standardberichte für verschiedene Appliance-Komponenten.

   - **Wenn die Organisationskomponente nicht für die Appliance aktiviert ist oder Sie auf einen Bericht auf Organisationsebene zugreifen möchten, melden Sie sich bei der Administratorkonsole der Appliance an: `https://appliance_hostname/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option** *Organisationsmenü in Verwaltungskopfzeile anzeigen* **aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus. Klicken Sie anschließend auf Berichterstellung.**

     Berichte auf Organisationsebene enthalten Standardberichte für verschiedene Appliance-Komponenten. Wenn für Ihre Appliance die Organisationskomponente aktiviert ist, liefern diese Berichte Informationen speziell für die ausgewählte Organisation.

   Die Liste *Berichte* wird angezeigt.
2. Klicken Sie auf den Titel eines Berichts.

   Je nach Art des Berichts wird entweder die Seite *Berichtsdetail* oder die erste Seite des Berichts-Assistenten angezeigt.
3. Klicken Sie unten auf der Seite auf **Duplizieren**.

   Je nach Art des Berichts wird entweder die Seite *Berichtsdetail* oder die erste Seite des Berichts-Assistenten angezeigt.
4. Ändern Sie Berichtdetails nach Bedarf und klicken Sie dann auf **Speichern**.

SQL-SELECT-Anweisungen in mit dem Berichts-Assistenten erstellten Berichten bearbeiten

Sie können die SQL-Anweisungen für vom Assistenten erstellte Berichte mit einem Einzelthema ändern.

Dies ist nützlich, wenn Sie SQL-Anweisungen ändern oder in einen neuen Bericht kopieren möchten. Die Option zum Bearbeiten steht nicht für Berichte mit mehreren Themen zur Verfügung.

1. Führen Sie eine der folgenden Aktionen aus, um die Liste *Berichte* aufzurufen:

   - **Wenn für Ihre Appliance die Organisationskomponente aktiviert ist, können Sie folgendermaßen auf einen Bericht auf Systemebene zugreifen:**

     Melden Sie sich bei der Systemadministratorkonsole der Appliance an: `https://`**appliance_hostname**`/system`. Oder wählen Sie in der Dropdown-Liste rechts oben auf der Seite den Eintrag **System** aus. Klicken Sie anschließend auf **Berichterstellung**.

Berichte auf Systemebene enthalten konsolidierte Berichte, die Informationen von allen Organisationen zusammenfassen, sowie Standardberichte für verschiedene Appliance-Komponenten.

- **Wenn die Organisationskomponente nicht für die Appliance aktiviert ist oder Sie auf einen Bericht auf Organisationsebene zugreifen möchten, melden Sie sich bei der Administratorkonsole der Appliance an: `https://appliance_hostname/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option** *Organisationsmenü in Verwaltungskopfzeile anzeigen* **aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus. Klicken Sie anschließend auf Berichterstellung.**

  Berichte auf Organisationsebene enthalten Standardberichte für verschiedene Appliance-Komponenten. Wenn für Ihre Appliance die Organisationskomponente aktiviert ist, liefern diese Berichte Informationen speziell für die ausgewählte Organisation.

Die Liste *Berichte* wird angezeigt.

2. Klicken Sie auf den Titel eines vom Assistenten erstellten Berichts mit einem Einzelthema.

   Der Berichts-Assistent wird angezeigt.
3. Klicken Sie am unteren Rand des Formulars auf **SQL bearbeiten**, um die *Berichtsdetailseite* anzuzeigen.
4. Bearbeiten oder kopieren Sie den Text im Feld *SQL* nach Bedarf und klicken Sie dann auf **Speichern**.

> **HINWEIS:** Beim Kopieren einer SQL-Anweisung zwischen verschiedenen Arten von Berichten müssen Sie die SQL-Anweisung vor dem Verwenden ggf. anpassen. Wenn Sie beispielsweise die SQL-Anweisung aus einem Anwendungs-Compliance-Bericht kopieren und in einen Bericht einfügen, für den die Option *Ergebnisse zusammenfassen* für Organisationen ausgewählt ist, meldet die Appliance Fehler in der SQL-Anweisung. Sie können den Bericht erst speichern, wenn die Fehler behoben wurden.

Berichte aus Verlaufslisten erstellen

Sie können Berichte von jeder Verlaufsliste aus erstellen.

1. Rufen Sie die Verlaufsliste für Einstellungen, Assets oder Objekte auf.
   - Asset-Verlauf anzeigen
   - Objektverlauf anzeigen
   - Einstellungsverlauf anzeigen
2. Wählen Sie **Aktion auswählen** > **Bericht erstellen**.

   Die Seite *Berichtsdetail* wird angezeigt. Siehe Berichte über Listenseiten erstellen.

Ändern von Berichten

Sie können Berichte nach Bedarf bearbeiten oder löschen.

Berichte bearbeiten

Sie können beliebige benutzerdefinierte Berichte bearbeiten. Standardberichte, die zum Lieferumfang der Appliance gehören, können jedoch nicht bearbeitet werden.

Wenn Sie einen Standardbericht bearbeiten möchten, duplizieren Sie ihn zunächst und bearbeiten ihn dann. Siehe Berichte duplizieren.

1. Führen Sie einen der folgenden Schritte aus:
   - **Wählen Sie ggf. rechts oben auf der Seite aus der Dropdown-Liste eine Organisation aus, um Berichte auf Organisationsebene zu bearbeiten, und klicken Sie dann auf Berichterstellung.**
   - **Zum Bearbeiten von Berichten auf Systemebene melden Sie sich bei der Systemadministratorkonsole unter `http://appliance_hostname/system` an, oder wählen Sie rechts oben auf der Seite aus der Dropdown-Liste die Option System aus. Klicken Sie anschließend auf Berichterstellung (nur für Appliances mit aktivierter Organisationskomponente).**

   Die Seite *Berichte* wird angezeigt.
2. Klicken Sie auf den Titel eines Berichts, um die *Berichtsdetailseite* anzuzeigen.

Berichte löschen

Sie können beliebige benutzerdefinierte Berichte löschen. Standardberichte, die zum Lieferumfang der Appliance gehören, können nicht gelöscht werden.

1. Führen Sie einen der folgenden Schritte aus:
   - **Wählen Sie ggf. rechts oben auf der Seite aus der Dropdown-Liste eine Organisation aus, um Berichte auf Organisationsebene zu löschen, und klicken Sie dann auf Berichterstellung.**
   - **Zum Löschen von Berichten auf Systemebene melden Sie sich bei der Systemadministratorkonsole unter `http://appliance_hostname/system` an, oder wählen Sie rechts oben auf der Seite aus der Dropdown-Liste die Option System aus. Klicken Sie anschließend auf Berichterstellung (nur für Appliances mit aktivierter Organisationskomponente).**

   Die Seite *Berichte* wird angezeigt.
2. Aktivieren Sie das Kontrollkästchen neben einem oder mehreren Berichten.
3. Wählen Sie **Aktion auswählen > Löschen** und klicken Sie dann zum Bestätigen auf **Ja**.

Anpassen von Logos für Berichte

Das standardmäßig in Berichten verwendete Quest Logo kann durch ein eigenes Logo ersetzt werden.

Informationen zum Hochladen Ihres eigenen Logos finden Sie in den Abschnitten *Logo-Überschreibungen* unter:

- Allgemeine Appliance-Einstellungen bei aktivierter Organisationskomponente konfigurieren
- Allgemeine Appliance-Einstellungen ohne aktivierte Organisationskomponente konfigurieren

Planen von Berichten und Benachrichtigungen

Sie können Berichte und Benachrichtigungen planen, um die Aktivitäten auf Ihrer Appliance zu überwachen.

Ausführen von Berichten für Einzelorganisationen sowie von konsolidierten Berichten

Wenn die Organisationskomponente auf Ihrer Appliance aktiviert ist und Sie über mehrere Organisationen verfügen, können Sie Berichte für Einzelorganisationen für die einzelnen Organisationen getrennt ausführen.

Zusätzlich können Sie auch konsolidierte Berichte ausführen, die Informationen für alle Organisationen in einem einzigen Bericht zusammenfassen.

Berichte für Einzelorganisationen ausführen

Berichte für Einzelorganisationen zeigen Informationen für eine bestimmte Organisation an.

Falls die Organisationskomponente auf Ihrer Appliance nicht aktiviert ist oder wenn Sie nur über eine Einzelorganisation verfügen, liefern diese Berichte Informationen über die Standardorganisation.

1. Rufen Sie die Liste *Berichte* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Berichterstellung** und anschließend auf **Berichte**.
2. Klicken Sie in der Spalte *Bericht generieren* auf einen Formattyp für den Bericht.

   HTML-Berichte werden in einem neuen Fenster angezeigt. Bei anderen Formaten können Sie die Datei öffnen oder auf dem Gerät speichern.

   HINWEIS: Diagramme und Grafiken können nicht direkt aus dem Berichterstellungstool der Appliance erstellt werden. Um Diagramme und Grafiken zu erstellen, erstellen Sie einen Bericht im **XLS**-Format (Microsoft Excel) oder **CSV**-Format und importieren anschließend die Daten in ein Tool, das die Erstellung von Diagrammen und Grafiken unterstützt, beispielsweise Microsoft Excel.

   HINWEIS: Beachten Sie, dass Multibytezeichen, die beispielsweise für die Unterstützung japanischer oder chinesischer Zeichensätze verwendet werden, möglicherweise als unlesbare Zeichen angezeigt werden, wenn CSV-Dateien in Excel importiert werden. Weitere Informationen erhalten Sie vom **Quest Support** unter https://support.quest.com/contact-support.

Konsolidierte Berichte für Organisationen ausführen

Wenn die Organisationskomponente auf Ihrer Appliance aktiviert ist, können Sie konsolidierte Berichte ausführen, die Informationen für alle Organisationen in einem einzigen Bericht zusammenfassen.

1. Rufen Sie die Liste *Berichte* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Berichterstellung** und anschließend auf **Berichte**.
2. Klicken Sie in der Spalte *Bericht generieren* auf einen Formattyp für den Bericht.

   HTML-Berichte werden in einem neuen Fenster angezeigt. Bei anderen Formaten können Sie die Datei öffnen oder auf dem Gerät speichern.

HINWEIS: Diagramme und Grafiken können nicht direkt aus dem Berichterstellungstool der Appliance erstellt werden. Um Diagramme und Grafiken zu erstellen, erstellen Sie einen Bericht im **XLS**-Format (Microsoft Excel) oder **CSV**-Format und importieren anschließend die Daten in ein Tool, das die Erstellung von Diagrammen und Grafiken unterstützt, beispielsweise Microsoft Excel.

HINWEIS: Beachten Sie, dass Multibytezeichen, die beispielsweise für die Unterstützung japanischer oder chinesischer Zeichensätze verwendet werden, möglicherweise als unlesbare Zeichen angezeigt werden, wenn CSV-Dateien in Excel importiert werden. Weitere Informationen erhalten Sie vom **Quest Support** unter https://support.quest.com/contact-support.

Planen von Berichten

Zur Überwachung Ihrer Umgebung können Sie auf der Appliance einen Zeitplan einrichten, nach dem Berichte zu bestimmten Zeiten und in bestimmten Intervallen ausgeführt und an Administratoren gesendet werden. Dies ist nützlich, um Software, Geräte und den Zustand des Systems nachzuverfolgen.

Zeitpläne für Berichte hinzufügen

Sie können Berichtszeitpläne hinzufügen, damit die Appliance Berichte zu bestimmten Zeiten automatisch ausführen kann. Dies ist bei regelmäßig zu erstellenden Berichten hilfreich, z. B. bei Berichten zur Softwarelizenz-Compliance.

1. Führen Sie einen der folgenden Schritte aus:
   - **Wählen Sie ggf. rechts oben auf der Seite aus der Dropdown-Liste eine Organisation aus, um Berichte auf Organisationsebene zu planen, und klicken Sie dann auf Berichterstellung.**
   - **Zum Planen von Berichten auf Systemebene melden Sie sich bei der Systemadministratorkonsole unter `http://appliance_hostname/system` an, oder wählen Sie rechts oben auf der Seite aus der Dropdown-Liste die Option System aus. Klicken Sie anschließend auf Berichterstellung (nur für Appliances mit aktivierter Organisationskomponente).**

   Die Seite *Berichte* wird angezeigt.
2. Führen Sie einen der folgenden Schritte aus:
   - **Klicken Sie neben einem Bericht auf die Schaltfläche Zeitplan. .**
   - **Klicken Sie auf der linken Navigationsleiste auf Berichtszeitpläne und wählen Sie anschließend Aktion auswählen > Neu, um die *Detailseite für den Berichtszeitplan* anzuzeigen.**
3. Geben Sie die folgenden Einstellungen an:

Option	Beschreibung
Name	Der Anzeigename des Zeitplans. Der Name sollte möglichst aussagekräftig sein, um diesen Zeitplan leichter von anderen Zeitplänen unterscheiden zu können.
Bericht	Der Name des Berichts, den Sie planen. Der Name wird automatisch generiert, wenn Sie auf der Seite *Berichte* auf die Schaltfläche **Zeitplan** neben einem Bericht klicken.
Formate	Das Format des Berichts

Option	Beschreibung
Beschreibung	Eine Beschreibung des Zeitplans. Diese Beschreibung wird auf der Seite *Berichte planen* angezeigt.

4. Geben Sie im Abschnitt *Benachrichtigen* folgende Einstellungen an:

Option	Beschreibung
Betreff	Die Betreff-Zeile der E-Mail-Nachricht, die den Bericht enthält.
Empfänger	Die E-Mail-Adressen, an die der Bericht gesendet werden soll. Trennen Sie mehrere Adressen durch Kommata.
Keine leeren Berichte senden	Legt fest, ob der Bericht immer gesendet werden soll oder nur dann, wenn Ergebnisse gefunden wurden. Mit dieser Option verhindern Sie, dass die Appliance den Bericht auch dann verschickt, wenn dieser leer ist.
Meldung	Jegliche Informationen, die Sie im Nachrichtentext übermitteln möchten.
Optionen für Anhänge	Das Format des Berichts. Wählen Sie **Anhang**, um die Datei an die E-Mail-Nachricht anzuhängen, oder wählen Sie **ZIP-Anhang**, um die Datei als ZIP-Archiv anzuhängen.

5. Geben Sie im Abschnitt *Zeitplan* folgende Einstellungen an:

Option	Beschreibung
Kein(e)	Die Ausführung erfolgt im Zusammenhang mit einem Ereignis anstatt zu einem bestimmten Datum oder zu einem bestimmten Zeitpunkt.
jede Stunde	Der Vorgang wird im angegebenen Intervall durchgeführt.
Täglich/an einem bestimmten Tag um HH:MM	Die Erfassung wird täglich zu einem bestimmten Zeitpunkt oder an einem bestimmten Wochentag um eine bestimmte Uhrzeit ausgeführt.
Ausführen am n-ten jedes Monats/eines bestimmten Monats um HH:MM	Die Erfassung wird jeden Monat oder in einem bestimmten Monat an einem festgelegten Datum zu einer festgelegten Uhrzeit ausgeführt.
Ausführen am n-ten Wochentag **jedes Monats/ eines bestimmten Monats um HH:MM**	Die Erfassung wird jeden Monat oder in einem bestimmten Monat an einem festgelegten Wochentag zu einer festgelegten Uhrzeit ausgeführt.
Benutzerdefiniert	Führen Sie die Erfassung nach einem benutzerdefinierten Zeitplan aus.

Option	Beschreibung

	Verwenden Sie das Standard-5-Feld-Cron-Format (das erweiterte Cron-Format wird nicht unterstützt):
	`* * * * *`
	`| | | | +————————Wochentag (0-6) (Sonntag=0)`
	`| | | +————————Monat (1-12)`
	`| | +————————Monatstag (1-31)`
	`| +————————Stunde (0-23)`
	`+————————Minute (0-59)`
	Verwenden Sie bei der Angabe von Werten die folgenden Zeichen:
	• **Leerzeichen( )**: Die einzelnen Felder mit einem Leerzeichen trennen.
	• **Sternchen (*)**: Ein Sternchen repräsentiert den gesamten Wertebereich in einem Feld. Zum Beispiel repräsentiert ein Sternchen im Stundenfeld eine beliebige Stunde.
	• **Kommas (,)**: Mehrere Werte in einem Feld werden mit einem Komma getrennt. Zum Beispiel werden mit `0,6` im Feld „Wochentag“ Sonntag und Samstag angegeben.
	• **Bindestriche (-)**: Mit einem Bindestrich wird ein Wertebereich in einem Feld angegeben. Zum Beispiel entspricht `1-5` im Feld „Wochentag“ `1,2,3,4,5`, d. h. Montag bis Freitag.
	• **Schrägstriche (/)**: Die Angabe der Zeitabstände, mit denen eine Aktion wiederholt werden soll, erfolgt mit einem Schrägstrich. Zum Beispiel entspricht `*/3` im Feld Stunde `0,3,6,9,12,15,18,21`. Das Sternchen (`*`) gibt jede Stunde an, mit `/3` erfolgt aber eine Einschränkung auf durch drei teilbare Stunden.
	Beispiele:
	• `15 * * * *` Jeden Tag 15 Minuten nach jeder vollen Stunde ausführen
	• `0 22 * * *` Jeden Tag um 22:00 Uhr ausführen
	• `0 0 1 1,6 *` Am 1. Januar und 1. Juni um 00:00 Uhr ausführen
	• `30 8,12 * * 1-5` An Wochentagen um 08:30 Uhr und 12:30 Uhr ausführen
	• `0 2 */2 * *` Jeden zweiten Tag um 02:00 Uhr ausführen

Aufgabenplan anzeigen	Klicken Sie, um den Aufgabenplan anzuzeigen. Im Dialogfeld *Aufgabenplan* wird eine Liste der geplanten Aufgaben angezeigt. Klicken Sie auf eine Aufgabe, um die Aufgabendetails anzuzeigen.

Option	Beschreibung
	Weitere Informationen hierzu finden Sie unter Aufgabenpläne anzeigen.

6. Klicken Sie auf **Speichern**.

Berichtszeitpläne löschen

Berichtszeitpläne ermöglichen es der Appliance, Berichte zu bestimmten Zeiten und in bestimmten Intervallen auszuführen. Wenn Sie Berichtszeitpläne löschen, werden sowohl die Berichtskriterien als auch die Zeitplaneinstellungen aus der Appliance entfernt.

Berichtszeitpläne können jederzeit nach Bedarf gelöscht werden.

1. Führen Sie einen der folgenden Schritte aus:
   - **Wählen Sie ggf. rechts oben auf der Seite aus der Dropdown-Liste eine Organisation aus, um einen Zeitplan für das Ausführen von Berichten auf Organisationsebene zu löschen, und klicken Sie dann auf Berichterstellung.**
   - **Zum Löschen von Berichtszeitplänen auf Systemebene melden Sie sich bei der Systemadministratorkonsole unter `http://appliance_hostname/system` an, oder wählen Sie rechts oben auf der Seite aus der Dropdown-Liste die Option System aus. Klicken Sie anschließend auf Berichterstellung (nur für Appliances mit aktivierter Organisationskomponente).**

   Die Seite *Berichte* wird angezeigt.
2. Klicken Sie auf der linken Navigationsleiste auf **Berichtszeitpläne**, um die Seite *Berichtszeitpläne* anzuzeigen.
3. Aktivieren Sie das Kontrollkästchen neben einem oder mehreren Berichtszeitplänen.
4. Wählen Sie **Aktion auswählen** > **Löschen** und klicken Sie dann zum Bestätigen auf **Ja**.

Zeitplanung für Benachrichtigungen

Zur Überwachung Ihrer Umgebung können Sie die Appliance so konfigurieren, dass Administratoren bei Erfüllung bestimmter Kriterien per E-Mail informiert werden. Dies ist hilfreich bei der Überwachung des Systemzustands und der Geräteeigenschaften.

Sie können Benachrichtigungszeitpläne nach Bedarf hinzufügen, bearbeiten und löschen.

Benachrichtigungszeitpläne über den Bereich "Berichterstellung" hinzufügen

Sie können Benachrichtigungszeitpläne für Geräte, Erkennungsscans und Assets im Bereich *Berichterstellung* hinzufügen.

1. Rufen Sie die Listenseite *Benachrichtigungszeitpläne* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.

b. Klicken Sie in der linken Navigationsleiste auf **Berichterstellung** und anschließend auf **Benachrichtigungen**.

2. Wählen Sie unter **Aktion auswählen** eine der folgenden Aktionen aus:
   - **Neu > Gerätebenachrichtigung**
   - **Neu > Erkennungsbenachrichtigung**
   - **Neu > Asset-Benachrichtigung**
   - **Neu > Benachrichtigung über Überwachungswarnungen**

   Der Bereich *Benachrichtigung* wird angezeigt.

3. Wählen Sie Benachrichtigungskriterien aus. Gehen Sie beispielsweise folgendermaßen vor, um eine Benachrichtigung zu senden, wenn Geräte unter Windows 7 seit 24 Stunden keine Verbindung mit der Appliance hergestellt haben:

   a. Legen Sie die erforderlichen Kriterien für die Suche nach Geräte fest, auf denen das Betriebssystem Windows 7 installiert ist:

   ```
   Betriebssystem: Name des Betriebssystems | hat | Windows 7
   ```

   b. Wählen Sie in der Dropdown-Liste für Operatoren **UND** aus und klicken Sie auf **Zeile hinzufügen**.

   c. Legen Sie die erforderlichen Kriterien fest, um Geräte zu finden, die in den letzten 24 Stunden keine Verbindung zur Appliance hergestellt haben:

   ```
   Identitätsinformationen des Geräts: Zeitpunkt der letzten Synchronisierung
   | > | 24 Stunden
   ```

4. Geben Sie die folgenden Informationen unterhalb der Benachrichtigungskriterien ein.

Feld	Beschreibung
Titel	Die Informationen, die in der *Betreff*-Zeile der E-Mail-Benachrichtigung stehen sollen. Diese werden auch als Name der Benachrichtigung auf der Seite *Benachrichtigungszeitpläne* angezeigt.
Empfänger	Die E-Mail-Adresse oder -Adressen der gewünschten Empfänger. Es müssen vollständige, gültige E-Mail-Adressen verwendet werden. Um E-Mails an mehrere Adressen zu senden, trennen Sie die Adressen durch Kommas oder verwenden E-Mail-Verteiler.
Häufigkeit	Das Intervall, in dem die Appliance die Abfrage ausführt, um die gewählten Kriterien mit Elementen im Inventar zu vergleichen. Werden Kriterien erfüllt, wird eine Benachrichtigung gesendet.

5. **Optional**: Klicken Sie auf **Testen**, um die Kriterien zu überprüfen.

Die Liste wird aktualisiert, damit nur die Elemente angezeigt werden, die den festgelegten Kriterien entsprechen. Es werden keine Benachrichtigungen während des Tests versendet.

6. Klicken Sie auf **Speichern**.

Die Benachrichtigung wird erstellt und auf der Seite *Benachrichtigungszeitpläne* angezeigt. Weitere Informationen zum Planen der Benachrichtigungshäufigkeit finden Sie unter Benachrichtigungszeitpläne bearbeiten.

Benachrichtigungszeitpläne über Listenseiten hinzufügen

Sie können Benachrichtigungszeitpläne von Listenseiten hinzufügen, beispielsweise von der Seite *Geräte*, *Software*, *Softwarekatalog*, *Erkennung* oder *Assets*.

1. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
2. Rufen Sie eine Listenseite auf, z. B. die Liste *Geräte*, und klicken Sie oberhalb der Liste rechts auf die Registerkarte **Benachrichtigung**.

   Der Bereich *Benachrichtigung* wird angezeigt.

3. Geben Sie die Kriterien an, die für den Benachrichtigungszeitplan verwendet werden sollen.

   Siehe Beispiel: Nach verwalteten Geräten mithilfe der Kriterien der Erweiterten Suche suchen.

4. Geben Sie die folgenden Informationen unterhalb der Benachrichtigungskriterien ein.

Feld	Beschreibung
Titel	Die Informationen, die in der *Betreff*-Zeile der E-Mail-Benachrichtigung stehen sollen. Der Titel wird auch als Name der Benachrichtigung auf der Seite *Benachrichtigungszeitpläne* angezeigt.
Empfänger	Die E-Mail-Adresse oder -Adressen der gewünschten Empfänger. Es müssen vollständige, gültige E-Mail-Adressen verwendet werden. Um E-Mails an mehrere Adressen zu senden, trennen Sie die Adressen durch Kommas oder verwenden E-Mail-Verteiler.
Häufigkeit	Das Intervall, in dem die Appliance die Abfrage ausführt, um die gewählten Kriterien mit Elementen im Inventar zu vergleichen. Werden Kriterien erfüllt, wird eine Benachrichtigung gesendet.

5. **Optional**: Klicken Sie auf **Testen**, um die Kriterien zu überprüfen.

   Die Liste wird aktualisiert, damit nur die Elemente angezeigt werden, die den festgelegten Kriterien entsprechen. Es werden keine Benachrichtigungen während des Tests versendet.

6. Klicken Sie auf **Speichern**.

Die Benachrichtigung wird erstellt und auf der Seite *Benachrichtigungszeitpläne* angezeigt. Benachrichtigungen sind standardmäßig aktiviert. Weitere Informationen zum Deaktivieren von Benachrichtigungen oder zum Hinzufügen einer Beschreibung zu einer Benachrichtigung finden Sie unter Benachrichtigungszeitpläne bearbeiten.

Benachrichtigungszeitpläne bearbeiten

Sie können Benachrichtigungen nach Bedarf aktivieren, deaktivieren, bearbeiten und ihre Häufigkeit ändern.

1. Rufen Sie die Listenseite *Benachrichtigungszeitpläne* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Berichterstellung** und anschließend auf **Benachrichtigungen**.
   c. Klicken Sie auf den Namen einer Benachrichtigung.
2. Ändern Sie die Eigenschaften wie gewünscht:

Feld	Beschreibung
Aktiviert	Angabe darüber, ob Benachrichtigung aktiviert ist oder nicht. Wählen Sie **Aktiviert**, um der Appliance zu gestatten, die Abfrage auszuführen und die entsprechenden Benachrichtigungen mit der gewählten Häufigkeit zu senden. Wählen Sie **Deaktiviert**, um die Appliance daran zu hindern, die Abfrage auszuführen und Benachrichtigungen zu senden.
Name	Die Informationen, die in der *Betreff*-Zeile der E-Mail-Benachrichtigung stehen sollen. Wenn Sie Benachrichtigungen im Bereich *Benachrichtigung* erstellen, geben Sie diese Informationen im Feld *Titel* ein.
Empfänger	Die E-Mail-Adresse oder -Adressen der gewünschten Empfänger. Es müssen vollständige, gültige E-Mail-Adressen verwendet werden. Um E-Mails an mehrere Adressen zu senden, trennen Sie die Adressen durch Kommas oder verwenden E-Mail-Verteiler.
Beschreibung	Geben Sie nach Bedarf beliebige weitere Informationen ein.
Häufigkeit	Das Intervall, in dem die Appliance die Abfrage ausführt, um die gewählten Kriterien mit Elementen

Feld	Beschreibung
	im Inventar zu vergleichen. Werden Kriterien erfüllt, wird eine Benachrichtigung gesendet.

3. **Optional**: Um den Bericht mithilfe des Assistenten zu bearbeiten, klicken Sie oberhalb der Schaltfläche **Speichern** neben *Um die Benachrichtigung erneut mit dem ursprünglichen Editor zu bearbeiten* auf **hier klicken**.
4. **Optional**: Um die SQL-Kriterien zu ändern, die eine Benachrichtigung auslösen, aktivieren Sie oberhalb der Schaltfläche **Speichern** das Kontrollkästchen *Um die Benachrichtigung erneut mit diesem Editor zu bearbeiten*.

   Achten Sie bei Bearbeitung der SQL-Abfrage unbedingt darauf, die folgenden Anweisungen vom Typ `as` zu verwenden:

   ```
   MACHINE.NAME AS SYSTEM_NAME
   ```

   ```
   MACHINE.ID as TOPIC_ID
   ```

   Beispiel:

   ```
   SELECT MACHINE.NAME AS SYSTEM_NAME, SYSTEM_DESCRIPTION, MACHINE.IP,
   MACHINE.MAC, MACHINE.ID as TOPIC_ID FROM MACHINE WHERE ((SYSTEM_DESCRIPTION =
   'Test Computer'))
   ```

5. Klicken Sie auf **Speichern**.

Benachrichtigungszeitpläne löschen

Wenn Sie Benachrichtigungszeitpläne löschen, werden sowohl die Benachrichtigungskriterien als auch die Zeitplaneinstellungen aus der Appliance entfernt.

Benachrichtigungszeitpläne können jederzeit nach Bedarf gelöscht werden.

1. Rufen Sie die Listenseite *Benachrichtigungszeitpläne* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Berichterstellung** und anschließend auf **Benachrichtigungen**.
2. Aktivieren Sie das Kontrollkästchen neben einem oder mehreren Benachrichtigungszeitplänen.
3. Wählen Sie **Aktion auswählen > Löschen** und klicken Sie dann zum Bestätigen auf **Ja**.

Überwachen von Servern

Die Appliance bietet Ihnen ein Modul, mit dem Sie eine grundlegende Leistungsüberwachung für die Server im Inventar ausführen können.

Informationen zur Serverüberwachung

Die Überwachungsfunktion der Appliance ist für Serverbetriebssysteme konzipiert und bietet standardmäßige Überwachungsprofile, die Kriterien für Leistungswarnungen für jedes Betriebssystem definieren. Sie können weitere benutzerdefinierte Profile mit ähnlichen oder anderen Kriterien definieren, die auf alternative Ereignisprotokolle oder Protokolle auf Betriebssystemebene verweisen.

HINWEIS: Die Serverüberwachung wird für Raspberry Pi-Geräte mit Raspbian Linux BS nicht unterstützt.

Details zu BS-Versionen, die für Serverüberwachung unterstützt werden, finden Sie in den Anleitungen mit den **technischen Daten**.

HINWEIS: Damit die agentenbasierte Überwachung auf einem RHEL-Gerät mit Security-Enhanced Linux (SELinux) funktioniert, muss SELinux entweder deaktiviert sein oder im „Permissive Mode“ ausgeführt werden. Sie können den SELinux Modus durch Bearbeiten der Datei `/etc/selinux/config` und Neustarten des Geräts ändern. Weitere Informationen zum Aktivieren oder Deaktivieren von SELinux unter Red Hat Enterprise Linux finden Sie unter https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/6/html/Security-Enhanced_Linux/sect-Security-Enhanced_Linux-Working_with_SELinux-Enabling_and_Disabling_SELinux.html.

Komponenten der Überwachungsoberfläche auf der Registerkarte "Überwachung" der Appliance-Navigationsleiste

Abschnitt	Beschreibung
Geräte	Zeigt für jedes überwachte Gerät die kritischste Warnung, die Warnungsanzahl, die Anzahl an das Gerät gebundener Profile und Wartungsfenster sowie einen Link zu einer Detailseite, auf der Konfigurationseinstellungen für das Gerät bearbeitet werden können. In diesem Abschnitt können auch die Erstellungs- und Änderungszeit der Warnung, die IP-Adresse des überwachten Geräts und der Aktivierungsstatus der Option Warnung bei Konfigurationsänderung angezeigt werden.
Warnungen	Zeigt die Warnstufe, eine Übersicht über die Warnungen, einen Link zu Warnungsdetails, Erstellungsdatum und -zeit der Warnung, die Uhrzeit der letzten Wiederholung, die Anzahl der Wiederholungen, die IP-Adresse und den Status.
Profile	Zeigt den Profilnamen, eine Liste der Standardprofile und hinzugefügten Profile, die Anzahl von Geräten, an die das Profil gebunden ist, und ob das Profil einem Gerät mit einem bestimmten Betriebssystemtyp automatisch hinzugefügt wird.

Abschnitt	Beschreibung
	Die Kriterien für das Auslösen einer Warnung werden in einem Profil konfiguriert. Im Profil werden Protokollpfad und -datei, der Suchtext für die Suche im Protokoll sowie der zugewiesene Schweregrad der Warnung definiert. Sie können mehrere Profile an ein Gerät binden, wenn Sie mehrere Protokolle überwachen möchten.
Wartungsfenster	Zeigt den Namen des Wartungsfensters, die Anzahl von Geräten, an die das Wartungsfenster gebunden ist, ob das Wartungsfenster allen Geräten automatisch hinzugefügt wird und einen Link zu einer Detailseite, auf der der Zeitplan und Standardeinstellungen für das Betriebssystem bearbeitet werden können. In diesem Abschnitt können auch eine Beschreibung sowie die Erstellungs- und Änderungszeit des Wartungsfensters angezeigt werden.
Log Enablement Packages	Zeigt Basisvorlagen für die Zuverlässigkeitsanalyse von Windows und den Systemmonitor (PerfMon) sowie Open-Source-Perl-Skripte für Fremdsysteme (nicht Windows) an, mit deren Hilfe Sie Überwachungsfunktionen erweitern und Probleme mit der System- und Anwendungsleistung ermitteln können.

Überwachungsprofile

Mithilfe der standardmäßigen und benutzerdefinierten Überwachungsprofile kann Ihre Appliance folgende Funktionen bereitstellen:

- Überwachung von Windows Ereignisprotokollen
- Überwachung von Dateisystemprotokollen aus Fremdsystemen (Nicht-Windows)
- Überwachung von Konfigurationsänderungen

Darüber hinaus können Sie Protokollaktivierungspakete (Log Enablement Packages, LEPs) verwenden, um Folgendes bereitzustellen:

- Schwellenwertüberwachung
- Anwendungsüberwachung

Sie können Ihre Profile herunterladen, damit andere sie verwenden können, und benutzerdefinierte Profile hochladen, die von anderen entwickelt und verfügbar gemacht wurden.

Kostenlose oder lizenzierte Serverüberwachung

Im Lieferumfang der Appliance ist mit der Standardlizenz eine Überwachungsfunktion für bis zu fünf Server enthalten. Sie können diese Serveranzahl bei Bedarf mit einer zusätzlichen Lizenz erweitern. Um anzuzeigen, wie viele Geräte unter Ihrer Lizenz verwaltet werden können, klicken Sie im Seitenhilfebereich, der durch Klicken auf **Hilfe** in der oberen rechten Ecke der Seite verfügbar ist, auf **Informationen zur Appliance**. In der Zeile für die *Verwaltungskapazitätsauslastung* werden die *überwachten Server* angezeigt. Sie enthält einen Vergleich der Anzahl von Geräten, für die die Überwachung gegenwärtig aktiviert ist, und der Gesamtanzahl von Geräten, die mit der vorhandenen Lizenz überwacht werden können.

Arbeiten mit Warnungen

Warnungen werden in der **Administratorkonsole** angezeigt, wo sie überprüft und nach dem Beheben des Problems verworfen werden können. Die Appliance bietet zudem weitere Funktionen. Beispielsweise können Sie:

- Durch bestimmte Warnungen E-Mail-Benachrichtigungen auslösen
- Direkt aus einer Warnung ein Dienstticket erstellen
- Warnungen an ein Mobilgerät senden, auf dem die KACE GO-App verwendet wird

Die Appliance bietet verschiedene Funktionen für die effiziente Verarbeitung von Warnungen:

- **Warnungskonsolidierung (Wiederholungsanzahl)**: Die Appliance analysiert die Warnungen auf Eindeutigkeit, um überflüssige Benachrichtigungen zu verhindern, und gibt für identische Warnungen mit einer Wiederholungsanzahl an, wie oft die Warnung generiert wurde.
- **Beschränkung der Warnungsanzahl**: Damit nicht zu viele doppelte Daten gesendet werden, beschränkt die Appliance die Datenerfassung auf 50 Warnungen pro Erfassung. Anschließend erstellt die Appliance eine allgemeine Warnung, um auf eine anormale Aktivität hinzuweisen, die die Aufmerksamkeit des Benutzers erfordert.
- **Bereinigung**: Der Benutzer kann Warnungen verwerfen (ausblenden, aber in der Datenbank belassen) oder manuell oder automatisch nach einer festgelegten Anzahl von Tagen löschen. Die Appliance beschränkt die Speicherung von Warnungen für ein Gerät jedoch automatisch auf 2000. Wenn diese Zahl erreicht ist, beginnt sie, Warnungen aus der Datenbank zu löschen.

Erste Schritte bei der Serverüberwachung

Im Lieferumfang der Appliance ist eine Überwachungsfunktion für eine festgelegte Anzahl von Servern enthalten. Für Server im Inventar können Sie die Überwachung aktivieren, sodass das Gerät ab der nächsten Inventarisierung Warnungen meldet.

HINWEIS: Ihre Produktlizenzvereinbarung berechtigt Sie zur Verwaltung einer festgelegten Anzahl von Geräten, die als verwaltete Computer, andere Geräte (keine Computer) und überwachte Geräte klassifiziert sind. Wenn Sie die Überwachung auf einem Gerät aktivieren, wird das Gerät einmal als verwalteter Computer und einmal als überwachtes Gerät gezählt.

Überwachung für Geräte aktivieren

Sie können die Überwachung für alle in Frage kommenden Server im Inventar aktivieren (entsprechend der von Ihrer Appliance-Lizenz vorgeschriebenen Anzahl an Geräten, höchstens jedoch 200 Server).

Für die Überwachung kommen Geräte mit Serverbetriebssystemen in Frage. Andere Geräte (keine Computer) und Computer ohne Serverbetriebssysteme können nicht überwacht werden.

Die Appliance bietet zwei Methoden zum Aktivieren der Überwachung.

- Überwachung für einen oder mehrere Server über die Geräte-Inventarliste aktivieren
- Überwachung für einen Server über dessen Gerätedetail-Seite aktivieren

Aktivierter Server: Ein Symbol in der Spalte *Status* auf der Seite *Gerät* des Abschnitts *Inventar* zeigt an, dass die Überwachung aktiviert ist (und ob sie aktiv ist oder angehalten wurde):

- : Die Serverüberwachung ist für dieses vom Agenten verwaltete Gerät aktiviert und aktiv.
- : Die Serverüberwachung ist für dieses vom Agenten verwaltete Gerät angehalten.
- : Die Serverüberwachung ist für dieses ohne Agent verwaltete Gerät aktiviert und aktiv.
- : Die Serverüberwachung ist für dieses ohne Agent verwaltete Gerät angehalten.

Verwandte Themen

Deaktivieren der Überwachung für ein oder mehrere Geräte

Überwachung für ein Gerät anhalten

Überwachung für einen oder mehrere Server über die Geräte-Inventarliste aktivieren

Über die Inventarliste *Geräte* können Sie können die Überwachung für einen oder mehrere Server aktivieren.

1. Rufen Sie die Inventarseite *Geräte* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Inventar** und anschließend auf **Dashboard**.
2. Aktivieren Sie die Kontrollkästchen aller Geräte, für die Sie die Überwachung aktivieren möchten.
3. Wählen Sie **Aktion auswählen** > **Überwachen aktivieren**.

   Informationen über den Erfolg oder Misserfolg der Aktion werden oben auf der Liste angezeigt und der *Status* des Gerätes ändert sich: Ein Überwachungssymbol wird angezeigt.

   Klappt die Aktivierung der Überwachung nicht, kann das daran liegen, dass das Betriebssystem des Gerätes oder der Gerätetyp nicht unterstützt wird oder dass die laut Lizenz zulässige Anzahl an überwachbaren Geräten überschritten ist.
4. **Optional**: Wählen Sie links in der Navigationsleiste **Überwachen** > **Geräte** aus. Klicken Sie dann auf den Namen eines Gerätes, um dessen Überwachungseinstellungen auf der Seite *Überwachungsdetail* dieses Gerätes zu ändern.
   - **Überwachung anhalten oder erneut aktivieren. Siehe Überwachung für ein Gerät anhalten.**
   - **Überwachung von Konfigurationsänderungen aktivieren. Siehe Warnungen bei Gerätekonfigurationsänderungen empfangen.**
   - **Überwachungsprofile hinzufügen oder ändern. Siehe Verwenden von Überwachungsprofilen.**
   - **Wartungsfenster hinzufügen. Siehe Wartungsfenster planen, während dessen keine Alarme von einem Gerät erfasst werden.**

   Bei mehreren aktivierten Geräten müssen Sie diese Schritte wiederholen.

Verwandte Themen

Überwachung für einen Server über dessen Gerätedetail-Seite aktivieren

Überwachung für einen Server über dessen Gerätedetail-Seite aktivieren

Sie können die Überwachung eines einzelnen Servers über dessen Gerätedetail-Seite aktivieren.

1. Rufen Sie die *Gerätedetailseite* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Inventar** und anschließend auf **Dashboard**.
   c. Klicken Sie auf den Namen eines Geräts.
2. Scrollen Sie nach unten und klicken Sie unter **Aktivitäten** auf *Überwachung*, um den Abschnitt zu erweitern.

   Wenn ein Gerät nicht überwacht werden kann, weil es nicht über ein Serverbetriebssystem verfügt, wird der Abschnitt *Überwachung* mit der Meldung **Betriebssystem wird derzeit von der Überwachung nicht unterstützt** angezeigt.
3. Klicken Sie auf **Überwachung aktivieren**, um die Überwachung zu starten und Details zur standardmäßigen Überwachungskonfiguration für das Gerät anzuzeigen.

   Wenn die Überwachung aktiviert ist, wird im Abschnitt *Überwachung* der Name des Überwachungsprofils angezeigt, das standardmäßig an das Gerät gebunden ist. Falls ein Standardwartungsfenster definiert wurde, wird dessen Name ebenfalls angezeigt. Auch werden bis zu zehn aktuelle Warnungen angezeigt, sofern vorhanden.
4. **Optional**: Klicken Sie auf **Überwachungsdetails bearbeiten**, um auf der Seite *Überwachungsdetail* Änderungen an der Überwachungskonfiguration des Geräts vorzunehmen.
   - **Überwachung anhalten oder erneut aktivieren. Siehe Überwachung für ein Gerät anhalten.**
   - **Überwachung von Konfigurationsänderungen aktivieren. Siehe Warnungen bei Gerätekonfigurationsänderungen empfangen.**
   - **Überwachungsprofile hinzufügen oder ändern. Siehe Verwenden von Überwachungsprofilen.**
   - **Wartungsfenster hinzufügen. Siehe Wartungsfenster planen, während dessen keine Alarme von einem Gerät erfasst werden.**

Verwandte Themen

Überwachung für Geräte aktivieren

Erwerben eines neuen Lizenzschlüssels für höhere Server-Überwachungskapazität

Um die erweiterten Überwachungsfunktionen für bis zu 200 Server nutzen zu können, müssen Sie einen neuen Lizenzschlüssel erwerben. Wenden Sie sich an das Quest Sales-Team, um den Schlüssel zu erhalten.

1. Navigieren Sie auf der Quest KACE Website zur Seite mit den *Kaufinformationen*: https://quest.com/buy.
2. Auf der Seite *Kaufinformationen* stehen Ihnen die folgenden drei Methoden zum Kontaktieren des Sales-Teams zur Auswahl:
   - **Rufen Sie die kostenlose Nummer für Ihren Standort an.**
   - **Senden Sie eine E-Mail an die E-Mail-Adresse für Ihren Standort.**
   - **Füllen Sie das** *Kontaktformular* **aus und senden Sie es.**

Geben Sie im Feld *Kommentare* an, dass Sie die Appliance bereits nutzen und Zugriff auf die Serverüberwachungsfunktion erhalten möchten.

Aktualisieren Sie die Informationen zum Lizenzschlüssel in der Appliance.

Übernehmen eines neuen Lizenzschlüssels für höhere Server-Überwachungskapazität

Sie können die Server Überwachungskapazität durch die Anwendung eines neuen Lizenzschlüssels erhöhen.

Sie haben Ihren neuen Lizenzschlüssel erhalten.

1. Rufen Sie die Seite *Einstellungen* der Appliance auf:
   - **Wenn die Organisationskomponente nicht für die Appliance aktiviert ist, melden Sie sich bei der Administratorkonsole an: `https://appliance_hostname/admin`, und wählen Sie dann Einstellungen > Systemsteuerung aus.**
   - **Wenn die Organisationskomponente für die Appliance aktiviert ist, melden Sie sich bei der Systemverwaltungskonsole der Appliance an: `https://appliance_hostname/system`. Oder wählen Sie in der Dropdown-Liste rechts oben auf der Seite den Eintrag System aus, und klicken Sie dann auf Einstellungen > Systemsteuerung.**
2. Klicken Sie auf **Appliance-Aktualisierungen**, um die Seite *Appliance-Aktualisierungen* anzuzeigen.
3. Geben Sie im Abschnitt *Informationen zur Lizenz* Ihren neuen Lizenzschlüssel ein und klicken Sie anschließend auf **Aktualisieren**.
4. Klicken Sie im Dialogfeld **Bestätigen** auf *Ja*, um das System neu zu starten.

Wenn Sie sich nach dem Neustart erneut bei der Appliance anmelden, stehen Ihnen sämtliche Funktionen zur Verfügung.

Verwenden von Überwachungsprofilen

Überwachungsprofile definieren die Kriterien für die Erzeugung einer Warnung, indem sie den im Protokoll des Geräts zu suchenden Text festlegen und diesen Text mit einer definierten Warnstufe verknüpfen.

Die Appliance enthält einen Satz von Standardprofilen für die Überwachung der Protokolle von Geräten mit unterstützten Betriebssystemen und auch für SNMP-Trap-Geräte. Darüber hinaus können Sie vorhandene Überwachungsprofile bearbeiten, eigene Profile erstellen und von anderen Benutzern erstellte Profile hochladen. Außerdem können Sie auf die standardmäßigen Log Enablement Packages (LEPs) zur Aktivierung der Anwendungs- und Schwellenwertüberwachung zugreifen.

Die verfügbaren Überwachungsprofile werden auf der Seite Überwachung *Profile* aufgelistet

TIPP: Wenn Sie nur die Protokollüberwachungsprofile in der Ecke oben rechts anzeigen wollen, klicken Sie auf **Anzeigen nach** > **Typ** > **Protokoll**. Um die Überwachungsprofile für SNMP-Trap-Geräte anzuzeigen, klicken Sie auf **Anzeigen nach** > **Typ** > **SNMP-Trap**.

Im Standardprofil für die Erzeugung von Warnungen für Mac OS X Geräte ist beispielsweise `/var/log/system.log` als das Protokoll angegeben, in dem die Überwachungsfunktion nach Text sucht, der zur Auslösung einer Warnung führt. In der folgenden Tabelle werden der standardmäßige Suchtext im Feld *Einschlusstext* und die zugeordneten Warnstufen beschrieben.

Im Protokoll gesuchter Text	Warnstufe
`critical`	**Kritisch**

Im Protokoll gesuchter Text	Warnstufe
`error`	**Fehler**
`fatal`	**Fehler**
`fail`	**Fehler**
`appliance monitor alert`	**Fehler**
`warn`	**Warnung**
`unavailable`	**Warnung**

Sie können weitere Warnungen hinzufügen, die an Ihre betrieblichen Anforderungen angepasst sind.

Für die folgenden unterstützten Betriebssysteme sind Standardprofile verfügbar:

- CentOS
- Debian
- FreeBSD
- Mac OS X
- Oracle Enterprise Linux
- Red Hat Enterprise Linux
- Solaris
- SUSE Linux
- Ubuntu
- Windows Server

Bei Geräten mit Linux Betriebssystemen gibt es je nach Version des Betriebssystems verschiedene Protokollpfade für MySQL und Apache Protokolle. Siehe Profil-Protokollpfade für MySQL und Apache.

Für agentenlose Geräte, die unter Verwendung des SNMP-Trap-Mechanismus überwacht werden, müssen Sie Trap-Nachrichtenformate und -ausdrücke zur Erfassung der spezifische Trap-Elemente angeben. Siehe SNMP-Trap-Meldungen und Warnmeldungskriterien konfigurieren.

Auf der Listenseite *Log Enablement Packages* veröffentlicht Quest Basisvorlagen für die Windows Zuverlässigkeitsanalyse und den Systemmonitor (PerfMon) sowie Open Source-Perl-Skripte für Fremdsysteme (nicht Windows), mit deren Hilfe Benutzer Überwachungsfunktionen erweitern und Probleme mit der System- und Anwendungsleistung ermitteln können. Diese Vorlagen und Skripte sind verfügbar, sodass sie nicht neu erstellt werden müssen. Die zusätzlichen Vorlagen und Skripte sind nicht erforderlich für die Überwachung in der Appliance, die damit erstellten Profile sind jedoch hilfreich für die Überwachung von Leistungsschwellenwerten.

Aus Gründen der Einfachheit ist zudem ein Standardprofil verfügbar, das verwendet werden kann, um optionale Vorlagen für die Windows Zuverlässigkeitsanalyse und den Systemmonitor (PerfMon) auf verwaltete Windows Server 2003 Geräte herunterzuladen. Siehe Geräte mit Windows Server 2003 mit einem Log Enablement Package (LEP) von ITNinja einrichten.

Profile bearbeiten

Sie können die Warnungskriterien und Protokollpfade für alle vorhandenen Profile ändern, hinzufügen oder entfernen.

Informationen dazu, wie Sie ein vorhandenes Profil als Vorlage für das Erstellen eines Profils verwenden, finden Sie unter Neue Profile basierend auf einem Standardprofil erstellen.

Um Ereignisse zu identifizieren, für die Warnungen ausgelöst werden sollen, geben Sie Zeichenfolgen oder reguläre Ausdrücke in *Einschlusstext* ein, um den entsprechenden Meldungsinhalt anzugeben. Wenn Sie beispielsweise die Zeichenfolge Physischer Speicher eingeben, wird eine Warnung für jede Meldung ausgegeben, die diese Zeichenfolge enthält.

Durch Verwendung eines regulären Ausdrucks können Sie mehrere Möglichkeiten berücksichtigen. Wenn Sie beispielsweise Warnungen für jeden Laufwerks-Mount-Punkt, bei dem Laufwerksfehler vorliegen, in der Form „Laufwerk /dev/[jeder Laufwerk-Mount-Punkt] weist Laufwerksfehler auf“ erstellen möchten, können Sie Laufwerk /dev/[a-z]{1,} weist Laufwerksfehler auf im *Einschlusstext* verwenden. Warnungen werden für alle Meldungen ausgelöst, die den Text „Laufwerk /dev/“ enthalten, gefolgt von jedem Wort beliebiger Länge, das die Zeichen a-z enthält, gefolgt von „weist Laufwerksfehler auf“.

Sie können bestimmte Ereignisse davon ausschließen, dass sie Warnungen auslösen, wenn Sie sie unnötig oder ablenkend finden. Um die Warnungen herauszufiltern, die Sie nicht erhalten möchten, geben Sie mit *Ausschlusstext* den Inhalt an, der eine ungewünschte Warnung identifiziert. Sie können mit *Ausschlusstext* ganze Kategorien von Warnungen herausfiltern oder *Ausschlusstext* in Verbindung mit *Einschlusstext* verwenden, um einen Untersatz einer Warnungskategorie zu definieren. Siehe Beispiele für Einschluss- und Ausschlusstext für Überwachungsprofile.

1. Rufen Sie die Listenseite *Profile* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Überwachung** und anschließend auf **Profile**.
2. Aktivieren Sie das Kontrollkästchen für das vorhandene Profil, das Sie bearbeiten möchten, und klicken Sie auf **Aktion auswählen** > **Bearbeiten**, um die Seite *Profildetail* anzuzeigen.
3. **Optional**: Ändern Sie den *Namen* und die *Beschreibung* des Profils, um auf die Änderungen hinzuweisen.

   HINWEIS: Wenn Sie eines der Standardprofile bearbeiten, ist es nicht möglich, Änderungen am Feld *Automatisch hinzufügen zu* vorzunehmen.
4. Nehmen Sie die erforderlichen Änderungen an den Einstellungen für die *Kriterien* vor.
   - **Ändern Sie** *Einschließen-Filter* **(nur SNMP-Traps) oder** *Einschlusstext* **(alle anderen Überwachungsprofile).**
     1. Klicken Sie in der Zeile mit dem zu ändernden Einschlusstext (oder Filter für SNMP-Traps) auf die Schaltfläche **Bearbeiten**: .
     2. Geben Sie den neuen Suchtext oder Filter ein.
   - **Optional. Ändern Sie** *Ausschließen-Filter* **(nur SNMP-Traps) oder** *Ausschlusstext* **(alle anderen Überwachungsprofile).**
     1. Klicken Sie in der Zeile mit dem zu ändernden Text (oder Filter für SNMP-Traps), um bestimmte Warnungen auszuschließen, auf die Schaltfläche **Bearbeiten**: .
     2. Geben Sie den neuen Ausschlusstext oder Ausschließen-Filter ein.
   - **Geben Sie den neuen Suchtext ein und wählen Sie ggf. in der Dropdown-Liste Groß-/Kleinschreibung beachten den Eintrag** *Ja* **aus.**
   - **Nur SNMP-Traps. Erstellen Sie jedes Mal, wenn das Gerät eine bestimmte SNMP-Warnung empfängt, ein Service Desk-Ticket.**
     - Klicken Sie in der Zeile mit einem SNMP-Einschließen- und Ausschließen-Filter (wie konfiguriert) in der Spalte *Ticket erstellen* auf **Warteschlange auswählen** und wählen Sie eine Ticket-Warteschlange aus, die Sie verwenden möchten, um ein Service Desk-Ticket zu erstellen. Das Gerät erstellt ein Service Desk-Ticket in der angegebenen Ticket-Warteschlange, wenn es eine Warnung erhält, die aus dem spezifischen Einschließen-Filter resultiert. Das mit der

Warnung verknüpfte Gerät wird im Service Desk-Ticket als ausgewählt angezeigt. Der Name und die Zusammenfassung des Ereignisses, das die SNMP-Warnung ausgelöst hat, werden in den Ticketdetails angezeigt. Weitere Informationen zu Service Desk-Tickets finden Sie unter Verwalten von Service Desk-Tickets, -Prozessen und -Berichten.

- **Ändern Sie die *Warnstufe*.**
  1. Klicken Sie in der Zeile mit der zu ändernden Warnstufe auf die Schaltfläche **Bearbeiten**: .
  2. Wählen Sie in der Dropdown-Liste *Stufe* eine der fünf Optionen aus: **Kritisch**, **Fehler**, **Warnung**, **Info** und **Wiederhergestellt**.
- **Fügen Sie ein Warnungskriterium hinzu.**
  1. Klicken Sie unter der Kategorieüberschrift *Kriterien* auf die Schaltfläche **Hinzufügen**: .
  2. Geben Sie die Ebene, Einschlusstext, Ausschlusstext (optional) und Groß-/Kleinschreibung an.

5. Klicken Sie unten auf der Seite auf **Speichern**.

HINWEIS: Mit der Schaltfläche **Auf Werkseinstellungen zurücksetzen** unten auf der Seite können Sie ein Standardprofil auf die Werkseinstellungen für das jeweilige Betriebssystem zurücksetzen.

Verwandte Themen

Herausfiltern von Warnmeldungen mit der Einschluss- und Ausschlusstext-Funktion auf der Seite "Profil-Details"

Beispiele für Einschluss- und Ausschlusstext für Überwachungsprofile

SNMP-Trap-Meldungen und Warnmeldungskriterien konfigurieren

Sie können SNMP-Trap-Meldungen und Warnmeldungskriterien auf der Seite Profile konfigurieren.

- SNMP-Trap-Überwachung auf der Appliance aktivieren. Weitere Informationen hierzu finden Sie unter Sicherheitseinstellungen für die Appliance konfigurieren
- Aktivieren der Überwachung auf Ihren SNMP-Geräten. Weitere Informationen hierzu finden Sie unter Aktivieren der Überwachung für ein oder mehrere Geräte

SNMP (Simple Network Management Protocol) ist ein Protokoll zum Überwachen von verwalteten Geräten in einem Netzwerk. Dieses Protokoll wird von Dell Open Manage und vielen Produkten von Drittanbietern unterstützt. Wenn Sie diese Funktion auf dem Gerät aktivieren und die zugehörigen Geräte ebenfalls für die Überwachung aktiviert sind, kann das Gerät SNMP-Traps von den überwachten agentenlosen Geräten die SNMP-Verbindungen verwenden wie Drucker, Projektoren und Routern empfangen.

SNMP-Traps sind Meldungen, die von Netzwerkgeräte initiiert und an den Trap-Empfänger auf dem Gerät gesendet werden. Zum Beispiel kann ein Router eine Meldung senden, wenn seine Stromversorgung ausfällt. Oder ein Drucker leitet eine Meldung weiter, wenn das Druckerpapier fehlt. Das Gerät erhält diese Traps und generiert Warnungen bei bestimmten Geräten die vordefinierten Grenzwerte erreicht werden.

Sie können SNMP-Trap-Meldungen und Warnmeldungskriterien mit der Seite *Profile Detail* konfigurieren.

Sie können bestimmte Ereignisse je nach Bedarf einbeziehen oder ausschließen.

1. Rufen Sie die Listenseite *Profile* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.

b. Klicken Sie in der linken Navigationsleiste auf **Überwachung** und anschließend auf **Profile**.

2. Führen Sie einen der folgenden Schritte aus.
   - Wählen Sie zur Erstellung eines neuen SNMP-Trap-Profils **Aktion wählen> Neu> SNMP-Trap-Profil**.
   - Um ein vorhandenes SNMP-Trap-Profile zu bearbeiten, wählen Sie es in der Liste und **Aktion wählen** > **Bearbeiten**.
   - Um ein vorhandenes SNMP-Trap-Profile zu duplizieren, wählen Sie es in der Liste und **Aktion wählen** > **Duplizieren und bearbeiten**.

   Die Seite *Profildetail* wird angezeigt.
3. **Optional**: Ändern Sie den *Namen* und die *Beschreibung* des Profils, um auf die Änderungen hinzuweisen.

   HINWEIS: Wenn Sie eines der Standardprofile bearbeiten, ist es nicht möglich, Änderungen am Feld *Automatisch hinzufügen zu* vorzunehmen.
4. Nehmen Sie die erforderlichen Änderungen an den Einstellungen für das *Trap-Nachrichtenformat* vor.

   Beispiel: `%Td (%Tn => %To) %Vz`

   Sie können die folgenden Elemente in Ihrer SNMP-Trap-Meldung verwenden:

Element	Beschreibung
`%Aa`	Die Agentenadresse.
`%Ah`	Der Agenten-Hostname.
`%d`	Lokaler Tag.
`%m`	Lokaler Monat.
`%y`	Lokales Jahr.
`%h`	Stunde vor Ort.
`%i`	Minute vor Ort.
`%s`	Sekunde vor Ort.
`%u`	Unix-Zeitstempel.
`%Td`	Trap-Beschreibung.
`%Tm`	Trap-MIB (Management Information Base).
`%Tn`	Trap-Name.
`%To`	Trap-OID (Objekt-ID).
`%Tt`	Trap-Typ (0-5 generisch; 6 - Unternehmen).
`%Tv`	Trap-Version (Inform, Trap {v1, v2 oder v3}).

Element	Beschreibung
`%Vd`**#**	Variablenbindungsbeschreibung (wobei '#' eine Zahl ist, die die Position des Elements in der Sequenz darstellt).
`%Vn`**#**	Variablenbindungsname (wobei '#' eine Zahl ist, die die Position des Elements in der Sequenz darstellt).
`%Vo`**#**	Variablenbindungs-OID (wobei '#' eine Zahl ist, die die Position des Elements in der Sequenz darstellt).
`%Vt`**#**	Variablenbindungstyp (wobei '#' eine Zahl ist, die die Position des Elements in der Sequenz darstellt).
`%Vv`**#**	Variablenbindungswert (wobei '#' eine Zahl ist, die die Position des Elements in der Sequenz darstellt).
`%Vz`	Zeigt alle Variablenbindungen an (`Name: Wert`, `Name: Wert`, `Name: Wert`). Wenn ein Name (aufgrund einer fehlenden MIB-Datei) fehlt, wird stattdessen die OID angezeigt.

5. Geben Sie nach Bedarf eine oder mehrere Warnstufen an.

   Folgende Warnstufe sind verfügbar: Kritisch, Fehler, Warnung, Info und Wiederhergestellt.

   - Klicken Sie unter *Kriterien* auf +, um eine neue Warnstufe hinzuzufügen.
   - Um eine bestehende Warnstufe zu bearbeiten, klicken Sie in der Zeile, die die Warnstufe enthält auf .

6. Legen Sie für jede Ebene Einschließen- und/oder Ausschließen-Ausdrücke fest und geben Sie an, ob die Ausdrücke Groß- /Kleinschreibung berücksichtigen. Diese Begriffe ermöglichen es Ihnen, bestimmte Ereignisse bei der Erkennung ein- oder auszuschließen.

   Die Syntax für eingeschlossene und ausgeschlossene Ausdrücke lautet wie folgt:

   `<`**Field_Type**`> {TRAP_OID|TRAP_NAME|TRAP_DESCRIPTION|TRAP_TYPE|TRAP_MIB|VARBIND} {=|!=|>|<|>=|<=} <`**Field_Value**`> [<AND|OR> <`**Condition_A**`>] [<AND|OR> <`**Condition_B**`>] ...`

   Beispiel:

   - `TRAP_OID = Labels.1.3.6.1.4.1.8072.2.3.2.1”`: Eine Warnung wird ausgegeben, wenn die Trap-OID enthält „`.1.3.6.1.4.1.8072.2.3.2.1`“.
   - `TRAP_NAME = "acctngFileFull" AND VARBIND = "acctngFileName|ABC"`: Eine Warnung wird ausgegeben, wenn der Trap-Name „`acctngFileFull`“ enthält und eine der Trap-Variablenbindungen „`acctngFileName`“ ist, mit einem Wert von „`ABC`“.

7. Klicken Sie unten auf der Seite auf **Speichern**.

HINWEIS: Mit der Schaltfläche **Auf Werkseinstellungen zurücksetzen** unten auf der Seite können Sie ein Standardprofil auf die Werkseinstellungen für das jeweilige Betriebssystem zurücksetzen.

Neue Profile basierend auf einem Standardprofil erstellen

Sie können ein Standardprofil oder ein vorhandenes Überwachungsprofil als Vorlage für das Erstellen eines neuen Profils verwenden, indem Sie es kopieren und die Kopie bearbeiten.

Jedem Gerät können mehrere Profile zugewiesen werden. Sie können zusätzliche Profile erstellen, die verschiedene Warnungen generieren, und die Profile an Geräte binden, denen bereits ein oder mehrere Profile zugeordnet sind.

1. Rufen Sie die Listenseite *Profile* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Überwachung** und anschließend auf **Profile**.
2. Aktivieren Sie das Kontrollkästchen für das vorhandene Profil, das Sie als Vorlage verwenden möchten, und klicken Sie auf **Aktion auswählen** > **Duplizieren und bearbeiten**, um die Seite *Profildetail* anzuzeigen.
3. Benennen Sie das Profil um und ändern Sie seine Beschreibung
4. **Optional**: Ändern Sie den *Namen* und die *Beschreibung* des Profils, um auf die Änderungen hinzuweisen.

   HINWEIS: Wenn Sie eines der Standardprofile bearbeiten, ist es nicht möglich, Änderungen am Feld *Automatisch hinzufügen zu* vorzunehmen.
5. Geben Sie für den Protokollpfad den entsprechenden Pfad für das Betriebssystem bzw. die Anwendung an.

   Sie können den in der folgenden Tabelle aufgeführten Basispfad für das Betriebssystem verwenden.

Betriebssystem	Protokollpfad
CentOS	`/var/log/messages`
Debian	`/var/log/syslog`
Fedora	`/var/log/messages`
FreeBSD	`/var/log/messages`
Mac OS X	`/var/log/system.log`
openSUSE	`/var/log/messages`
Oracle Enterprise Linux	`/var/log/messages`
Red Hat Enterprise Linux	`/var/log/messages`
Solaris	`/var/adm/messages`
SUSE Enterprise Linux	`/var/log/messages`
Ubuntu	`/var/log/syslog`

Betriebssystem	Protokollpfad
Windows	`application` für Windows Anwendungen **HINWEIS:** Sie müssen den *vollständigen Namen* des Ereignisprotokolls verwenden, der in den Eigenschaften des Protokolls angezeigt wird. Öffnen Sie zum Überprüfen des vollständigen Namens die *Ereignisanzeige*. Erweitern Sie *Windows Protokolle*, klicken Sie mit der rechten Maustaste auf das Ereignisprotokoll und wählen Sie **Eigenschaften** aus. Verwenden Sie die im Dialogfeld *Protokolleigenschaften* angezeigte Version des vollständigen Namens. `Microsoft-Windows TaskScheduler/Operational` für die Windows Aufgabenplanung (betriebsbereit)

Alternativ können Sie einen Pfad zu einem Protokoll eingeben, das neben den grundlegenden Ereignisprotokollen weitere Daten enthält. Wenn Sie beispielsweise eine Anwendung unter SUSE haben, die ihre Daten an ein spezielles Protokoll wie `/var/log/`**<meinAnwendungsprotokoll>** sendet, können Sie diesen Pfad in einem neuen Profil verwenden und den Suchtext sowie die Warnstufe wie hier beschrieben definieren.

Bei Geräten mit Linux Betriebssystemen gibt es je nach Version des Betriebssystems verschiedene Protokollpfade für MySQL und Apache Protokolle. Siehe Profil-Protokollpfade für MySQL und Apache.

HINWEIS: Es kann nur ein Protokollpfad in einem Profil festgelegt werden. Sie müssen für mehrere Protokolle mehrere Profile erstellen.

6. Nehmen Sie die erforderlichen Änderungen an den Einstellungen für die *Kriterien* vor.
   - **Ändern Sie den *Einschlusstext*.**
     1. Klicken Sie in der Zeile mit dem zu ändernden Einschlusstext auf die Schaltfläche **Bearbeiten**: .
     2. Geben Sie den neuen Suchtext ein und wählen Sie ggf. in der Dropdown-Liste **Groß-/Kleinschreibung beachten** den Eintrag *Ja* aus.
     3. Klicken Sie rechts neben der Zeile auf **Speichern**.
   - **Optional: Ändern Sie den *Ausschlusstext*.**
     1. Klicken Sie in der Zeile mit dem zu ändernden Text, um bestimmte Warnungen auszuschließen, auf die Schaltfläche **Bearbeiten**: .
     2. Geben Sie den neuen Ausschlusstext ein und wählen Sie ggf. in der Dropdown-Liste *Groß-/Kleinschreibung beachten* den Eintrag **Ja** aus.
     3. Klicken Sie rechts neben der Zeile auf **Speichern**.
   - **Ändern Sie die *Warnstufe*.**
     1. Klicken Sie in der Zeile mit der zu ändernden Warnstufe auf die Schaltfläche **Bearbeiten**: .
     2. Wählen Sie in der Dropdown-Liste *Stufe* eine der fünf Optionen aus: **Kritisch**, **Fehler**, **Warnung**, **Info** und **Wiederhergestellt**.
     3. Klicken Sie rechts neben der Zeile auf **Speichern**.
   - **Fügen Sie eine Warnung hinzu.**
     1. Klicken Sie unter der Kategorieüberschrift *Kriterien* auf die Schaltfläche **Hinzufügen**: .

2. Legen Sie die Warnstufe, den Suchtext und die Einstellung für die Groß-/Kleinschreibung fest und klicken Sie dann rechts neben der Zeile auf **Speichern**.
3. Wiederholen Sie diese Schritte für alle Warnungen, die Sie hinzufügen möchten.
4. **Optional**: Ordnen Sie die neuen Warnungskriterien mit der Schaltfläche **Drag** (Ziehen) neu an: ≡.

7. Klicken Sie unten auf der Seite auf **Speichern**.

Das Profil ist nun verfügbar und kann Geräten auf ihrer Seite *Überwachungsdetail* zugewiesen werden.

Profil-Protokollpfade für MySQL und Apache

Bei Geräten mit Linux Betriebssystemen gibt es je nach Version des Betriebssystems verschiedene Protokollpfade für MySQL und Apache Protokolle.

HINWEIS: Es kann nur ein Protokollpfad in einem Profil festgelegt werden. Sie müssen für mehrere Protokolle mehrere Profile erstellen.

Aktuelle Tabellen mit den Protokollpfaden für MySQL und Apache Protokolle finden Sie unter http://www.itninja.com/blog/view/mysqland-apache-profile-log-path-locations.

Hochladen eines Profils, das von einem anderen Benutzer erstellt wurde

Wenn ein anderer Benutzer ein benutzerdefiniertes Profil erstellt hat, das andere verwenden sollen, können Sie es in die Appliance hochladen.

Sie haben Zugriff auf eine XML-Profil-Datei, die ein anderer Benutzer erstellt hat.

1. Rufen Sie die Listenseite *Profile* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Überwachung** und anschließend auf **Profile**.
2. Wählen Sie **Aktion auswählen > Profile hochladen** aus, um das Dialogfeld *Profile hochladen* aufzurufen.
3. Klicken Sie auf **Datei auswählen**, um zum gewünschten Profil zu navigieren. Wählen Sie es aus und klicken Sie dann auf **Hochladen**.

   Sie können mehr als ein Profil hinzufügen.

Das oder die Profile werden unten in der Liste *Profile* angezeigt.

Sie können das neue Profil bei Bedarf bearbeiten. Siehe Profile bearbeiten.

Herunterladen eines Profils, damit es von anderen verwendet werden kann

Sie können ein benutzerdefiniertes Profil herunterladen, damit andere Benutzer es verwenden können.

1. Rufen Sie die Listenseite *Profile* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen*

aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.

b. Klicken Sie in der linken Navigationsleiste auf **Überwachung** und anschließend auf **Profile**.

2. Aktivieren Sie das Kontrollkästchen für die Profile, die Sie herunterladen wollen. Wählen Sie dann **Aktion auswählen** > **Profile herunterladen** aus, um die Profile an Ihren Ordner *Downloads* zu senden.

   Der XML-Dateiname des Profils wird vom Profilnamen auf der Profil-Detail-Seite abgeleitet und mit einer UNIX Zeitmarke ergänzt.

Verteilen Sie das Profil.

Zusätzliche Profile an ein Gerät binden

Wenn Sie die Serverüberwachung auf einem Gerät aktivieren, weist die Appliance dem Gerät das Standardprofil und den entsprechenden Standardprotokollpfad für das Betriebssystem des Geräts zu. Sie können bei Bedarf weitere selbst erstellte benutzerdefinierte Profile oder Profile aus anderen Quellen (z. B. ITNinja) hinzufügen.

1. Rufen Sie die Seite *Überwachungsdetail* auf:
   a. Klicken Sie in der linken Navigationsleiste auf **Überwachung** und anschließend auf **Geräte**.
   b. Klicken Sie auf den Namen eines Geräts, um die Seite *Überwachungsdetail* anzuzeigen.
2. Klicken Sie in das Feld *Profile*, um eine Dropdown-Liste der definierten Profile anzuzeigen, und wählen Sie das gewünschte Profil aus.
3. Klicken Sie auf **Speichern**.

Nicht standardmäßige Protokolldatumsformate definieren

Beim Überprüfen der Protokolldateien erkennt und verwendet die Appliance für jedes Betriebssystem das Standardformat für Protokolldatum und -uhrzeit. Wenn Sie in Ihren Protokollen jedoch ein ungebräuchliches Format verwenden, müssen Sie dieses Format definieren, damit das Protokoll korrekt von der Serverüberwachungsfunktion analysiert werden kann.

HINWEIS: In den meisten Fällen sollte dieses Feld leer bleiben.

HINWEIS: Das Format des Protokolldatums ist nicht relevant für Windows Ereignisprotokolle.

1. Rufen Sie die Listenseite *Profile* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Überwachung** und anschließend auf **Profile**.
2. Aktivieren Sie das Kontrollkästchen für das vorhandene Profil, das Sie bearbeiten möchten, und klicken Sie auf **Aktion auswählen** > **Bearbeiten**, um die Seite *Profildetail* anzuzeigen.
3. Geben Sie das nicht standardmäßige Protokolldatumsformat in das Feld *Format des Protokolldatums* ein.

   Klicken Sie neben *Format des Protokolldatums* auf ?, um die unterstützten Zeichen für das Format sowie entsprechende Beispiele anzuzeigen.
4. Klicken Sie unten auf der Seite auf **Speichern**.

Konfigurieren der Anwendungs- und Schwellenwertüberwachung mit Log Enablement Packages (LEP)

Für die Überwachung von Leistungsschwellenwerten und Anwendungen wie Exchange, Internetinformationsdienste (Internet Information Services, IIS) usw. sind sogenannte Protokollaktivierungspakete (Log Enablement Packages, LEPs) erforderlich, auf die Sie über die Listenseite *Log Enablement Packages* zugreifen können.

Auf der Listenseite *Log Enablement Packages* veröffentlicht Quest Basisvorlagen für die Windows Zuverlässigkeitsanalyse und den Systemmonitor (PerfMon) sowie Open Source-Perl-Skripte für Fremdsysteme (nicht Windows), mit deren Hilfe Benutzer Überwachungsfunktionen erweitern und Probleme mit der System- und Anwendungsleistung ermitteln können. Diese Vorlagen und Skripte sind verfügbar, sodass sie nicht neu erstellt werden müssen. Die zusätzlichen Vorlagen und Skripte sind nicht erforderlich für die Überwachung in der Appliance, die damit erstellten Profile sind jedoch hilfreich für die Überwachung von Leistungsschwellenwerten.

Windows PerfMon-Vorlage

In der Appliance ist ein standardmäßiges Windows Betriebssystem- und ein Anwendungs-LEP-Profil vordefiniert. Dieses Profil enthält die spezifischen Kriterien für das Ereignisprotokoll sowie allgemeine Kriterien, die Microsoft für von PerfMon ausgelöste Ereignisse verwendet. Die über LEPs auf der Listenseite "Log Enablement Packages" für Microsoft Server 2008 verfügbaren PerfMon-Basisvorlagen gelten für das System (CPU, Arbeitsspeicher, Festplatte), Exchange, SQL, IIS, Active Directory und Hyper-V.

HINWEIS: PerfMon-Vorlagen für Microsoft Server 2003 sind über ITNinja verfügbar.

Perl-Skripte (Nicht-Windows)

Bei den Paketen handelt es sich jeweils um ein Open-Source-Perl-Skript, das mithilfe des integrierten Betriebssystemplaners regelmäßig ausgeführt wird: cron, fcron usw. Das Perl-Skript führt bei seiner Ausführung eine Reihe von Befehlen aus, um die Auslastung von CPU, Speicher und lokalen Volumes zu ermitteln. Übersteigt die Auslastung den im Paket definierten Schwellenwert, wird eine Warnung in das Systemprotokoll geschrieben. Die Skripte sind zur Protokollierung im Systemprotokoll konfiguriert und beinhalten ein Präfix für jedes Ereignis. Um die Konfiguration zu vereinfachen, enthält die Appliance daher für alle Profile für andere Betriebssysteme als Windows vordefinierte Kriterien in den Standardwerten für das Systemprotokoll.

Über ITNinja verfügbare Pakete

ITNinja ist eine produktübergreifende IT-Community, in der sich IT-Spezialisten austauschen können, und eine umfassende Ressource für Informationen zur Konfiguration und Bereitstellung. Sie können nach Themen zu bestimmter Software und anderen Themen wie Bereitstellung, Verwaltung, Konfiguration und Fehlerbehebung suchen und selbst Informationen veröffentlichen. Die Community für die Serverüberwachung finden Sie unter http://itninja.com/community/k1000-monitoring.

Bei ITNinja finden Sie PerfMon-Vorlagen, die über die standardmäßig auf der Listenseite *Log Enablement Packages* verfügbaren Vorlagen hinausgehen. Dort stehen beispielsweise Vorlagen zur Konfiguration der Überwachung vieler Windows Server 2003-Protokolle zur Verfügung. Die Appliance-Funktion zum Installieren von LEPs unterstützt Windows Server 2003 nicht. Installieren Sie das entsprechende LEP mithilfe von PowerShell. Eine Dokumentation dieser Methode finden Sie bei ITNinja.

Benutzer der Appliance-Überwachungsfunktion, die Mitglieder der ITNinja-Community sind, können eigene Vorlagen und Skripte zur Erweiterung der Bibliothek verfügbarer LEPs bereitstellen. Ähnlich wie bei Windows Server 2003 Paketen müssen diese LEPs über eine auf ITNinja dokumentierte Methode installiert werden, da sie vom für Standardpakete verfügbaren Installationsvorgang nicht abgedeckt werden.

LEPs auf überwachten Geräten installieren

Sie können auf Windows-Geräten und Geräten mit anderen Betriebssystemen direkt von der Appliance Log Enablement Packages (LEP) installieren.

1. Rufen Sie die Listenseite *Log Enablement Packages* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Überwachung** und dann auf **Log Enablement Packages**.
2. Aktivieren Sie das Kontrollkästchen für das Paket oder die Pakete, die Sie auf Geräten installieren möchten. Wählen Sie dann **Aktion > Zu Geräten hinzufügen** aus, um die Seite *Log Enablement Pakete installieren* aufzurufen.

   Wenn Sie mehrere Pakete auswählen, können Sie sowohl Windows und als auch Pakete für andere Betriebssysteme installieren. In diesem Fall zeigt die Seite *Log Enablement Pakete installieren* einen separaten Abschnitt für Windows Pakete für und einen separaten Bereich für Nicht-Windows Pakete. Wenn alle ausgewählten Pakete den gleichen Typ haben, wird nur der Abschnitt für den betreffenden Typ angezeigt.
3. Wählen Sie die Geräte aus, für die Sie das Paket oder die Pakete hinzufügen wollen.
   a. Klicken Sie in das Textfeld *Geräte*, um eine Liste der Geräte im Inventar anzuzeigen, die zu den rechts unter *Ausgewählte Pakete* aufgelisteten Paketen kompatibel sind.
   b. Wählen Sie aus der Liste das oder die gewünschten Geräte aus.
4. **Optional**: Für Windows Pakete deaktivieren Sie das Kontrollkästchen *Windows und Anwendungs-LEP-Profil hinzufügen*, wenn das Profil bereits an das Gerät bzw. die Geräte gebunden ist und Sie es nicht erneut installieren möchten.
5. Legen Sie fest, wie Sie die Installation ablaufen soll, wenn eines der Pakete bereits auf einem Gerät installiert ist.
   - **Lassen Sie** *Ersetzen* **ausgewählt, wenn das aktuelle Paket über eine bestehende Version neu installiert werden soll.**
   - **Wählen Sie** *Überspringen* **aus, wenn Sie das womöglich derzeit auf dem Gerät installierte Paket behalten möchten. Sie könnten beispielsweise früher Änderungen an dem Paket vorgenommen haben und möchten diese nicht verlieren.**
6. Klicken Sie auf **Installieren**.
7. **Optional**: Zeigen Sie den Fortschritt der Installation an.
   a. Klicken Sie in der linken Navigationsleiste im Abschnitt **Überwachen** auf **Geräte** und wählen Sie den Namen des überwachten Geräts aus, um die zugehörige Seite *Überwachungsdetail* anzuzeigen.

      Unten auf der Seite wird der Abschnitt "Protokoll für LEP-Installation" angezeigt, der eine Zusammenfassung des Installationsprozesses für dieses spezielle Gerät enthält.
   b. **Optional**: Klicken Sie auf **Alle LEP-Installationsprotokolle für dieses Gerät anzeigen**, um weitere Details zu erhalten.

Geräte mit Windows Server 2003 mit einem Log Enablement Package (LEP) von ITNinja einrichten

Windows Server 2003 Log Enablement Packages (LEP) werden nicht in der LEP-Liste der Appliance angezeigt. Auch wird Windows Server 2003 von der Appliance-Funktion zum Installieren von Log Enablement Packages

(LEP) nicht unterstützt. Sie können jedoch Pakete von ITNinja erhalten, die Geräte mit Windows 2003 überwachen. Der Setup-Vorgang ist dann jedoch anders.

Fügen Sie das von einem Agenten oder ohne Agent verwaltete Gerät mit Windows Server 2003 dem Inventar in der Appliance hinzu. Siehe Informationen zur Geräteverwaltung.

Das Einrichten umfasst Aktionen auf dem zu überwachenden Servergerät und in der Appliance. Auf dem Servergerät laden Sie ein Protokollaktivierungspaket von ITNinja herunter und starten den Systemmonitor (PerfMon). In der Appliance aktivieren Sie die Überwachung für das Gerät, definieren das Profil für das Überwachungspaket und binden das Profil an das Gerät.

HINWEIS: Hier wird das Verfahren zum Installieren eines Pakets auf einem Gerät beschrieben. Zum Installieren mehrerer Pakete in einem Vorgang gibt es bei ITNinja Anleitungen für die Verwendung von PowerShell-Skripten. Siehe http://itninja.com/community/k1000-monitoring.

1. Laden Sie das entsprechende Überwachungs-LEP von ITNinja herunter.
   a. Rufen Sie die ITNinja-Community-Seite für die Überwachung auf: http://itninja.com/community/k1000-monitoring.
   b. Suchen Sie auf der Registerkarte **Downloads** nach dem Paket für die Leistungskategorie mit den gewünschten Leistungsindikatoren.

   Sie können Ihre Suche mithilfe der Suchfunktion eingrenzen.

   c. Klicken Sie auf **Herunterladen**, um die HTM-Datei für das Paket herunterzuladen.
   d. Kopieren Sie die HTM-Datei **<Leistungskategorie>**`_Alerts.htm` auf das zu überwachende Gerät.
2. Starten Sie auf dem zu überwachenden Gerät mit Windows Server 2003 den Systemmonitor und erweitern Sie den Ordner **Leistungsprotokolle und -warnungen**.
3. Klicken Sie unter **Leistungsprotokolle und -warnungen** mit der rechten Maustaste auf **Warnungen** und wählen Sie **Neue Warnungseinstellungen** aus. . ..
4. Navigieren Sie im Dialogfeld *Öffnen* zum Speicherort des Pakets, wählen Sie es aus und klicken Sie auf **Öffnen**.
5. Bestätigen Sie im Dialogfeld *Neue Warnungseinstellungen* den Namen des Pakets und klicken Sie auf **OK**, um die Eigenschaftenseite für das Paket anzuzeigen.
6. Übernehmen oder bearbeiten Sie die LEP-Eigenschaften:
   - **Übernehmen Sie die Standardeinstellungen und klicken Sie auf OK, um die Seite zu schließen.**
   - **Optional: Verwenden Sie ggf. die Registerkarte Allgemein der Eigenschaftenseite, um Leistungsindikatoren hinzuzufügen oder zu entfernen und die Schwellenwerte zu ändern. Klicken Sie anschließend auf OK. Siehe Überwachungs-Protokollaktivierungspaket (Log Enablement Package, LEP) für Geräte unter Windows Server 2003 bearbeiten.**
7. Klicken Sie im Fenster "Leistung" mit der rechten Maustaste auf den Namen des Pakets und wählen Sie **Starten** aus, um die Überwachung zu starten.

   Aktivieren Sie dann auf der Appliance die Überwachungsfunktion für das Gerät, erstellen Sie ein Profil und weisen Sie das Profil dem Gerät zu.
8. Aktivieren Sie in der Appliance die Überwachung für das Gerät.
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Inventar** und anschließend auf **Dashboard**.
   c. Klicken Sie auf den Namen des Geräts, um die zugehörige Seite *Gerätedetail* anzuzeigen.
   d. Scrollen Sie nach unten und klicken Sie unter **Aktivitäten** auf *Überwachung*, um den Abschnitt zu erweitern.
   e. Klicken Sie auf **Überwachung aktivieren**, um die Überwachung zu starten und Details zur standardmäßigen Überwachungskonfiguration für das Gerät anzuzeigen.

Wenn die Überwachung aktiviert ist, wird im Abschnitt *Überwachung* der Name des Überwachungsprofils angezeigt, das standardmäßig an das Gerät gebunden ist. Falls ein Standardwartungsfenster definiert wurde, wird dessen Name ebenfalls angezeigt.

9. Erstellen Sie auf der Seite *Profildetail* das Profil für das Überwachungspaket.
   a. Klicken Sie in der linken Navigationsleiste auf **Überwachung** und anschließend auf **Profile**.
   b. Aktivieren Sie auf der Listenseite *Profile* das Kontrollkästchen neben **ITNinja-Plug-In-Vorlage für Windows** und klicken Sie auf **Aktion auswählen** > **Duplizieren und bearbeiten**, um die Seite *Profildetail* anzuzeigen.
   c. Bearbeiten Sie den Namen und geben Sie eine Beschreibung für das Überwachungsprofil ein.
   d. Verwenden Sie den *Protokollpfad* von Windows Server 2003: Anwendung.
   e. Lassen Sie das Feld *Format des Protokolldatums* leer.
   f. **Optional**: Klicken Sie auf **Bearbeiten** ( ) und wählen Sie im Dropdown-Menü unter *Stufe* eine Warnstufe aus, wenn Sie eine andere Stufe als **Fehler** überwachen möchten.
   g. Klicken Sie am Ende der Zeile mit den Kriterien auf **Speichern** und anschließend unten auf der Seite auf **Speichern**.
10. Fügen Sie das neue Profil dem Gerät hinzu.
   a. Klicken Sie in der linken Navigationsleiste auf **Überwachung** und anschließend auf **Geräte**.
   b. Klicken Sie auf den Namen des Geräts, um die zugehörige Seite *Überwachungsdetail* anzuzeigen.
   c. Klicken Sie in das Feld *Profile*, um eine Dropdown-Liste der verfügbaren Profile anzuzeigen, und wählen Sie das erstellte Profil aus.
   d. Klicken Sie auf **Speichern**.

Das Profil ist nun an das Gerät gebunden.

Überwachungs-Protokollaktivierungspaket (Log Enablement Package, LEP) für Geräte unter Windows Server 2008 oder höher bearbeiten

Sie können die Leistungsindikatoren in einem Überwachungs-LEP, das auf einen Server installiert wurde, hinzufügen, entfernen und konfigurieren.

Das Protokollaktivierungspaket wurde auf dem Gerät installiert. Siehe LEPs auf überwachten Geräten installieren.

1. Starten Sie auf dem Gerät, das Sie überwachen möchten, den Systemmonitor, erweitern Sie den Ordner **Datensammlersatz** und anschließend den Ordner **Benutzerdefiniert**.
2. Wählen Sie den im LEP definierten Datensammlersatz aus.
3. **Optional**: Wenn das Paket momentan ausgeführt wird, klicken Sie mit der rechten Maustaste auf den Namen des Datensammlersatzes und wählen Sie **Beenden** aus.
4. Klicken Sie im rechten Fensterbereich mit der rechten Maustaste auf den Datensammler (DataCollector) und wählen Sie **Eigenschaften** aus, um das Dialogfeld *Eigenschaften* anzuzeigen.
5. Bearbeiten Sie das Paket auf den Registerkarten des Dialogfelds *Eigenschaften*:

Option	Beschreibung
Warnungen	Auf der Registerkarte **Warnungen** können Sie das Schwellenwertattribut und das Intervallattribut eines Leistungsindikators bearbeiten. Sie können auf dieser Registerkarte auch Leistungsindikatoren hinzufügen und entfernen. So konfigurieren Sie den Leistungsindikator:

Option	Beschreibung
	a. Wählen Sie den Leistungsindikator unter *Leistungsindikatoren* aus. b. Bearbeiten Sie den Warnungsauslöser mithilfe der Dropdown-Liste *Warnung bei* und des Felds *Grenze*. c. Bearbeiten Sie das Sammlungsintervall mithilfe der Dropdown-Menüs *Probenintervall* und *Einheiten*. d. Klicken Sie auf **OK**, um die Änderungen zu speichern. So fügen Sie dem LEP einen Leistungsindikator hinzu: a. Klicken Sie auf **Hinzufügen**, um das Dialogfeld zum Hinzufügen von Leistungsindikatoren anzuzeigen. Leistungsindikatoren für lokal installierte Anwendungen werden unter *Verfügbare Leistungsindikatoren* angezeigt. Sie können auch Objekte und Leistungsindikatoren von einem Remote-System auswählen, wenn Sie die Liste unter *Leistungsindikatoren auswählen von Computer* oder die Schaltfläche **Durchsuchen** verwenden. b. Wählen Sie unter *Verfügbare Leistungsindikatoren* die Leistungsindikatoren aus, die Sie hinzufügen möchten, und klicken Sie auf **Hinzufügen >>**. c. Klicken Sie auf **OK**, um zur Seite *Eigenschaften* zurückzukehren. So entfernen Sie einen Leistungsindikator aus dem LEP: a. Wählen Sie den Leistungsindikator unter *Leistungsindikatoren* aus. b. Klicken Sie auf **Entfernen**. c. Klicken Sie auf **OK**, um die Änderungen zu speichern.
Warnungsaktion	Der Zweck des Pakets besteht darin, Ereignisse im Ereignisprotokoll zu erfassen und der Überwachungsfunktion der Appliance dadurch die Auswahl einer Warnung zu ermöglichen. Das Kontrollkästchen *Einen Eintrag im Ereignisprotokoll der Anwendung protokollieren* muss daher aktiviert bleiben.
Warnungstask	Auf dieser Registerkarte können Sie eine Aufgabe definieren, die bei der Auslösung der Warnung ausgeführt wird.

6. Klicken Sie unten im Dialogfeld **Eigenschaften** auf *OK*, um zum Systemmonitor zurückzukehren.
7. Klicken Sie im Ordner **Benutzerdefiniert** mit der rechten Maustaste auf das Paket und wählen Sie **Starten** aus, um die Überwachung zu starten.

Überwachungs-Protokollaktivierungspaket (Log Enablement Package, LEP) für Geräte unter Windows Server 2003 bearbeiten

Sie können die Leistungsindikatoren in einem Überwachungs-LEP, das auf einen Server installiert wurde, hinzufügen, entfernen und konfigurieren.

Das Protokollaktivierungspaket wurde auf dem Gerät installiert. Siehe LEPs auf überwachten Geräten installieren.

1. Starten Sie auf dem Gerät, das Sie überwachen möchten, den Systemmonitor und erweitern Sie den Ordner **Leistungsprotokolle und -warnungen**.
2. Klicken Sie auf **Warnungen** und klicken Sie dann im Detailbereich mit der rechten Maustaste auf das gewünschte LEP.
3. **Optional**: Wird das Paket derzeit ausgeführt, klicken Sie mit der rechten Maustaste auf das LEP und wählen Sie **Beenden** aus.
4. Klicken Sie ggf. erneut mit der rechten Maustaste auf den LEP-Namen und wählen Sie **Eigenschaften** aus, um das Dialogfeld *Eigenschaften* anzuzeigen.
5. Bearbeiten Sie das Paket auf der Registerkarte **Allgemein** des Dialogfelds *Eigenschaften*:
    a. Wählen Sie unter *Leistungsindikatoren* einen Leistungsindikator aus, um seine aktuelle Konfiguration anzuzeigen.
    b. Bearbeiten Sie den Warnungsauslöser mithilfe der Dropdown-Liste *Warnung bei folgendem Wert* und des Felds *Grenze*.
    c. Bearbeiten Sie das Sammlungsintervall mithilfe der Dropdown-Menüs *Intervall* und *Einheiten* für die Einstellung *Daten erfassen alle*.
    d. Legen Sie unter *Ausführen als* Kontoberechtigungen fest.

    - Standardmäßig wird das Paket mit den Berechtigungen des Systemkontos ausgeführt. Zur weiteren Ausführung mit diesen Berechtigungen übernehmen Sie die `<Standardeinstellung>` für *Ausführen als*.
    - Integrierte Gruppen haben Zugriff auf die folgenden Leistungsindikatorfunktionen:

Gruppe	Funktionen
Mitglieder der lokalen Administratorgruppe	Alle Leistungsindikatorfunktionen verfügbar
Mitglieder der Gruppe Benutzer	• Können die Anzeigeeigenschaften des Systemmonitors ändern • Können Protokolldateien im Systemmonitor anzeigen • Können keine Warnungseinstellungen erstellen
Mitglieder der Gruppe Systemmonitorbenutzer	• Können alle für die Gruppe Benutzer verfügbaren Funktionen verwenden • Können Echtzeitprotokolle im Systemmonitor anzeigen und die Anzeigeeigenschaften des Systemmonitors in Echtzeit ändern • Können keine Warnungseinstellungen erstellen oder ändern
Mitglieder der Gruppe Leistungsprotokollbenutzer	• Können alle für die Gruppe Systemmonitorbenutzer verfügbaren Funktionen verwenden • Können Warnungseinstellungen erstellen und ändern, nachdem der Gruppe die Anmeldung als Batchbenutzer zugewiesen wurde

6. **Optional**: Fügen Sie dem LEP einen Leistungsindikator hinzu:
   a. Klicken Sie im Dialogfeld *Eigenschaften* auf **Hinzufügen**, um das Dialogfeld *Leistungsindikatoren hinzufügen* anzuzeigen.

      Wenn *Lokale Leistungsindikatorobjekte verwenden* aktiviert ist, werden Leistungsindikatoren für lokal installierte Anwendungen unter *Indikatoren aus Liste auswählen* angezeigt. Sie können auch Objekte und Leistungsindikatoren von einem Remote-System auswählen, wenn Sie die Liste unter *Leistungsindikatoren auswählen von Computer* verwenden.

   b. Wählen Sie unter *Leistungsindikatoren auswählen von Computer* die Leistungsindikatoren aus, die Sie hinzufügen möchten, und klicken Sie auf **Hinzufügen**.
   c. Klicken Sie auf **OK**, um zur Seite *Eigenschaften* zurückzukehren.
7. **Optional**: Entfernen Sie einen Leistungsindikator aus dem LEP:
   a. Wählen Sie im Dialogfeld "Eigenschaften" unter *Zähler* den gewünschten Leistungsindikator aus.
   b. Klicken Sie auf **Entfernen**.
   c. Klicken Sie auf **OK**, um die Änderungen zu speichern.
8. Klicken Sie unten im Dialogfeld **Eigenschaften** auf *OK*, um zum Systemmonitor zurückzukehren.
9. Klicken Sie im Detailbereich mit der rechten Maustaste auf das LEP und wählen Sie **Starten** aus, um die Überwachung zu starten.

Verwalten der Geräteüberwachung

Nachdem die Überwachung für ein Gerät aktiviert wurde, können Sie konfigurieren, wie und wann die Überwachung erfolgt, und die Überwachung auf Geräteebene verwalten.

Überwachung für ein Gerät anhalten

Sie können die Überwachung anhalten, wenn Sie verhindern möchten, dass die Überwachungsfunktion Warnungen generiert, während Sie an einem Gerät arbeiten oder Änderungen an einem Gerät vornehmen.

HINWEIS: Wenn Sie die Überwachung bei regelmäßigen Wartungsaufgaben basierend auf einem festgelegten Zeitplan anhalten möchten, können Sie Zeitpläne für Wartungsfenster festlegen. Siehe Wartungsfenster planen, während dessen keine Alarme von einem Gerät erfasst werden.

Informationen zum gleichzeitigen Anhalten oder Fortsetzen der Überwachung für mehrere Geräte finden Sie unter Überwachung für mehrere Geräte anhalten oder fortsetzen.

1. Rufen Sie die Seite *Überwachungsdetail* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Überwachung** und anschließend auf **Geräte**.
   c. Klicken Sie in der Spalte *Gerät* auf das gewünschte Gerät, um die zugehörige Seite *Überwachungsdetail* anzuzeigen.
2. Aktivieren Sie das Optionsfeld *Angehalten* und klicken Sie auf **Speichern**.

Ein Symbol in der Spalte *Status* auf der Seite *Gerät* des Abschnitts *Inventar* zeigt an, dass die Überwachung angehalten wurde:

- : Die Serverüberwachung ist für dieses vom Agenten verwaltete Gerät angehalten.
- : Die Serverüberwachung ist für dieses ohne Agent verwaltete Gerät angehalten.

Überwachung für mehrere Geräte anhalten oder fortsetzen

Sie können die Überwachung für mehrere Geräte gleichzeitig anhalten. Ebenso ist es möglich, die Überwachung für mehrere Geräte fortzusetzen.

1. Rufen Sie die Listenseite *Überwachte Geräte* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Überwachung** und anschließend auf **Geräte**.
2. Aktivieren Sie die Kontrollkästchen aller Geräte, für die Sie die Überwachung anhalten oder fortsetzen möchten.
3. Klicken Sie auf **Aktion auswählen** > **Überwachung anhalten** oder **Überwachung fortsetzen**.

   Der Eintrag in der Spalte *Überwachung* für die Geräte ändert sich entsprechend dem neuen Status in *Angehalten* oder *Aktiv*.

Abrufintervall und Einstellungen für das automatische Verwerfen oder Löschen von Warnungen festlegen

Sie können einige allgemeine Überwachungseinstellungen konfigurieren, um festzulegen, wie oft die Appliance Warnungen aus den Protokollen abruft. Außerdem können Sie die Appliance so konfigurieren, dass Warnungen nach einer bestimmten Anzahl von Tagen automatisch verworfen und gelöscht werden.

Durch das Verwerfen wird eine Warnung auf der Listenseite *Warnungen* und in den Dashboard-Widgets ausgeblendet. Durch das Löschen wird eine Warnung aus der Datenbank entfernt. Verworfene Warnungen können wiederhergestellt werden, gelöschte Warnungen jedoch nicht.

1. Rufen Sie die Seite *Überwachungseinstellungen* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Einstellungen** und anschließend auf **Überwachungseinstellungen**.
2. Legen Sie das Abrufintervall fest (in Minuten).

   Das Mindestintervall beträgt 10 Minuten.
3. **Optional**: Legen Sie fest, dass Warnungen nach einer bestimmten Anzahl von Tagen von der Appliance verworfen werden sollen.
   a. Wählen Sie *Warnungen automatisch verwerfen* aus.
   b. Geben Sie die Anzahl von Tagen an.
4. **Optional**: Legen Sie fest, dass Warnungen nach einer bestimmten Anzahl von Tagen von der Appliance gelöscht werden sollen.
   a. Wählen Sie *Warnungen automatisch löschen* aus.
   b. Geben Sie die Anzahl von Tagen an.
5. Klicken Sie auf **Speichern**.

Verwandte Themen

Warnungen verwerfen

Warnungen löschen

Verworfene Warnungen in der Warnungsliste abrufen und überprüfen

Ping-Test deaktivieren

Ping-Tests sind standardmäßig aktiviert, wenn Sie die Überwachung für ein Gerät aktivieren. Da Ping-Tests in bestimmten Fällen jedoch zu einer Flut von Warnungen führen können, bietet die Appliance die Möglichkeit, sie zu deaktivieren.

Bei einem Ping-Test werden Internet Control Message-Protokoll (ICMP)-Echoanforderungspakete an das jeweilige Ziel gesendet. Einige Firewalls blockieren ICMP-Pakete. Daher ist es aufgrund der Häufigkeit von Ping-Tests möglich, dass eine große Anzahl von Warnungen aufgrund abgelehnter Tests generiert wird. In diesen Fällen kann die Übersichtlichkeit der Überwachungsergebnisse durch Deaktivieren der Ping-Tests verbessert werden.

1. Rufen Sie die Seite *Überwachungseinstellungen* auf:

a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.

b. Klicken Sie in der linken Navigationsleiste auf **Einstellungen** und anschließend in der *Systemsteuerung* auf **Überwachungseinstellungen**.

2. Deaktivieren Sie *Ping-Test aktivieren*.
3. Klicken Sie auf **Speichern**.

Warnungen bei Gerätekonfigurationsänderungen empfangen

Sie können die Überwachung so einrichten, dass eine Warnung generiert wird, wenn die Konfiguration eines überwachten Geräts geändert wird.

Wenn Sie diese Funktion aktivieren, wird jedes Mal, wenn eine Gerätekonfigurationsänderung erkannt wird, eine Warnung generiert. Sie können festlegen, welche Arten von Änderungen für die Gerätebestände erkannt werden sollen, indem Sie sie im Dialogfeld *Gerät*, auf das Sie über die Seite *Asset-Verlaufskonfiguration* zugreifen können auswählen.

Beispiele für Konfigurationsänderungen sind das Hinzufügen eines neuen Datenträgers oder logischen Laufwerks, eine Erhöhung oder Verringerung des Speicherplatzes, eine Partitionsänderung usw. Vollständige Informationen zur Seite *Asset-Verlaufskonfiguration* und zur Auswahl von Konfigurationsänderungen finden Sie unter Asset-Verlaufsabonnements konfigurieren.

1. Rufen Sie die Seite *Überwachungsdetail* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Überwachung** und anschließend auf **Geräte**.
   c. Klicken Sie auf den Namen eines Geräts.
2. Aktivieren Sie das Kontrollkästchen *Warnung bei Konfigurationsänderung aktivieren*.
3. Klicken Sie auf **Speichern**.

Wartungsfenster planen, während dessen keine Alarme von einem Gerät erfasst werden

Wartungsfenster bieten Ihnen die Möglichkeit, bestimmte Zeitfenster für die Durchführung von Serverwartungsaufgaben zu reservieren. So können Sie verhindern, dass die Überwachungsfunktion das System während dieser Zeiten mit einer übermäßigen Anzahl von Warnungen überschwemmt.

Jedem überwachten Gerät können mehrere Wartungsfenster zugewiesen werden. Sie können eine Bibliothek von Wartungsfenstern erstellen und je nach Bedarf Kombinationen dieser Wartungsfenster auf überwachte Geräte anwenden.

1. Rufen Sie die Seite *Wartungsfensterdetail* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen*

aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.

b. Klicken Sie in der linken Navigationsleiste auf **Überwachung** und anschließend auf **Wartungsfenster**.

c. Wählen Sie **Aktion auswählen > Neu**.

2. Geben Sie die folgenden Informationen an:

Option	Beschreibung
Name	Ein Name, der das Wartungsfenster identifiziert. Der Name wird auf der Liste *Wartungsfenster* angezeigt.
Beschreibung	Informationen zum Zweck des Wartungsfensters.
Add Automatically To (Automatisch hinzufügen zu)	• **Keine**: Das Wartungsfenster wird einem Gerät nicht automatisch hinzugefügt, wenn die Überwachung für das Gerät aktiviert wird. • **Alle**: Das Wartungsfenster wird einem Gerät automatisch hinzugefügt, wenn die Überwachung für das Gerät aktiviert wird.

3. Geben Sie im Abschnitt *Zeitplan* folgende Zeitplanungseinstellungen an:

Option	Beschreibung
Täglich/an einem bestimmten Tag von HH:MM bis HH:MM	Das Wartungsfenster wird täglich oder an einem festgelegten Wochentag zu einer festgelegten Uhrzeit für eine bestimmte Dauer gestartet.
Ausführen am n-ten jedes Monats/eines bestimmten Monats von HH:MM bis HH:MM	Das Wartungsfenster wird jeden Monat oder in einem festgelegten Monat am gleichen Tag zu einer festgelegten Uhrzeit für eine bestimmte Dauer gestartet.

HINWEIS: Für den Zeitplan gilt das 24-Stunden-Format.

4. Klicken Sie auf **Speichern**.
5. Wenden Sie das Wartungsfenster auf der Seite *Überwachungsdetail* eines überwachten Geräts auf das Gerät an:

   a. Klicken Sie in der linken Navigationsleiste auf **Überwachung** und anschließend auf **Geräte**.

   b. Klicken Sie auf den Namen eines Geräts, um die Seite *Überwachungsdetail* anzuzeigen.

   c. Klicken Sie in das Feld *Wartungsfenster*, um eine Dropdown-Liste der definierten Wartungsfenster anzuzeigen, und wählen Sie das gewünschte Fenster aus.
6. Klicken Sie auf **Speichern**.

Überwachungsspezifische Rollen erstellen und zuweisen

Sie können Benutzerrollen zum Steuern der Berechtigungen für die Arbeit mit Warnungen und Profilen erstellen.

Sie können beispielsweise eine Rolle für einen Mitarbeiter erstellen, der auf Warnungen reagieren und Service-Desk-Tickets für sie erstellen kann, aber nicht berechtigt ist, Geräten Profile hinzuzufügen oder Wartungsfenster festzulegen.

Wenn die Organisationskomponente auf Ihrer Appliance aktiviert ist, hängen die für Benutzerrollen verfügbaren Berechtigungen von der Organisationsrolle ab, die der Organisation zugewiesen ist. Siehe Verwalten von Organisationsrollen und Benutzerrollen.

HINWEIS: Die vordefinierten Rollen können nicht geändert werden: Administrator, Kein Zugriff, Administrator mit Leseberechtigung und Benutzer.

1. Rufen Sie die Seite *Rollendetail* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie auf der linken Navigationsleiste auf **Einstellungen** und anschließend auf **Rollen**.
   c. Klicken Sie auf **Aktion auswählen** > **Neu**, um die Seite *Rollendetail* zu öffnen.
2. Geben Sie im Feld *Name* einen Namen ein, beispielsweise Mitarbeiter Warnungsüberwachung.
3. Geben Sie im Feld *Beschreibung* eine Kurzbeschreibung der Rolle ein, beispielsweise Für Mitarbeiter, die für die Beantwortung von Warnungen zuständig sind.

   Diese Beschreibung wird zusammen mit dem Namen in der Liste *Rollen* angezeigt.
4. Klicken Sie auf den Link **Überwachung** unter Administratorkonsole *Berechtigungen*, um die Berechtigungseinstellungen für die Serverüberwachung anzuzeigen.
5. Legen Sie die Berechtigungen entsprechend der Zugriffsebene fest, die Sie der Rolle zuweisen möchten:
   - **Alle schreiben**
   - **Alle lesen**
   - **Alle ausblenden**
   - **Benutzerdefiniert:**

Sie können die Berechtigungen SCHREIBEN, LESEN oder AUSBLENDEN für die folgenden Überwachungsseiten kombinieren.

Kategorie	Seite (einschließlich Detailseite)	Relevante Berechtigungen für die Aktionen
Überwachung	**Geräte**	• Warnungen bestätigen (verwerfen) • Überwachung von Konfigurationsänderungen aktivieren • Überwachung anhalten oder fortsetzen • Profile hinzufügen oder entfernen • Wartungsfenster hinzufügen oder entfernen • Überwachung deaktivieren • Warnungen exportieren
	Warnungen	• Warnungen bestätigen (verwerfen) • Service Desk-Ticket erstellen • Benachrichtigungen festlegen • Warnungen abrufen • Warnungen löschen • Warnungen exportieren
	Profile	• Profile erstellen • Profile bearbeiten • Profile löschen • Profile von allen Geräten entfernen • Hoch- und herunterladen von Profilen
	Wartungsfenster	• Wartungsfenster erstellen • Wartungsfenster bearbeiten • Wartungsfenster löschen • Wartungsfenster von allen Geräten entfernen • Wartungsfenster exportieren
	Überwachungs-LEP	• Hinzufügen zu Geräten • Exportieren von LEPs

6. Weisen Sie der Rolle ggf. die Berechtigung zum Aktivieren der Überwachung auf einem Gerät zu.

Da ein Benutzer die Überwachung auf der Seite *Gerätedetail* des Geräts aktiviert, muss die Berechtigung im Abschnitt *Inventar* festgelegt werden.

   a. Klicken Sie auf den Link **Inventar** unter Administratorkonsole *Berechtigungen*, um die Berechtigungseinstellungen für das Inventar anzuzeigen.
   b. Legen Sie *Geräte* auf **SCHREIBEN** fest.

7. Klicken Sie auf **Speichern**.
8. Weisen Sie die Rolle einem Benutzer zu.
   a. Klicken Sie auf der linken Navigationsleiste auf **Einstellungen** und anschließend auf **Benutzer**.
   b. Aktivieren Sie das Kontrollkästchen neben dem Benutzer, dem Sie die Rolle zuweisen möchten.
   c. Klicken Sie auf **Aktion auswählen** > **Rolle übernehmen** > **Name der Rolle**.

Deaktivieren der Überwachung für ein oder mehrere Geräte

Wenn Sie ein Gerät nicht mehr überwachen möchten, können Sie die Funktion deaktivieren. Das Gerät wird dann nicht mehr auf Ihr Lizenzlimit angerechnet.

Sie können die Überwachung für ein Gerät an drei Stellen deaktivieren. Zwei davon beziehen sich auf einzelne Geräte, eine Stelle ermöglicht die Anwendung auf eine Gruppe von Geräten.

- Deaktivieren der Überwachung auf der Seite *Gerätedetail* des Geräts:
  1. Klicken Sie in der linken Navigationsleiste auf **Inventar** und anschließend auf **Dashboard**.
  2. Klicken Sie auf den Namen eines Geräts.
  3. Scrollen Sie nach unten und klicken Sie unter **Aktivitäten** auf *Überwachung*, um den Abschnitt zu erweitern.
  4. Klicken Sie auf **Überwachung deaktivieren**.
  5. Bestätigen Sie die Aktion im Bestätigungsdialogfeld.
- Deaktivieren der Überwachung auf der Seite *Überwachungsdetail* des Geräts:
  1. Klicken Sie in der linken Navigationsleiste auf **Überwachung** und anschließend auf **Geräte**.
  2. Klicken Sie auf den Namen eines Geräts.
  3. Klicken Sie auf **Überwachung deaktivieren**.
  4. Bestätigen Sie die Aktion im Bestätigungsdialogfeld.
- Deaktivieren Sie die Überwachung für mehrere Geräte in der Liste *Geräte*.
  1. Klicken Sie in der linken Navigationsleiste auf **Überwachung** und anschließend auf **Geräte**.
  2. Aktivieren Sie die Kontrollkästchen vor allen Geräten, für die Sie die Überwachung deaktivieren möchten.
  3. Wählen Sie **Aktion auswählen** > **Überwachung deaktivieren** aus.
  4. Bestätigen Sie die Aktion im Bestätigungsdialogfeld.

Durch das Deaktivieren der Überwachung werden die Warnungen des Geräts nicht gelöscht. Für Warnungen im Zusammenhang mit einem deaktivierten Gerät wird auf der Listenseite *Überwachungswarnungen* der Hinweis **Das Gerät wurde gelöscht oder wird nicht mehr überwacht** in der Spalte *Gerät* angezeigt. Wenn Sie die Überwachung für das Gerät wieder aktivieren, behandelt die Appliance das Gerät jedoch wie ein neues zu überwachendes Gerät. In diesem Fall wird für die vorherigen Warnungen des Geräts weiterhin **Das Gerät wurde gelöscht oder wird nicht mehr überwacht** angezeigt.

Informationen zum Löschen von Warnungen finden Sie unter Warnungen löschen.

Aktivieren der Überwachung für ein oder mehrere Geräte

Wenn Sie ein Gerät überwachen möchten, können Sie mit der Überwachung beginnen. Geräte, die zur Überwachung aktiviert sind, werden auf Ihr Lizenzlimit angerechnet.

WICHTIG: Die Aktivierung der Überwachung auf SNM-verwalteten Geräten wird nicht auf das Lizenzlimit angerechnet.

Sie können die Überwachung für ein Gerät an drei Stellen aktivieren. Zwei davon beziehen sich auf einzelne Geräte, eine Stelle ermöglicht die Anwendung auf eine Gruppe von Geräten.

- Aktivieren der Überwachung auf der Seite *Gerätedetail* des Geräts:
    1. Klicken Sie in der linken Navigationsleiste auf **Inventar** und anschließend auf **Dashboard**.
    2. Klicken Sie auf den Namen eines Geräts.
    3. Scrollen Sie nach unten und klicken Sie unter **Aktivitäten** auf *Überwachung*, um den Abschnitt zu erweitern.
    4. Klicken Sie auf **Überwachung aktivieren**.
    5. Bestätigen Sie die Aktion im Bestätigungsdialogfeld.
- Aktivieren Sie die Überwachung für mehrere Geräte in der Liste *Geräte*.
    1. Klicken Sie in der linken Navigationsleiste auf **Inventar** und anschließend auf **Dashboard**.
    2. Aktivieren Sie die Kontrollkästchen vor allen Geräten, für die Sie die Überwachung aktivieren möchten.
    3. Wählen Sie **Aktion auswählen** > **Überwachen aktivieren**.
    4. Bestätigen Sie die Aktion im Bestätigungsdialogfeld.

Die Aktivierung der Überwachung für ein Gerät ermöglicht es diesem Gerät, Alarme zu erzeugen, wenn bestimmte Schwellenwerte erreicht werden. Wenn Sie die Überwachung für das Gerät erneut aktivieren, behandelt die Appliance das Gerät wie ein neues zu überwachendes Gerät. In diesem Fall werden vorherigen Gerätewarnungen angezeigt als **Gerät wurde gelöscht oder wird nicht mehr überwacht**. Informationen zum Löschen von Warnungen finden Sie unter Warnungen löschen.

Arbeiten mit Warnungen

Wenn die Serverüberwachung eine Warnung generiert, stehen Ihnen verschiedene Möglichkeiten für die weitere Bearbeitung der Warnung zur Verfügung.

Sie können auf Grundlage der Warnung ein Service Desk-Ticket oder eine automatisierte E-Mail-Benachrichtigung erstellen. Nachdem Sie die Warnung entsprechend Ihren Verfahrensweisen bearbeitet haben, können Sie sie verwerfen oder löschen.

Wenn Sie Ihrem Dashboard Überwachungs-Widgets hinzugefügt haben, können Sie auf einen Blick die neuesten Warnungen mit Links zu den Listenseiten *Überwachungswarnungen* und *Überwachte Geräte* sehen.

Die folgenden Symbole geben die Warnstufe an:

- : **Kritisch**
- : **Fehler**
- : **Warnung**
- : **Information**
- : **Wiederhergestellt**

Verwandtes Thema

Informationen zu Dashboard-Widgets

Hinzufügen von Benachrichtigungszeitplänen über die Listenseite "Überwachungswarnungen"

Sie können für Geräte, Warnstufen, Meldungen und andere Warnungsinformationen Benachrichtigungszeitpläne für Überwachungswarnungen hinzufügen. Anhand dieser Zeitpläne kann die Appliance Administratoren per E-Mail oder Push-Benachrichtigungen an ein KACE GO Mobilgerät benachrichtigen, wenn bestimmte Kriterien erfüllt sind.

Sie haben Ihre E-Mail-Benachrichtigungseinstellungen konfiguriert.

1. Führen Sie zum Anzeigen der Seite *Überwachungswarnungen* einen der folgenden Schritte aus:
   - **Wenn das Widget** *Überwachungswarnungen* **installiert und das** *Dashboard* **geöffnet ist, klicken Sie auf Überwachungswarnungen.**
   - **Klicken Sie in der linken Navigationsleiste auf Überwachung > Warnungen.**
2. Aktivieren Sie das Kontrollkästchen für die Zeile mit der Warnmeldung und klicken Sie anschließend oberhalb der Warnungsliste rechts auf **Benachrichtigung**, um den Fensterbereich *Benachrichtigung* anzuzeigen.
3. Wählen Sie Benachrichtigungskriterien aus. Um eine Benachrichtigung zu senden, wenn Informationswarnungen generiert werden, geben Sie beispielsweise Folgendes ein:

   ```
   Stufe | ist | Information
   ```

4. Geben Sie die folgenden Informationen unterhalb der Benachrichtigungskriterien ein.

Feld	Beschreibung
Titel	Die Informationen, die in der *Betreff*-Zeile der E-Mail-Benachrichtigung stehen sollen.
E-Mail-Empfänger	Die E-Mail-Adresse oder -Adressen der gewünschten Empfänger. Es müssen vollständige, gültige E-Mail-Adressen verwendet werden. Um E-Mails an mehrere Adressen zu senden, trennen Sie die Adressen durch Kommas oder verwenden E-Mail-Verteiler.
Häufigkeit	Das Intervall, in dem die Appliance die Abfrage ausführt, um die gewählten Kriterien mit Elementen

Feld	Beschreibung
	im Inventar zu vergleichen. Werden Kriterien erfüllt, wird eine Benachrichtigung gesendet.

5. **Optional**: Aktivieren Sie das Kontrollkästchen *An KACE Go senden*, wenn die Warnung an ein Mobilgerät weitergeleitet werden soll, auf dem die KACE GO App installiert ist.

   Diese Option ist nur verfügbar, wenn der Mobilgerätezugriff aktiviert ist. Siehe Konfigurieren des Mobilgerätezugriffs.

6. **Optional**: Klicken Sie auf **Testen**, um die Kriterien zu überprüfen.

   Die Liste wird aktualisiert, damit nur die Elemente angezeigt werden, die den festgelegten Kriterien entsprechen. Es werden keine Benachrichtigungen während des Tests versendet.

7. Klicken Sie auf **Speichern**.

Die Benachrichtigung wird erstellt und auf der Seite *Benachrichtigungszeitpläne* angezeigt. Weitere Informationen zum Planen der Benachrichtigungshäufigkeit finden Sie unter Benachrichtigungszeitpläne bearbeiten.

Verwandte Themen

Informationen zu Benachrichtigungen

Zeitplanung für Benachrichtigungen

Service-Desk-Tickets aus Warnungen erstellen

Sie können anhand einer Serverüberwachungswarnung ein Service Desk-Ticket erstellen. Die Felder im Ticketformular werden dabei automatisch mit den Informationen aus der Warnung ausgefüllt.

1. Führen Sie zum Anzeigen der Liste *Überwachungswarnungen* einen der folgenden Schritte aus:
   - **Wenn das Widget** *Überwachungswarnungen* **installiert und das** *Dashboard* **geöffnet ist, klicken Sie auf Überwachungswarnungen.**
   - **Klicken Sie in der linken Navigationsleiste auf Überwachung > Warnungen.**
2. Aktivieren Sie das Kontrollkästchen für die Zeile mit der Warnmeldung und klicken Sie anschließend auf **Aktion auswählen** > **Neues Ticket**.
   - Wenn Sie ein Ticket basierend auf einer Warteschlange erstellen möchten, wenn es mehrere Ticket-Warteschlangen in der Organisation gibt, wählen Sie eine Warteschlange aus der Dropdown-Liste **Ticket** aus.
   - Wenn Sie ein Ticket basierend auf einer Prozessvorlage erstellen möchten, wählen Sie den Prozess aus der Dropdown-Liste **Prozess** aus.

   Die Felder *Titel*, *Übersicht*, *Absender* und *Gerät* enthalten Informationen aus der Warnung.
3. **Optional**: Ändern Sie die Angaben in den Feldern *Titel* und *Übersicht* entsprechend den Verfahrensweisen Ihres Unternehmens.
4. Füllen Sie das Formular mit den weiteren erforderlichen Informationen aus und klicken Sie anschließend auf **Speichern**, um das Ticket zu speichern und die Seite *Details zum Ticket* zu schließen. Oder klicken Sie auf **Änderungen übernehmen**, um das Ticket zu speichern und seine Bearbeitung fortzusetzen.

Option	Beschreibung
Titel	(Erforderlich) Eine kurze Beschreibung des Problems. Sie können den von der Überwachungsfunktion generierten Titel durch einen Titel Ihrer Wahl ersetzen.
Übersicht	Eine ausführlichere Beschreibung des Problems.

Option	Beschreibung

	Dieses Feld umfasst eine umfassende Reihe von Bearbeitungsoptionen zum Formatieren Ihrer Inhalte, wie Schaltflächen für fettgedruckten Text, Hyperlinks, Listen oder Textfarbe.
	Beispiel:
	• Um Fettdruck auf eine Textfolge anzuwenden, wählen Sie diese im Editor aus und klicken auf B.
	• Um Bilder hinzuzufügen, klicken Sie auf , und geben Sie die URL der Bilddatei oder einen lokalen Dateipfad an, oder legen Sie das Bild einfach in dem angegebenen Bereich ab.
	  ◦ Sie können Screenshots auch kopieren und direkt in das Textfeld einfügen.
	  ◦ Alle Bilder, die Sie auf diese Weise einfügen, werden als Dateianhänge zum Ticket hinzugefügt. Sie sind gegebenenfalls auch in der E-Mail-Kommunikation enthalten.
	  ◦ Wenn Sie ein Bild aus dem Textfeld löschen, wird der zugehörige Dateianhang nicht entfernt. Dateianhänge können Sie im Abschnitt *Anlage* der Ticket-Seite verwalten. Weitere Informationen hierzu finden Sie unter Screenshots und Anhänge zu Service-Desk-Tickets hinzufügen oder aus ihnen löschen.
	• Um externe Links hinzuzufügen, klicken Sie auf .
	• Um extern gehostete Videos einzubetten, klicken Sie auf .

Absender	Der Anmeldename des Benutzers, der das Ticket sendet. Der Absender kann durch Auswahl eines anderen Anmeldenamens in der Dropdown-Liste geändert werden. Klicken Sie auf , um die Kontaktinformationen des Absenders anzuzeigen.
Asset	Das Asset, auf das sich die Informationen im Ticket beziehen. Wählen Sie ein Asset aus der Dropdown-Liste aus. Klicken Sie auf , um die Asset-Details anzuzeigen.
Nach den dem Absender zugewiesenen Assets filtern	Filtern Sie die Asset-Liste basierend auf den Assets, die dem Absender zugewiesen sind.
Gerät	Das Gerät, auf das sich die Informationen im Ticket beziehen. Diese Informationen werden von der

Option	Beschreibung
	Überwachungsfunktion bereitgestellt. Klicken Sie auf , um die Gerätedetails anzuzeigen.
Nach den dem Absender zugewiesenen Geräten filtern	Filtern Sie die Asset-Liste basierend auf den Geräten, die dem Absender zugewiesen sind.
Auswirkungen	Die Anzahl der Benutzer, die bei der Arbeit beeinträchtigt sind oder nicht arbeiten können.
Kategorie	Eine Klassifizierung des Problems.
Status	Der aktuelle Status des Tickets. Dieses Feld wird nicht angezeigt, wenn Sie ein Ticket aus einer Prozessvorlage erstellen oder bearbeiten.
Priorität	Die Bedeutung des Tickets.
Besitzer	Der Benutzer, der während des Lebenszyklus des Tickets für dessen Verwaltung verantwortlich ist.
Fällig	Datum und Uhrzeit für den geplanten Abschluss des Tickets. Falls keine Service Level-Vereinbarungen aktiviert sind, wird als Fälligkeitsdatum standardmäßig Kein(e) festgelegt. Sind Service Level-Vereinbarungen aktiviert, wird das Fälligkeitsdatum automatisch gemäß den SLA-Einstellungen berechnet. Das Fälligkeitsdatum wird basierend auf der Priorität berechnet, die beim Übermitteln des Tickets festgelegt wurde. Wurde die Priorität nach der Ticketübermittlung geändert, wird das Fälligkeitsdatum gemäß der neuen Priorität, jedoch basierend auf dem Datum und der Uhrzeit der ursprünglichen Übermittlung neu berechnet. Wird die Konfiguration der SLA-Auflösungszeit geändert, gilt sie nur für neue Tickets. Alte Tickets sind davon nicht betroffen. Siehe Konfigurieren von Service Level-Vereinbarungen. Wählen Sie **Manuelles Datum** aus, um Fälligkeitsdatum und -uhrzeit manuell festzulegen. Wenn Service Level-Vereinbarungen aktiviert sind, werden in diesem Fall Fälligkeitsdatum und -uhrzeit berechnet und als Option angezeigt, jedoch nicht ausgewählt.
CC-Liste	Eine Liste der Benutzer, die im Fall eines Ticketereignisses eine Benachrichtigungs-E-Mail erhalten. Die Empfänger in der CC-Liste erhalten eine E-Mail auf der Grundlage des Ticketereignisses und der für die Warteschlange **E-Mail bei Ereignissen** konfigurierten Einstellung **Ticket CC**.

Option	Beschreibung

Lösung	Die Lösung des mit dem Ticket verknüpften Problems.
	Dieses Feld umfasst eine umfassende Reihe von Bearbeitungsoptionen zum Formatieren Ihrer Inhalte, wie Schaltflächen für fettgedruckten Text, Hyperlinks, Listen oder Textfarbe.
	Beispiel:
	• Um Fettdruck auf eine Textfolge anzuwenden, wählen Sie diese im Editor aus und klicken auf B.
	• Um Bilder hinzuzufügen, klicken Sie auf , und geben Sie die URL der Bilddatei oder einen lokalen Dateipfad an, oder legen Sie das Bild einfach in dem angegebenen Bereich ab.
	  ◦ Sie können Screenshots auch kopieren und direkt in das Textfeld einfügen.
	  ◦ Alle Bilder, die Sie auf diese Weise einfügen, werden als Dateianhänge zum Ticket hinzugefügt. Sie sind gegebenenfalls auch in der E-Mail-Kommunikation enthalten.
	  ◦ Wenn Sie ein Bild aus dem Textfeld löschen, wird der zugehörige Dateianhang nicht entfernt. Dateianhänge können Sie im Abschnitt *Anlage* der Ticket-Seite verwalten. Weitere Informationen hierzu finden Sie unter Screenshots und Anhänge zu Service-Desk-Tickets hinzufügen oder aus ihnen löschen.
	• Um externe Links hinzuzufügen, klicken Sie auf .
	• Um extern gehostete Videos einzubetten, klicken Sie auf .

Zugehörige Ticketinformationen	Dieser Abschnitt wird nicht angezeigt, wenn Sie ein Ticket aus einer Prozessvorlage erstellen.
Ticket hinzufügen	Um ein zusätzliches Ticket zu der zugehörigen Ticketinformation hinzuzufügen, klicken Sie.
Referrer	**Referrer** ist ein schreibgeschütztes Feld mit einem Ticketverweis auf ein Ticket, das mithilfe des Abschnitts **Siehe auch** auf dieses Ticket verweist.
Zusammengeführte Tickets	In diesem Abschnitt können Sie die Liste der Tickets bearbeiten, die mit diesem Ticket zusammengeführt wurden. Alle Tickets, die Sie zusammenführen möchten, müssen derselben Warteschlange angehören. Wenn Sie Tickets auf

Option	Beschreibung
	der Seite *Ticketdetails* zusammenführen, wird das offene Ticket zum Hauptticket. Alle anderen zusammengeführten Tickets werden archiviert, wenn Sie sie zusammenführen. Weitere Informationen finden Sie unter Zusammenführen von Tickets. Um ein zusammengeführtes Ticket hinzuzufügen, klicken Sie auf **Tickets zum Zusammenführen hinzufügen/Zusammengeführte Tickets bearbeiten** und wählen Sie ein Ticket aus der angezeigten Liste aus.
Prozessinformationen	Dieser Abschnitt wird nur angezeigt, wenn Sie ein Ticket aus einer Prozessvorlage erstellen. Alle Einstellungen in diesem Abschnitt sind schreibgeschützt. Umfassende Informationen zum Erstellen und Konfigurieren von Prozessvorlagen finden Sie unter Hinzufügen, Bearbeiten und Aktivieren von Prozessvorlagen
Prozess	Der Name der diesem Ticket zugeordneten Prozessvorlage.
Prozesstyp	Der Prozesstyp.
Prozessstatus	Der Status des dieser Prozessvorlage zugeordneten Workflows. Zum Beispiel *Genehmigung ausstehend*.
Übergeordnet	Der Name der diesem übergeordneten Ticket, wie in der Prozessvorlage, die diesem Ticket zugeordnet ist, definiert wurde.
Prozessgenehmigungen	Eine Liste aller Benutzer, die als Genehmiger für dieses Ticket zugordnet sind, falls zutreffend. Die Genehmiger werden in Stufen aufgeführt, wie in der Prozessvorlage definiert. Jede Stufe kann je nach Bedarf einen oder mehrere Genehmiger haben. Die Einstellungen für Genehmiger und Stufe werden auch in diesem Abschnitt aufgeführt, wie z. B. Zeitlimit für Genehmigungen und die Benachrichtigungen. Wenn Sie einen Prozessticket erstellen, beginnt das Zeitlimit für den ersten Genehmiger. Wenn dieser Benutzer das Ticket genehmigt, beginnt das Zeitlimit für den nächsten usw.
Prozessaktivitäten	Eine Liste der Prozessaktivitäten von denen jede ein untergeordnetes Ticket repräsentiert und in Stufen aufgeführt wird, wie in der Prozessvorlage definiert. Mehrere Tickets können der gleichen Stufe zugewiesen werden, falls das erforderlich sein sollte. Wenn z. B. die erste Stufe die Bestellung von Ausstattungen und Verbrauchsmaterialien für eine Neueinstellung ist, könnten mehrere separate untergeordnete Tickets für die Bestellung von Geräten, Büroausstattungen und Verbrauchsmaterialien sinnvoll sein, die

Option	Beschreibung
	alle Stufe 1 zugewiesen sind. Bei der Erstellung eines Prozesstickets werden alle der Stufe 1 zugewiesenen Prozesstickets automatisch erstellt. Tickets der Stufe 2 werden erstellt, wenn alle Tickets der Stufe 1 abgeschlossen sind. Tickets der Stufe 3 werden erstellt, wenn alle Tickets der Stufe 2 abgeschlossen sind usw.
Ticket hinzufügen	Um ein zusätzliches Ticket zu der zugehörigen Ticketinformation hinzuzufügen, klicken Sie.
Referrer	**Referrer** ist ein schreibgeschütztes Feld mit einem Ticketverweis auf ein Ticket, das mithilfe des Abschnitts **Siehe auch** auf dieses Ticket verweist.
Kommentare	Kommentare, die zum Ticket hinzugefügt werden sollen. Außerdem können Sie Dateianhänge, Screenshots, automatische Antworten oder Inhalte aus Artikeln der Wissensdatenbank als Ticket-Kommentare hinzufügen. Weitere Informationen hierzu finden Sie unter: • Tickets Kommentare hinzufügen • Screenshots und Anhänge zu Service-Desk-Tickets hinzufügen oder aus ihnen löschen Wenn Sie eine automatische Antwort als Lösung für dieses Ticket hinzufügen möchten, klicken Sie auf **Vordefinierte Antwort** und wählen Sie eine Antwortvorlage aus. Die ausgewählte Antwortvorlage wird im Feld **Auflösung** angezeigt. Sie können mehrere Antwortvorlagen als Auflösungseinträge hinzufügen. Sie werden in der Reihenfolge angezeigt, in der Sie sie ausgewählt haben. **TIPP:** Um eine Antwortvorlage zu erstellen oder zu bearbeiten, speichern Sie Ihre Änderungen und klicken Sie auf **Verwalten**. Dadurch gelangen Sie zur Seite *Antwortvorlagen*. Weitere Informationen über Antwortvorlagen finden Sie unter Antwortvorlagen anzeigen und bearbeiten.
Knowledge Base-Artikel	Rufen Sie einen Wissensdatenbank-Artikel auf und fügen Sie seinen Inhalt zu den Ticket-Kommentaren hinzu. Weitere Informationen zu Knowledge Base-Artikeln finden Sie unter Verwalten von Knowledge Base-Artikeln.

Verwandte Themen

Verwalten von Service Desk-Tickets, -Prozessen und -Berichten

Mit erweiterten Suchkriterien nach Warnungen suchen

Mit der Advanced Page-Level Search (erweiterte Suche auf Seitenebene) können Sie auf der jeweils aktuellen Seite mithilfe verschiedener Kombinationen von Kriterien nach Informationen suchen.

Dieses Beispiel zeigt, wie Sie mit der erweiterten Suche nach kritischen Warnungen im Zusammenhang mit einem Verbindungsproblem suchen.

1. Führen Sie zum Anzeigen der Seite *Überwachungswarnungen* einen der folgenden Schritte aus:
   - **Wenn das Widget** *Überwachungswarnungen* **installiert und das** *Dashboard* **geöffnet ist, klicken Sie auf Überwachungswarnungen.**
   - **Klicken Sie in der linken Navigationsleiste auf Überwachung > Warnungen.**
2. Klicken Sie über der Liste *Überwachungsalarme* auf der rechten Seite auf **Erweiterte Suche**.

   Der Bereich *Erweiterte Suche* wird angezeigt.

3. Geben Sie die erforderlichen Kriterien für die Suche nach einer Warnstufe an:

   `Informationen zu Überwachungswarnungen: Stufe | ist | Kritisch`
4. Wählen Sie in der Dropdown-Liste mit den Operatoren die Option **UND** aus, klicken Sie zum Hinzufügen einer neuen Zeile auf **Zeile hinzufügen** und geben Sie anschließend die erforderlichen Kriterien für die Suche nach Warnungen an, deren Meldung den Text **Verbindung kann nicht hergestellt werden** enthält:

   `Informationen zu Überwachungswarnungen: Meldung | hat | Verbindung kann nicht hergestellt werden`
5. Klicken Sie auf **Suchen**.

Die Liste wird aktualisiert, damit nur die Geräte angezeigt werden, die den festgelegten Kriterien entsprechen.

Filtern von Warnungen mit der Einschluss- und Ausschlusstext-Funktion

Wenn Sie zu viele Warnungen eines bestimmten Typs erhalten oder eine bestimmte Warnung verfolgen möchten, können Sie Warnungen basierend auf dem Meldungstext und Schweregrad filtern.

Sie können bestimmte Ereignisse davon ausschließen, dass sie Warnungen auslösen, wenn Sie sie unnötig oder ablenkend finden. Um die Warnungen herauszufiltern, die Sie nicht erhalten möchten, geben Sie mit *Ausschlusstext* den Inhalt an, der eine ungewünschte Warnung identifiziert. Verwenden Sie *Ausschlusstext* in Verbindung mit *Einschlusstext*, um einen Untersatz einer Warnungskategorie zu definieren.

Es gibt zwei Methoden zum Filtern von Warnungen, die durch die Überwachungsfunktion gemeldet werden. Die eine erfolgt über die Seite *Profildetails* und die andere über das Dropdown-Menü **Aktion auswählen** der Listenseite *Überwachungswarnungen*.

Herausfiltern von Warnmeldungen mit der Einschluss- und Ausschlusstext-Funktion auf der Seite "Profil-Details"

Sie können erhaltene Warnungen auch nach Meldungstext und Schweregrad filtern.

Verwenden Sie *Ausschlusstext* in Verbindung mit *Einschlusstext*, um einen Untersatz einer Warnungskategorie zu definieren.

HINWEIS: Die Textübereinstimmung als Kriterium – wie beispielsweise Fehler – wird in Windows Ereignisprotokolle nach Schweregrad und hinsichtlich der eigentlichen Meldung abgeglichen.

1. Rufen Sie die Listenseite *Profile* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Überwachung** und anschließend auf **Profile**.
2. Aktivieren Sie das Kontrollkästchen für das vorhandene Profil, das Sie bearbeiten möchten, und klicken Sie auf **Aktion auswählen** > **Bearbeiten**, um die Seite *Profildetail* anzuzeigen.
3. Nehmen Sie die erforderlichen Einschluss- und Ausschluss-Einstellungen für die *Kriterien* vor.
   - **Ändern Sie den *Einschlusstext*.**
     1. Klicken Sie in der Zeile mit dem zu ändernden Einschlusstext auf die Schaltfläche **Bearbeiten**: .
     2. Geben Sie den neuen Suchtext ein.
   - **Ändern Sie den *Ausschlusstext*.**
     1. Klicken Sie in der Zeile mit dem zu ändernden Text, um bestimmte Warnungen auszuschließen, auf die Schaltfläche **Bearbeiten**: .
     2. Geben Sie den neuen Ausschlusstext ein.
   - **Wählen Sie bei Bedarf in der Dropdown-Liste *Groß-/Kleinschreibung* die Option Ja aus.**
   - **Fügen Sie ein Warnungskriterium hinzu.**
     1. Klicken Sie unter der Kategorieüberschrift *Kriterien* auf die Schaltfläche **Hinzufügen**: .
     2. Legen Sie die Ebene fest, schließen Sie Text ein oder aus und geben Sie die Groß-/Kleinschreibung an.
4. Klicken Sie unten auf der Seite auf **Speichern**.

Verwandte Themen

Beispiele für Einschluss- und Ausschlusstext für Überwachungsprofile

Profile bearbeiten

Warnungen mit der Ausschlusstext-Funktion auf der Listenseite "Überwachungswarnungen" filtern

Wenn Sie zu viele Warnungen von einer bestimmten Art haben, können Sie diese basierend auf dem Text der Nachricht filtern.

Sie können vollständige Nachrichten, Teile von Nachrichten, und grundlegende reguläre Ausdrücke im Feld *Ausschlusstext* dazu verwenden, Filterkriterien für erhaltene Warnungen zu definieren.

1. Rufen Sie die Liste *Überwachungswarnungen* auf:

a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.

b. Greifen Sie auf die Liste der Alarmmeldungen entweder vom Dashboard oder über die Navigationsleiste zu.

- **Wenn das Widget** *Überwachungswarnungen* **installiert und das** *Dashboard* **geöffnet ist, klicken Sie auf Überwachungswarnungen.**
- **Klicken Sie in der linken Navigationsleiste auf Überwachung > Warnungen.**

2. Aktivieren Sie das Kontrollkästchen neben einer Warnung.
3. Wählen Sie**Aktion auswählen > Warnungen wie die folgenden herausfiltern** aus.

   Das Dialogfeld *Warnungen wie die folgenden herausfiltern* wird angezeigt. Der Inhalt der Warnmeldung steht im Feld *Ausschlusstext*.
4. Bearbeiten Sie das Feld *Ausschlusstext* zum Verfeinern des Filters.

   Beispiel: Wenn Sie Warnungen für Festplattenfehler ausgeben wollen, aber keine Warnungen bei einer fragmentierten Festplatte, können Sie z. B. Folgendes eingeben:

Einschlusstext-Eintrag	Ausschlusstext-Eintrag
Fehlercode.*Disk /dev/sd[a-z]	ist fragmentiert

5. Klicken Sie auf **Speichern**.

   Das Profil, von dem die Warnmeldung generiert wurde, wird mit diesen Ausschlussinformationen geändert.

Verwandte Themen

Beispiele für Einschluss- und Ausschlusstext für Überwachungsprofile

Herausfiltern von Warnmeldungen mit der Einschluss- und Ausschlusstext-Funktion auf der Seite "Profil-Details"

Beispiele für Einschluss- und Ausschlusstext für Überwachungsprofile

In den Feldern *Einschlusstext* und *Ausschlusstext* können vollständige Nachrichten, Teile von Nachrichten und grundlegende reguläre Ausdrücke zur Definition von Kriterien verwendet werden.

Beispiele von Feldeinträgen zur Übereinstimmung mit Zeichenkettenformaten

Zeichenkettenformat (Ziel der Übereinstimmung)	Beispieldaten	Einschlusstext	Kommentare
[beliebiger Text]`Error 32768 Physical memory running low`[beliebiger Text]	`Error 32768 Physical memory running low`	`Error 32768 Physical memory running low`	Übereinstimmungen: „`Error 32768 Physical memory running low`“
`Drive /dev/`[beliebiger Datenträger-Bereitstellungspunkt] `has drive errors`	`Drive /dev/sdi has drive errors`	`Drive /dev/[a-z]{1,} has drive errors`	Übereinstimmungen: „`Drive /dev/`“ gefolgt von einem beliebigen Wort

Zeichenkettenformat (Ziel der Übereinstimmung)	Beispieldaten	Einschlusstext	Kommentare
			beliebiger Länge mit den Zeichen a–z gefolgt von „`has drive errors`“
`Error` nnnn`: Disk is` [beliebiger Text]	`2014-06-28: Error 4567: Disk is full`	`Error [0-9]{4}: Disk is`	Übereinstimmungen: „`Error`“ gefolgt von einer vierstelligen Zahl gefolgt von „`: Disk is`“
`Error` nnnnnn [eine Fehlermeldung]	`Error 4096 Drive has errors`	`Error [0-9]{1,8}`	Übereinstimmungen: „`Error`“ gefolgt von einer ein- bis achtstelligen Zahl
`[FATAL]` [eine Fehlermeldung]	`[FATAL] General exception occurred`	`[FATAL].*`	Übereinstimmungen: „`[FATAL]`“ gefolgt von einer beliebigen Meldung
`error reading` [Text] `on` [ein Volume]:	`error reading swap label on /dev/VolGroup00: [Errno 21] Is a directory`	`error reading.* on /dev/[a-zA-Z0-9]*:`	Übereinstimmungen: „`error reading`“ gefolgt von einem beliebigen Text gefolgt von „`on /dev/`“ gefolgt von einem beliebigen Bereitstellungspunkt beliebiger Länge mit den Zeichen a–z, A–Z und 0–9 gefolgt von einem Doppelpunkt

Beispiele für die gemeinsame Verwendung von Einschluss- und Ausschlusstext zur Filterung der Warnungsausgabe

Beispiel A: Zeichenkette als Ausschlusstext

In diesem Beispiel möchten Sie von einem bestimmten Datenträger-Bereitstellungspunkt keine Warnungen bezüglich fragmentierter Datenträger erhalten. Alle anderen Warnungen sollen jedoch ausgegeben werden.

```
2015-02-03T15:38:45.129748-06:00 SLES12u0x64 Error code 4: Disk /dev/sda has
errors 2015-02-03T15:38:45.129748-06:00 SLES12u0x64 Error code 5: Disk /dev/sda is
fragmented 2015-02-03T15:38:45.129748-06:00 SLES12u0x64 Error code 6: Disk /dev/sda
has a bad block
```

Wenn Sie Warnungen zu Festplattenfehlern und beschädigten Speicherblöcken ausgeben, aber keine Warnungen bei fragmentierten Datenträgern erhalten möchten, können Sie z. B. Folgendes eingeben:

Einschlusstext-Eintrag	Ausschlusstext-Eintrag
`Fehlercode.*Disk /dev/sd[a-z]`	`ist fragmentiert`

HINWEIS: *Einschlusstext* erkennt keine Zeilenumbrüche innerhalb des Textfelds. Wenn Sie also

```
code 5
code 7
```

HINWEIS: eingegeben haben, wird nach Übereinstimmungen für `code 5code 7` gesucht. In diesem Fall sollten Sie **Hinzufügen** verwenden, um eine separate Zeile für den zweiten Einschlusstext zu erstellen.

HINWEIS: *Ausschlusstext* erkennt jedoch Zeilenumbrüche innerhalb des Textfelds. Wenn Sie also

```
code 5
code 7
```

HINWEIS: eingegeben haben, wird nach Übereinstimmungen für `code 5` sowie für `code 7` gesucht. In diesem Fall müssen Sie **Hinzufügen** nicht verwenden, um eine separate Zeile für den zweiten Ausschlusstext zu erstellen.

Beispiel B: Grundlegender regulärer Ausdruck als Ausschlusstext

In diesem Beispiel möchten Sie von einem bestimmten Datenträger-Bereitstellungspunkt keine Warnungen bezüglich fragmentierter Datenträger oder Altersinformationen erhalten. Alle anderen Warnungen sollen jedoch ausgegeben werden.

```
2015-02-03T15:38:45.129748-06:00 SLES12u0x64 Error code 4: Disk /dev/sda has
errors 2015-02-03T15:38:45.129748-06:00 SLES12u0x64 Error code 5: Disk /dev/sda is
fragmented 2015-02-03T15:38:45.129748-06:00 SLES12u0x64 Error code 6: Disk /dev/sda
has a bad block 2015-02-03T15:38:45.129748-06:00 SLES12u0x64 Error code 7: Disk /
dev/sda is more than 3 years old
```

Um Warnungen für die bevorzugten Ereignisse auszugeben, aber gleichzeitig die Ereignisse auszuschließen, die Fehlercode 5 oder Fehlercode 7 enthalten, geben Sie Folgendes ein:

Einschlusstext-Eintrag	Ausschlusstext-Eintrag
`Fehlercode.*Disk /dev/sd[a-z]`	`Error code [5|7]`

Escape-Sequenz für Sonderzeichen in den Textfeldern „Einschlusstext“ und „Ausschlusstext“

Bei der Eingabe von Zeichen in die Textfelder „Einschlusstext“ oder „Ausschlusstext“ können Sie auch Sonderzeichen, wie z. B. einfache oder doppelte Anführungszeichen, verwenden. Wenn Sie jedoch entsprechende Sonderzeichen eingeben, müssen Sie einen Backslash (\) als Escape-Sequenz verwenden, damit die Suche ordnungsgemäß funktioniert.

Zeichen	Beschreibung
'	Einfache Anführungszeichen
”	Doppelte Anführungszeichen
`	Gravis
\	Backslash

Um beispielsweise nach **Received 'redoubt started' message** zu suchen, geben Sie Received \'redoubt started \' message ein.

Warnungen verwerfen

Wenn Sie eine Warnung bearbeitet haben, können Sie sie verwerfen, damit sie nicht mehr in den Listen mit aktiven Warnungen angezeigt wird.

Durch das Verwerfen wird eine Warnung nicht aus der Datenbank entfernt. Informationen zum Löschen von Warnungen aus der Datenbank finden Sie unter Warnungen löschen.

1. Führen Sie zum Anzeigen der Seite *Überwachungswarnungen* einen der folgenden Schritte aus:
   - **Wenn das Widget** *Überwachungswarnungen* **installiert und das** *Dashboard* **geöffnet ist, klicken Sie auf Überwachungswarnungen.**
   - **Klicken Sie in der linken Navigationsleiste auf Überwachung > Warnungen.**
2. Aktivieren Sie das Kontrollkästchen für die Zeile mit der Warnmeldung und klicken Sie anschließend auf **Aktion auswählen** > **Verwerfen**.

   Die Warnung wird nicht mehr in der Warnungsliste angezeigt.

Verwandtes Thema

Verworfene Warnungen in der Warnungsliste abrufen und überprüfen

Verworfene Warnungen in der Warnungsliste abrufen und überprüfen

Eine verworfene Warnung bleibt in der Datenbank erhalten und kann in der Warnungsliste abgerufen und dort überprüft werden.

HINWEIS: Gelöschte Warnungen können nicht abgerufen werden.

1. Führen Sie zum Anzeigen der Seite *Überwachungswarnungen* einen der folgenden Schritte aus:
   - **Wenn das Widget** *Überwachungswarnungen* **installiert und das** *Dashboard* **geöffnet ist, klicken Sie auf Überwachungswarnungen.**
   - **Klicken Sie in der linken Navigationsleiste auf Überwachung > Warnungen.**
2. Klicken Sie auf **Aktion auswählen** > **Verworfene Warnungen einschließen**.

   Alle verworfenen Warnungen werden wieder in der Warnungsliste angezeigt. Für diese Warnungen wird in der Spalte *Status* der Status *Verworfen* angezeigt.

Warnungen löschen

Nachdem Sie eine Warnung zufrieden stellend bearbeitet haben, können Sie sie aus der Datenbank löschen.

1. Rufen Sie die Liste *Überwachungswarnungen* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Überwachung** und anschließend auf **Geräte**.
2. Aktivieren Sie das Kontrollkästchen neben den gewünschten Warnungen.
3. Wählen Sie **Aktion auswählen** > **Löschen** und klicken Sie dann zum Bestätigen auf **Ja**.

Verwenden des Service Desks

Der Service Desk ist das in der Appliance enthaltene Trouble-Ticket-Erfassungssystem für Endbenutzer. Mit dem Service Desk können Benutzer Trouble-Tickets per E-Mail, über die Administratorkonsole oder über die Benutzerkonsole senden.

Konfigurieren des Service Desks

Die Konfiguration des Service Desks umfasst das Einrichten von Rollen, der Benutzerauthentifizierung, von Labels, Ticket- und E-Mail-Einstellungen, Warteschlangen und Anpassungen.

Systemanforderungen

Zum Verwenden des Service Desks benötigen Sie eine Appliance, einen E-Mail-Server und Benutzerkontoinformationen.

- **Appliance requirements (Appliance-Anforderungen)**: Die Verwendung des Service Desks setzt voraus, dass Sie eine Appliance eingerichtet und konfiguriert haben. Informationen zum Einrichten der Appliance-Servers finden Sie unter Konfigurieren der Appliance.
- **E-Mail-Serveranforderungen**: Sie benötigen einen der folgenden E-Mail-Servertypen zum Senden und Empfangen von Service Desk-E-Mails:
  - Einen POP3-E-Mail-Server. Informationen dazu finden Sie unter Informationen zu POP3-E-Mail-Konten.
  - Einen E-Mail-Server wie zum Beispiel den Microsoft Exchange Server. Anweisungen dazu, wie Sie diesen Server zum Herstellen einer Verbindung mit der Appliance konfigurieren, finden Sie unter Konfigurieren von SMTP-E-Mail-Servern.
- **Benutzerkontodaten**: Die Benutzerkontodaten können in einem LDAP-kompatiblen Verzeichnisdienst wie Microsoft Active Directory gespeichert werden. Werden Benutzerkontodaten gespeichert, kann der Service Desk effizient die Daten auffinden und importieren, die zur Autorisierung von Benutzern und Identifizierung anderer Elemente benötigt werden, die Sie verfolgen möchten. Sie können Benutzergruppen oder andere Einheiten filtern, indem Sie auf ihre LDAP-Attribute verweisen, beispielsweise Organisationseinheiten, Domänenkomponenten und Relative Distinguished Names. Siehe Konfigurieren von Benutzerkonten, LDAP-Authentifizierung und SSO.

Wenn Ihre Organisation klein ist, muss diese Anforderung nicht erfüllt werden, wenn Sie die erforderlichen Kontodaten manuell und für jeden Benutzer einzeln erstellen. Weitere Informationen zum manuellen Erstellen von Benutzern finden Sie unter Einrichten des Service Desks.

Informationen zum Service Desk

Der Standardname des Trouble-Ticket-Erfassungssystems für Endbenutzer, das Teil der Appliance **Benutzerkonsole** ist, lautet Service Desk. Mit dem Service Desk können Endbenutzer Trouble-Tickets per E-Mail oder über die **Benutzerkonsole** senden.

Ihr Helpdesk-Team bearbeitet diese Tickets per E-Mail, über die **Administratorkonsole**, `http://`**appliance_hostname**`/admin` oder über die KACE GO App. Sie können die Kategorien und Felder der Tickets nach Bedarf anpassen.

HINWEIS: In Vorgängerversionen der Appliance hieß der **Service Desk** noch **Helpdesk**. Wenn Sie ein Upgrade von einer Vorgängerversion ausführen, wird unter Umständen die Bezeichnung **Help Desk** oder eine benutzerdefinierte Formulierung auf der Registerkarte in der **Administratorkonsole** angezeigt. Sie können dieses Label wie in Umbenennen von Service Desk-Titeln und Labels beschrieben ändern.

Überblick über Setup-Aufgaben

Sie können Service Desk so konfigurieren, dass die Anforderungen bezüglich Unternehmensrichtlinien und -Branding erfüllt werden.

Zu Setup-Aufgaben zählen:

- **Benutzerrollen und Labels einrichten**: Erstellen Sie berechtigungsbasierte Rollen für die Verwaltung des Benutzerzugriffs. Siehe Einrichten von Rollen für Benutzerkonten.
- **Einrichten von Benutzerkonten**: Alle Service Desk-Benutzer und -Administratoren benötigen authentifizierte Benutzerkonten. Siehe Konfigurieren von Benutzerkonten, LDAP-Authentifizierung und SSO.
- **Anpassen von Ticketinformationen**: Fügen Sie nach Bedarf Eigenschaften wie Ticketkategorien, Status, Auswirkungen und Priorität hinzu. Geben Sie zusätzliche Informationen an, die in den Tickets enthalten sein sollen. Siehe Konfigurieren der Ticketeinstellungen.
- **Anpassen von E-Mail-Vorlagen**: Konfigurieren Sie die Service Desk-E-Mail-Vorlagen, die zum Senden von Benachrichtigungen verwendet werden. Siehe E-Mail-Vorlagen konfigurieren.
- **Einrichten von E-Mail-Benachrichtigungen**: Konfigurieren Sie die Events, die das Senden von E-Mail-Benachrichtigungen auslösen. Siehe Konfigurieren der E-Mail-Einstellungen.
- **Einrichten von Warteschlangen und Prozessen**:
  - **Warteschlangen**: Verwenden Sie Warteschlangen, um Tickets zu organisieren oder verschiedene Aufgaben wie beispielsweise Hardware- und Softwareaufgaben zu bearbeiten. Siehe Konigurieren von Service Desk-Ticketwarteschlangen.
  - **Prozesse:** Verwenden Sie Prozesse, um Beziehungen zwischen Tickets zu definieren, die Teil von wichtigen oder fortlaufenden Aufgaben sind. Sie können auch Beziehungen einrichten, indem Sie innerhalb von Tickets über- und untergeordnete Beziehungen verwenden. Siehe Verwenden von Service Desk-Prozessen.
- **Einrichten von Ticketregeln**: Konfigurieren Sie die Regeln, die Service Desk verwendet, um Tickets zu verarbeiten. Siehe Informationen zu Ticketregeln
- **Entscheidung, ob Benutzer zu einer Zufriedenheitsumfrage aufgefordert werden sollen**: Siehe Verwenden der Zufriedenheitsumfrage.
- **Konfigurieren der Geschäftszeiten und Feiertage**: Definieren Sie die Geschäftszeiten und die Feiertage Ihres Unternehmens. Diese Zeiten und Feiertage werden verwendet, um Fälligkeitsdaten von Tickets und Verletzungen von Service Level-Vereinbarungen (SLA) zu bestimmen. Siehe Konfigurieren der Service Desk-Geschäftszeiten und -Feiertage.
- **Konfigurieren von Service Level-Vereinbarungen (SLAs)**: Konfigurieren Sie die SLAs, die bei der Berechnung von Ticket-Fälligkeitsdaten und SLA-Verletzungen verwendet werden. Siehe Service Level-Vereinbarungen aktivieren.
- **KonfigurierenBenutzerkonsole der Startseiteneinstellungen**: Ändern Sie das Logo und die Willkommensnachricht auf der Startseite der **Benutzerkonsole**. Darüber hinaus können Sie

Schnellaktionen und Ankündigungen sowie Links zu Knowledge-Base-Artikeln, Tickets und andere Elemente anzeigen oder ausblenden. Siehe:

- Benutzerkonsole-Logo und Anmeldetext auf Verwaltungsebene ändern
- Interaktive Schaltflächen und Widgets auf der Startseite der Benutzerkonsole ein- oder ausblenden
- Benutzerkonsole-Ankündigungen hinzufügen, bearbeiten, ausblenden oder löschen
- Benutzerdefinierte Links auf der Startseite der Benutzerkonsole hinzufügen, bearbeiten oder löschen
- Links zu Knowledge Base-Artikeln auf der Startseite der Benutzerkonsole ein- oder ausblenden

Importieren von Tickets aus einem anderen System

Sie können Tickets aus einem anderen System importieren, indem Sie vorbereitete CSV-Dateien (durch Trennzeichen getrennte Datei) verwenden. Exportieren Sie Ihre Tickets zunächst in eine CSV-Datei, und importieren Sie dann mithilfe des Assistenten zum *Importieren von Tickets* diesen Inhalt in die Appliance. Der Assistent validiert die importierten Daten. Für bestimmte Felder müssen vordefinierte Formate verwendet werden, um zu verhindern, dass zugehörige Datensätze abgelehnt werden.

1. Exportieren Sie Ihre Ticketdaten in eine CSV-Datei.
2. Rufen Sie den Assistenten *für den Import von Tickets* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Service Desk** und anschließend auf **Konfiguration**.
   c. Klicken Sie im Fensterbereich **Konfiguration** im Abschnitt *Import* auf **Tickets importieren**.
3. Geben Sie im *Assistenten für den Ticketimport* auf der Seite *Select Ticket Import File (Ticket-Importdatei auswählen)* die CSV-Datei und die zugehörigen Optionen nach Bedarf an.

   TIPP: Sie können den Status des letzten Ticket-Imports überprüfen, indem Sie auf den Link unten auf der Seite klicken.

   a. Klicken Sie im Abschnitt *Datei hochladen (.csv)* auf **Datei auswählen**, und wählen Sie die CSV-Datei aus, die Ticketdaten enthält, die Sie importieren möchten.
   b. Wenn Ihre CSV-Datei über eine Kopfzeile verfügt, aktivieren Sie das Kontrollkästchen **Kopfzeile in Datei**.
   c. Geben Sie im Abschnitt *Importing to (Importieren nach)* die Warteschlange und Vorlage an, in die Sie Ihre Ticketdaten importieren möchten.
   d. Wenn Ihre Ticket-Daten einen oder mehrere Benutzer enthalten, die nicht in der Appliance-Datenbank vorhanden sind, und Sie diese beim Importieren der Tickets automatisch erstellen möchten, aktivieren Sie das Kontrollkästchen **Auto Create User (Benutzer automatisch erstellen)**.
   e. Klicken Sie auf **Weiter**.
4. Ordnen Sie im *Assistenten für den Ticketimport* auf der daraufhin angezeigten Seite *Feldzuordnung* die Felder der Ticketvorlage den in der CSV-Datei angegebenen Ticketfeldern zu.

   Beachten Sie beim Zuordnen von Ticketfeldern die folgenden Richtlinien:

   - Um ein Ticketfeld anzugeben, klicken Sie auf die Spalte **CSV-Felder**, und wählen Sie den entsprechenden Wert aus.
   - Für **Kommentarfelder** muss die folgende Syntax verwendet werden: `"<datetime>";"<user_name>";"<comment>";"<owners_only_flag>"`. Mehrere

Kommentare in einem einzelnen **Kommentarfeld** müssen mit `|EOL|` getrennt werden. Beispiel: `"01/01/2019 10:10";"Admin";"Dies ist ein Kommentarbeispiel";"J"|EOL|"01/02/2019 11:20";"Benutzer A";"Dies ist ein Kommentarbeispiel 2";"J"|EOL|"01/02/2019 12:00";"Admin";"Dies ist ein Kommentarbeispiel 3";"J"|EOL|`. Alternativ können Sie den primären Schlüssel verwenden, um mehrere Spalteneinträge im selben Ticketfeld zu kombinieren. Siehe Table 33 und Table 34.

- Für Felder vom Typ **Work Detail (Aufgabendetails)** muss die folgende Syntax verwendet werden: `"<user_name>";"<start_datetime>";"<end_datetime>";"[adjustment_time];[<note>]`. Mehrere Kommentare in einem einzelnen **Kommentarfeld** müssen mit `|EOL|` getrennt werden. Beispiel: `"Admin";"01/01/2019 08:10";"01/01/2019 10:30";"10";"Aufgabenhinweis"|EOL|"Benutzer B";"01/01/2019 11:20";"01/01/2019 12:30"`. Alternativ können Sie den primären Schlüssel verwenden, um mehrere Spalteneinträge im selben Ticketfeld zu kombinieren. Siehe Table 33 und Table 34.
- In einem **Kategoriefeld**, das Unterkategorien enthält, müssen Unterkategorien durch Doppelpunkte "::" getrennt werden. Beispiel: `Hardware::Drucker::Papier`. Wenn der Import Kategorien erkennt, die auf der Appliance bisher nicht vorhanden sind, werden diese Datensätze automatisch abgelehnt.
- Die Felder **Auswirkung** und **Priorität** müssen gültige Inhalte enthalten, die auf der Appliance vordefiniert sind.
- Benutzernamenfelder (z. B. **Absender**) akzeptieren die E-Mail-Adresse des Benutzers, den Benutzernamen, die Benutzer-ID und den Anzeigenamen. Mehrere Datensätze mit demselben Benutzernamen werden automatisch abgelehnt.
- Die Inhalte benutzerdefinierter Felder, die ein bestimmtes Datenformat erwarten (z. B. Links), werden überprüft und abgelehnt, wenn die Daten ungültig sind.
- Geben Sie in der Spalte **PS** an, ob eine Zeile ein primärer Schlüssel für die Datensätze ist. Alle Datensätze, die den gleichen Wert der Spalte haben, die als primärer Schlüssel markiert ist, werden zu einem einzigen Service Desk-Ticket zusammengefasst. Wenn Sie beispielsweise die Spalte **Titel** als Primärschlüssel für die Tickettabelle markieren und alle Ihre Datensätze in der CSV-Datei die exakt gleiche **Titelspalte** haben (z. B. *Mein Ticket*), führt der Import dazu, dass ein einzelnes Service Desk-Ticket erstellt wird, bei dem mehrere Einträge in derselben Spalte zusammengefasst werden. Alternativ können Sie beim Importieren der Spalten *Kommentar* und *Work Detail (Arbeitsdetails)* die Einträge mit `|EOL|` trennen. Die folgenden Beispiele zeigen Ihnen, wie Sie Ihre CSV-Eingabedatei strukturieren, wenn Sie mehrere Einträge in demselben Ticketfeld kombinieren möchten, entweder mithilfe der `|EOL|`-Trennzeichen (nur Spalten *Kommentar* und *Work Detail (Aufgabendetails)*) oder der Einstellung für den primärer Schlüssel (PS) (beliebige Spalte).

Beispiel: Mehrere Spalteneinträge mit |EOL|-Trennzeichen kombinieren (nur Spalten "Kommentar" und "Work Detail" (Aufgabendetails)

Titel	Status	Priorität	Besitzer	Kommentar
Titel A	Neu	Mittel	Admin	"6/15/2021 3:15:44 Kommentar AAA" |EOL| "6/17/2021 5:17:25 Kommentar BBB" |EOL| "6/19/2021 7:21:42 Kommentar CCC" |EOL|
Titel B	abgeschlossen	Hoch	Admin	„7/21/2021 2:18:31 Kommentar DDD" |EOL|

Titel	Status	Priorität	Besitzer	Kommentar
				"6/17/2021 04:56:56 Kommentar EEE" |EOL| "6/19/2021 06:28:32 Kommentar FFF" |EOL|

HINWEIS: Das `|EOL|`-Trennzeichen weist den Assistenten an, diese Einträge in einem einzigen *Kommentarfeld* zu kombinieren. Es besteht keine Notwendigkeit, die Spalte *Titel* als Primärschlüssel (*PS*) zu deklarieren. Die gleiche Syntax gilt für den Inhalt der Spalte *Work Detail (Aufgabendetails)*.

Beispiel: Kombinieren mehrere Spalteneinträge mithilfe der Primärschlüssel-Einstellung

Titel	Status	Priorität	Besitzer	Kommentar
Titel A	Neu	Mittel	Admin	"6/15/2021 3:15:44 Kommentar AAA"
Titel A				"6/17/2021 5:17:25 Kommentar BBB"
Titel A				"6/19/2021 7:21:42 Kommentar CCC"
Titel B	abgeschlossen	Hoch	Admin	"7/21/2021 2:18:31 Kommentar DDD
Titel B				"6/17/2021 04:56:56 Kommentar EEE"
Titel B				"6/19/2021 06:28:32 Kommentar FFF"

HINWEIS: Wenn Sie die Spalte *Titel* als Primärschlüssel (PS) deklarieren, werden alle Einträge mit demselben *Titel* (*Titel A* und *Titel B*) in einem einzigen *Kommentarfeld* zusammengefasst. Es sind keine `|EOL|`-Trennzeichen erforderlich. Der gleiche Mechanismus gilt auch für andere Spalten, einschließlich *Work Detail (Aufgabendetails)*.

- Die **PS**-Einstellung kann auch verwendet werden, um ein bestehendes Ticket zu aktualisieren. Sie haben beispielsweise *Ticket A* mit den in Table 35aufgeführten Daten hochgeladen. Sie können es leicht ersetzen, indem Sie eine aktualisierte CSV-Datei hochladen, die in Table 36 beschrieben ist, aber Sie müssen die Spalte *Titel* in den Einstellungen als primären Schlüssel (**PS**) festlegen:

Beispiel: Ursprüngliche CSV-Daten

Titel	Status	Priorität	Besitzer
Titel A	Neu	Hoch	Benutzer A

Beispiel: Aktualisierte CSV-Daten

Titel	Priorität	Besitzer
Titel A	Niedrig	Benutzer B

- Klicken Sie abschließend auf **Vorschau**.

5. Bestätigen Sie auf der angezeigten *Bestätigungsseite*, dass die Daten, die Sie importieren möchten, gültig sind.
   a. Prüfen Sie die folgenden Abschnitte:
   - **Einzufügende Datensätze**: Listet alle Ticketdatensätze aus der CSV-Datei auf, die als Service Desk-Tickets erstellt werden sollen.
   - **Datensätze für Aktualisierung**: Listet alle Ticketdatensätze aus der CSV-Datei auf, die vorhandene Service Desk-Tickets aktualisieren sollen.
   - **Datensätze abgelehnt**: Listet alle Ticketdatensätze aus der CSV-Datei auf, die aufgrund von Fehlern nicht als Service Desk-Tickets erstellt werden. Für jeden abgelehnten Datensatz gibt die Spalte *Grund* in diesem Abschnitt die Ursache des Fehlers an. Das zugehörige Ticketfeld wird rot markiert angezeigt. Überprüfen Sie den Inhalt dieses Felds, um das Problem besser zu verstehen. Wenn Sie beispielsweise Benutzer in Ihrer CSV-Datei enthalten sind, die nicht auf der Appliance vorhanden sind und das Kontrollkästchen **Auto Create User (Benutzer automatisch erstellen)** nicht aktiviert haben, wird für jeden dieser Benutzer ein Fehler ausgegeben. Sie können alle Fehler beheben, indem Sie die CSV-Importdatei bearbeiten oder die entsprechenden Importoptionen auf der Seite *Select Ticket Import File (Ticket-Importdatei auswählen)* ändern.

   b. Wenn Sie bereit sind, mit dem Import der Ticketdaten fortzufahren, klicken Sie auf **Importieren**.

   HINWEIS: Nachdem Sie mit dem Import begonnen haben, kann der Vorgang nicht gestoppt oder zurückgesetzt werden. Sie können jedoch alle Tickets löschen, sobald der Import abgeschlossen ist.

   Die Seite *Import Tickets - Status (Tickets importieren – Status)* wird angezeigt und gibt an, dass die Ticketdatensätze importiert werden. Die Zeit, die bis zum Abschluss des Importvorgangs erforderlich ist, hängt von der Menge der importierten Ticketdaten ab. Wenn Sie fertig sind, werden Sie in der Zeile *Status* über das Ergebnis des Importvorgangs informiert. Wenn während des Imports Fehler festgestellt werden, wird dies in der Zeile *Fehleinträge* angezeigt. Klicken Sie auf **Details anzeigen**, um weitere Informationen zu erhalten (falls zutreffend).

6. Wenn Sie mit dem Ergebnis des Imports zufrieden sind und keine zusätzlichen Datensätze importieren müssen, klicken Sie auf **Abgeschlossen**. Um ggf. weitere Tickets zu importieren, klicken Sie auf **Mehr importieren**, und wiederholen Sie den Importvorgang.

Konfigurieren der Service Desk-Geschäftszeiten und -Feiertage

Sie können Geschäftszeiten und Feiertage konfigurieren, um Service Level-Vereinbarungen (Service Level Agreements, SLAs) in Ihren Service Desk-Warteschlangen effektiv zu verfolgen und zu erfüllen. Wenn die Organisationskomponente für Ihre Appliance aktiviert ist, konfigurieren Sie Geschäftszeiten und Feiertage für jede Organisation separat.

Nach der Konfiguration der Geschäftszeiten und Feiertage müssen Sie die SLA-Einstellungen in jeder Service Desk-Ticketwarteschlange aktivieren, damit diese Geschäftszeiten und Feiertage verwendet werden.

Service Desk-Geschäftszeiten konfigurieren

Sie können den Service Desk so konfigurieren, dass bei der Berechnung von Fälligkeitsdaten für Tickets die Geschäftszeiten berücksichtigt werden. Wenn Sie mehrere Organisationen haben, können Sie die Geschäftszeiten für jede Organisation separat konfigurieren.

Nachdem Sie die Service Desk-Geschäftszeiten konfiguriert haben, müssen Sie Ticketwarteschlangen in den entsprechenden SLA-Einstellungen (Service Level Agreement, Service Level-Vereinbarung) so konfigurieren, dass diese Zeiten verwendet werden.

1. Rufen Sie die Seite *Geschäftszeiten* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Service Desk** und anschließend auf **Konfiguration**.
   c. Klicken Sie im Fensterbereich **Konfiguration** im Abschnitt *Geschäftszeiten und Feiertage* auf **Geschäftszeiten festlegen**.
2. Geben Sie für jeden Wochentag die Geschäftsstunden anhand der Start- und Endzeit an, indem Sie das Kontrollkästchen **24 Stunden geöffnet** oder das Kontrollkästchen **Abgeschlossen** aktivieren.
3. Klicken Sie auf **Speichern**.

Konfigurieren Sie Warteschlangen für die Verwendung von Geschäftszeiten in SLAs. Siehe Ticketwarteschlangen konfigurieren.

Service Desk-Feiertage konfigurieren

Sie können den Service Desk so konfigurieren, dass bei der Berechnung von Fälligkeitsdaten für Tickets die Unternehmensfeiertage berücksichtigt werden. Wenn Sie mehrere Organisationen haben, können Sie den Feiertagszeitplan für jede Organisation separat konfigurieren.

Nachdem Sie die Service Desk-Feiertage konfiguriert haben, müssen Sie in den entsprechenden SLA-Einstellungen (Service Level Agreement, Service Level-Vereinbarung) aktivieren, dass Ticketwarteschlangen diese Feiertage verwenden.

1. Rufen Sie die Seite *Feiertage* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Service Desk** und anschließend auf **Konfiguration**.
   c. Klicken Sie im Fensterbereich **Konfiguration** im Abschnitt *Geschäftszeiten und Feiertage* auf **Feiertage festlegen**.
2. Klicken Sie auf **Feiertag hinzufügen**, um der Liste einen neuen Feiertag hinzuzufügen. Klicken Sie auf die Schaltfläche **Bearbeiten** neben einem Feiertag, um ihn zu bearbeiten: . Klicken Sie neben einem Feiertag auf die Schaltfläche **Löschen**, um ihn zu entfernen: . Die Feiertage in der Liste können mithilfe der Dropdown-Liste **Nach Jahr filtern** nach dem Jahr gefiltert werden.
3. Klicken Sie auf **Speichern**.

Konfigurieren Sie Warteschlangen für die Verwendung von Feiertagen in SLAs. Siehe Ticketwarteschlangen konfigurieren.

Konfigurieren von Service Level-Vereinbarungen

Service Level-Vereinbarungen (Service Level Agreements, SLAs) sind die Regeln, die zur Berechnung der erwarteten Auflösungszeit oder der Fälligkeitsdaten für Service-Desk-Tickets basierend auf der Ticketpriorität verwendet werden.

Sie können die erwartete Auflösungszeit für jede Ticketpriorität festlegen und aktivieren, dass die SLAs die definierten Geschäftszeiten und Feiertage bei der Berechnung von Fälligkeitsdaten berücksichtigen. Wenn für Tickets mit der Priorität **Niedrig** eine Auflösungszeit von zwei Tagen festgelegt wurde und ein Ticket mit dieser Priorität an einem Tag vor einem Feiertag eingeht, wird der Feiertag bei der Berechnung des Fälligkeitsdatums von der zweitägigen Auflösungszeit ausgeschlossen.

Darüber hinaus wird bei überfälligen Tickets eine E-Mail an die im E-Mail-Ereignis „SLA-Verstoß" festgelegten E-Mail-Adressen versendet, sofern Benachrichtigungen und E-Mail-Ereignisse aktiviert sind. Die Häufigkeit der E-Mail-Benachrichtigungen wird in den SLA-Einstellungen konfiguriert und die Benachrichtigungen werden gemäß diesem Intervall gesendet. Dies gilt auch, wenn das Intervall Zeitpunkte außerhalb der Geschäftszeiten bzw. an Feiertagen enthält.

Service Level-Vereinbarungen aktivieren

Service Level-Vereinbarungen (SLAs) definieren die für die Bearbeitung und Lösung eines Tickets zulässige Zeit in jeder Warteschlange. Wenn Sie mehrere Service Desk-Warteschlangen haben, können Sie die SLA-Einstellungen für jede Warteschlange einzeln anpassen.

SLAs basieren auf den in der Warteschlange definierten Prioritätswerten. Deshalb sollten diese Werte vor der SLA-Konfiguration festgelegt werden. Siehe Ticketprioritätswerte anpassen. Auch können SLAs Geschäftszeiten und Feiertage nur dann abdecken, wenn diese Stunden und Feiertage definiert wurden. Siehe Konfigurieren der Service Desk-Geschäftszeiten und -Feiertage.

1. Rufen Sie die Seite *Warteschlangen-Detail* des Service Desks auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Service Desk** und anschließend auf **Konfiguration**.
   c. Klicken Sie im Fensterbereich **Konfiguration** auf **Warteschlangen**.
   d. Führen Sie zum Anzeigen der Seite *Warteschlangen-Detail* einen der folgenden Schritte aus:
   - Klicken Sie auf den Namen einer Warteschlange.
   - Wählen Sie **Aktion auswählen** > **Neu**.
2. Scrollen Sie nach unten zum Abschnitt *Service Level-Vereinbarung*. Für jeden für die Warteschlange definierten Prioritätswert wird eine Zeile angezeigt. Siehe Ticketprioritätswerte anpassen.
3. Geben Sie für jede Priorität – **Hoch**, **Mittel** und **Niedrig** – die folgenden Einstellungen an:

Option	Beschreibung
Aktiviert	Ob die SLA für die Priorität aktiviert ist. Wählen Sie das Kontrollkästchen aus, um die SLA zu aktivieren. Wählen Sie das Kontrollkästchen ab, um die SLA zu deaktivieren.

Option	Beschreibung
	HINWEIS: Wenn die Service Level-Vereinbarung für eine Priorität aktiviert wird, wird das Ticket-Fälligkeitsdatum automatisch auf Grundlage der für die Priorität festgelegten Auflösungszeit berechnet. Jeder Benutzer mit der Berechtigung zum Ändern des Felds DUE_DATE kann das automatisch berechnete Datum überschreiben.
Auflösungszeit	Die Zeit in Stunden oder Minuten für die aktivierte Priorität. Dieser Zeitraum wird verwendet, um das Fälligkeitsdatum und die Fälligkeitszeit eines Tickets automatisch basierend auf dem Datum und der Uhrzeit der Ticketübermittlung zu berechnen.
Geschäftszeiten/Feiertage verwenden	Ob die konfigurierten Geschäftszeiten und Feiertage bei der Berechnung der Ticket-Fälligkeitsdaten für jede Priorität verwendet werden sollen. Aktivieren Sie die Kontrollkästchen, um diese Einstellungen zu verwenden. Siehe Konfigurieren der Service Desk-Geschäftszeiten und -Feiertage.
Benachrichtigungswiederholung	Die Zeit in Stunden oder Minuten, zu dem E-Mail-Benachrichtigungen gesendet werden sollen. Die E-Mail-Benachrichtigung wird wiederholt bzw. erneut gesendet, wenn ein Ticket zum Fälligkeitsdatum noch nicht gelöst wurde. Die E-Mail wird an die im E-Mail-Ereignis für SLA-Verstöße angegebenen Benutzer gesendet, sofern diese Einstellung im Abschnitt E-Mail bei Ereignissen konfiguriert wurde. Siehe E-Mail-Auslöser und E-Mail-Vorlagen konfigurieren. **HINWEIS:** Um nur eine E-Mail-Benachrichtigung ohne Wiederholung zu senden, geben Sie "0" ein.

4. Klicken Sie auf **Speichern**.

Konigurieren von Service Desk-Ticketwarteschlangen

Service Desk-Tickets werden in Warteschlangen in der Appliance gespeichert. Die meisten Organisationen benötigen nur eine Ticketwarteschlange. Sie können diese eine Warteschlange anpassen oder je nach Bedarf weitere Warteschlangen erstellen und verwalten.

Siehe Verwalten von Warteschlangen für Service-Desk-Tickets.

Ticketwarteschlangen konfigurieren

Sie können die Einstellungen von Ticketwarteschlangen nach Bedarf anpassen.

1. Rufen Sie die Seite *Warteschlangen-Detail* des Service Desks auf:

a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://appliance_hostname/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.

b. Klicken Sie in der linken Navigationsleiste auf **Service Desk** und anschließend auf **Konfiguration**.

c. Klicken Sie im Fensterbereich **Konfiguration** auf **Warteschlangen**.

d. Führen Sie zum Anzeigen der Seite *Warteschlangen-Detail* einen der folgenden Schritte aus:

- Klicken Sie auf den Namen einer Warteschlange.
- Wählen Sie **Aktion auswählen** > **Neu**.

2. Legen Sie die folgenden Einstellungen fest:

Feld	Beschreibung
Name	Der Name der *Service Desk*-Warteschlange. Dieser Name wird im Feld *Von* angezeigt, wenn Benutzer E-Mail-Nachrichten vom Service Desk erhalten.
E-Mail-Adresse	Eine voll qualifizierte E-Mail-Adresse für den Server. Benutzer antworten normalerweise nicht an diese Adresse. Wenn Sie Benutzern die Beantwortung von E-Mails der Appliance ermöglichen möchten, geben Sie im Feld *Alternative E-Mail-Adresse* eine E-Mail-Adresse ein.
Ticket Number Prefix (Präfix Für Ticketnummer)	Geben Sie ein benutzerdefiniertes Ticket-Präfix für diese Warteschlange an. Sie können für jede Warteschlange ein anderes Präfix verwenden, um Ihren Service Desk-Workflow zu organisieren und diese mit entsprechenden Kategorien zu verknüpfen, wie z. B. HD für Helpdesk oder REQ für Hardware- und Softwareanforderungen.
Alternative E-Mail-Adresse	**Support@meinedomain.com** Die primäre E-Mail-Adresse, an die die Benutzer E-Mails senden. Die Appliance verwendet diese Adresse, um E-Mails vom Service Desk zu senden. Bestätigen Sie, dass der Domänenname für Ihren E-Mail-Service korrekt ist. **HINWEIS:** Diese gültige E-Mail-Adresse unterliegt den gleichen Spam- und Sicherheitsrisiken wie andere E-Mail-Adressen.

3. **Optional**: Konfigurieren Sie die SMTP-/POP3-Servereinstellungen. Klicken Sie auf **Warteschlangen-E-Mail-Einstellungen konfigurieren** und legen Sie die SMTP/POP3-Optionen auf der Seite *Service Desk Warteschlange-E-Mail-Einstellungen* nach Bedarf fest. Siehe Warteschlangen-spezifische E-Mail-Einstellungen konfigurieren.
4. Klicken Sie auf **Speichern**, um die Warteschlange zu erstellen und zusätzliche Einstellungen zu konfigurieren.
5. Geben Sie *Benutzereinstellungen* an:

Feld	Beschreibung
Alle Benutzer als Absender zulassen	Erlaubt jedem Benutzer der Appliance das Übermitteln von Tickets über diese Service Desk-Warteschlange.
Absender nach Label beschränken	Ausschließlich labelbasierte Auswahl von Absendern. Diese Option ist nur verfügbar, wenn **Alle Benutzer als Absender zulassen** nicht ausgewählt ist.
Alle Benutzer als genehmigende Person zulassen	Erlaubt allen Benutzern der Appliance das Genehmigen von Tickets über diese Service Desk-Warteschlange.
Genehmigende Personen nach Label beschränken	Ausschließlich labelbasierte Auswahl von genehmigenden Personen. Diese Option ist nur verfügbar, wenn **Alle Benutzer als genehmigende Person zulassen** nicht ausgewählt ist.
Besitzerlabel	Wenn Sie allen Benutzern ermöglichen möchten, Tickets zu genehmigen, wählen Sie **Alle Benutzer als Genehmiger zulassen** aus. Identifizieren Sie die Benutzer, die Tickets besitzen und verwalten dürfen (üblicherweise die IT-Mitarbeiter). Es muss ein Ticketbesitzer festgelegt werden, der für die Verwaltung des Tickets über seinen Lebenszyklus hinweg verantwortlich ist. Klicken Sie dazu auf **Verknüpfte Labels verwalten**. Wählen Sie in dem nun angezeigten Dialogfeld *Labels auswählen* ein oder mehrere Labels aus, die mit den Benutzern verknüpft sind, die Sie als Ticketbesitzer auswählen möchten. Schließen Sie das Dialogfeld.
E-Mails von unbekannten Benutzern annehmen	Ermöglicht unerkannten Benutzern Tickets zu erstellen. Wenn diese Option in der Warteschlangenkonfiguration aktiviert ist, kann für das Feld *Absender* eines Tickets eine beliebige E-Mail-Adresse angegeben werden. Der Absender wird der Appliance als Benutzer mit der Rolle *Nur Benutzerkonsole* hinzugefügt. Sie enthält standardmäßig die Berechtigung, Service Desk-Tickets zu erstellen, anzuzeigen oder zu ändern und ausschließlich über die **Benutzerkonsole** mit der Appliance zu interagieren. Sie können die Berechtigungsstufe für diese und andere Rollen nach Bedarf anpassen. Weitere Informationen hierzu finden Sie unter Einrichten von Rollen für Benutzerkonten. Wenn die Option deaktiviert ist, ist der oben genannte Vorgang nur möglich, wenn die E-Mail-Adresse des Absenders bereits mit einem Service Desk-Benutzerkonto verknüpft ist.

Feld	Beschreibung
Löschen von Tickets zulassen	Erlaubt Ticketbesitzern und Administratoren das Löschen von Tickets. Diese Einstellung ist nützlich, wenn Sie nicht möchten, dass Mitarbeiter Tickets löschen können. Sie können dieses Kontrollkästchen von Zeit zu Zeit deaktivieren, um alte Tickets zu entfernen, und es anschließend wieder aktivieren.
Übergeordnetes Ticket darf untergeordnete Tickets schließen	Ermöglicht dem System das automatische Abschließen untergeordneter Tickets beim Abschließen von übergeordneten Tickets.
Benutzern mit einer Administratorrolle gestatten, Tickets in dieser Warteschlange zu lesen und zu bearbeiten (nur **Administratorkonsole**)	Gewährt allen Benutzern mit **Administrator**rolle Lese- und Schreibberechtigungen.
Standardmäßige Ticket-Besitzerkommentare für die Anzeige "Nur Besitzer"	Automatische Aktivierung des Kontrollkästchens *Nur Besitzer*, wenn Kommentare zu Tickets hinzugefügt werden.
Ticket-Konfliktwarnung für Ticket-Eigentümer aktivieren	Zeigt ein Dialogfeld für Administratoren und Ticketbesitzer, das Konflikte zwischen abgesendeten Änderungen und von anderen Benutzern abgesendeten Änderungen zusammenfasst. Wenn Administratoren und Ticketbesitzer auf der Seite *Details zum Ticket* auf **Speichern** oder **Änderungen übernehmen** klicken, wird das Dialogfeld angezeigt, wenn das Ticket von anderen Benutzern bearbeitet und gespeichert wurde, während es zur Bearbeitung geöffnet war. Dies ermöglicht Administratoren und Ticketbesitzern im Konfliktfall zu entscheiden, ob sie ihre Änderungen verwerfen oder die Änderungen von anderen Benutzern überschreiben wollen. **HINWEIS:** Standardmäßig ist diese Warnung bei neuen Warteschlangen aktiviert und bei Warteschlangen deaktiviert, die mit der Appliance bis Version 6.3 erstellt wurden. Das Dialogfeld wird nur dann angezeigt, wenn andere Benutzer das Ticket geändert haben. Nur Administratoren und Ticketbesitzer erhalten diese Warnung. Für andere Benutzer wird das Dialogfeld nicht angezeigt. **HINWEIS:** In dem Dialogfeld sind alle von anderen Benutzern durchgeführten Änderungen zusammengefasst. Die Änderungen des aktuellen Benutzers werden aber nur dann zusammengefasst, wenn ein Konflikt mit von anderen Benutzern vorgenommenen Änderungen besteht.
Managern erlauben, die Tickets ihrer Mitarbeiter anzuzeigen und zu kommentieren	Ermöglicht Manager-Konten das Anzeigen und Bearbeiten von Kommentaren in Tickets, die von ihren Mitarbeitern eingesendet wurden. Weitere

Feld	Beschreibung
	Informationen hierzu finden Sie unter Ticket-Kommentare anzeigen.
Ticket-CC-Liste erlauben, das Ticket anzuzeigen und zu kommentieren	Erlaubt Benutzern, auf der Ticket-CC-Liste Kommentare zum Ticket hinzuzufügen.
Alle Benutzer zu Ticket CC-Liste hinzufügen, die einen Kommentar zu einem Ticket abgeben	Fügt alle Benutzer, die einen Kommentar zu einem Ticket abgeben, zu einer CC-Liste für dieses Ticket hinzu, damit sie bei weiteren Änderungen an dem Ticket jedes Mal per E-Mail benachrichtigt werden.
Alle Benutzer können ihre eigenen Kommentare bearbeiten/löschen (einschließlich Anhänge)	Erlaubt alle Benutzern, ihre eigenen Kommentare, einschließlich Dateianhängen, zu bearbeiten oder zu entfernen.
Benutzerlabel	Damit bestimmte Benutzer ihre eigenen Kommentare und Anhänge mit Labels bearbeiten oder löschen können, klicken Sie auf **Verknüpfte Labels verwalten**. Wählen Sie in dem nun angezeigten Dialogfeld *Labels auswählen* ein oder mehrere Labels aus, die mit den Benutzern verknüpft sind, die Sie auswählen möchten. Schließen Sie das Dialogfeld.
Alle Techniker können die von anderen eingegebenen Kommentare bearbeiten/ löschen(einschließlich Anhänge)	Erlaubt allen Technikern, Kommentare, die von anderen hinzugefügt wurden, einschließlich Dateianhängen, zu bearbeiten oder zu entfernen.
Techniker-label	Damit bestimmte Techniker ihre eigenen Kommentare und Anhänge mit Labels bearbeiten oder löschen können, klicken Sie auf **Verknüpfte Labels verwalten**. Wählen Sie in dem nun angezeigten Dialogfeld *Labels auswählen* ein oder mehrere Labels aus, die mit den Technikern verknüpft sind, die Sie auswählen möchten. Schließen Sie das Dialogfeld.
Einschränkungen für Ticketanhänge	Geben Sie an, wie Sie Einschränkungen für Dateianhänge ggf. handhaben möchten. • **Keine**: Benutzern erlauben, beliebige Dateitypen als Anhänge hinzuzufügen. • **Nur Bilder zulassen**: Nur Bilddateien dürfen als Anhänge hinzugefügt werden. • **Benutzerdefiniert**: Geben Sie die Dateierweiterungen an, die Sie als Anhänge zulassen möchten. Sie können auch alle Dateien ohne Erweiterungen zulassen. • **Alle Anhänge verhindern**: Benutzer können keine Dateianhänge hinzufügen.

6. Wählen Sie im Abschnitt *Archiveinstellungen* die Einstellungen für die Ticketarchivierung aus. Klicken Sie auf den Link **Einstellungen**, um die Ticketarchivierung zu aktivieren.

HINWEIS: Wenn die Ticketarchivierung abgeschaltet ist, siehe Ticketarchivierung aktivieren.

Option	Beschreibung
Archiv geschlossen für Tickets älter als	Das Alter der zu archivierenden Tickets. Wenn Sie z. B. **3 Monate** auswählen, werden die Tickets nach dem Ablauf von drei Monaten nach ihrer Eröffnung archiviert. Um zu verhindern, dass in der Warteschlange enthaltene Tickets archiviert werden, wählen Sie **Nie** aus. Archivierte Tickets können gegebenenfalls in der Warteschlange wiederhergestellt werden. Siehe Archivierte Tickets wiederherstellen.
Löschen von archivierten Tickets älter als	Das Alter von Tickets, die dauerhaft aus dem Archiv entfernt werden sollen. Wenn Sie z. B. **6 Monate** auswählen, werden archivierte Tickets nach dem Ablauf von sechs Monaten nach ihrer Eröffnung aus dem Archiv gelöscht. Um zu verhindern, dass in der Warteschlange enthaltene Tickets aus dem Archiv gelöscht werden, wählen Sie **Nie** aus. Gelöschte Tickets können nicht in der Warteschlange wiederhergestellt werden.

7. Wählen Sie im Abschnitt *Standardwerte für Tickets* die Standardwerte für neue Tickets aus. Beispiel:
   - **Kategorie**: Software
   - **Status**: Neu
   - **Auswirkungen**: 1 Person kann nicht arbeiten
   - **Priorität**: Mittel

   HINWEIS: Wenn eines dieser Felder auf der Seite *Felder und Layout anpassen* als Erforderlich gekennzeichnet ist, wird der Standardwert ignoriert und die Benutzer müssen einen Wert aus der Dropdown-Liste auswählen.
8. Wählen Sie im Abschnitt *E-Mail bei Ereignissen* die Kategorien von Benutzern aus, die beim Eintritt der angegebenen Ereignisse E-Mails erhalten. Jede Spalte entspricht einer Art von Service Desk-Benutzer(rolle) und jede Zeile entspricht einem Ticketereignis. Siehe E-Mail-Auslöser konfigurieren.
9. **Optional**: Konfigurieren Sie die *Einstellungen für die Service Level-Vereinbarung*. Hier können Sie Einstellungen für die Service Level-Vereinbarung auf der Grundlage der Ticketpriorität aktivieren. Im aktivierten Zustand werden für das Fälligkeitsdatum des Tickets automatisch die Auflösungszeit, die Geschäftszeiten und Feiertage berücksichtigt. Siehe Konfigurieren von Service Level-Vereinbarungen.
10. Im Abschnitt *Ticketregeln* können Sie Regeln für Tickets in der Warteschlange aktivieren. Sie können vordefinierte Regeln verwenden oder Ihre eigenen Regeln erstellen. Weitere Informationen zur Verwendung und Anpassung der Ticketregeln finden Sie unter Verwenden von Ticketregeln.
11. Klicken Sie auf **Speichern**.

Warteschlangen-spezifische E-Mail-Einstellungen konfigurieren

Sie können die E-Mail-Einstellungen für jede Ticket-Warteschlange einzeln festlegen.

Standardmäßig ist das Service Desk zur Verwendung eines internen SMTP-Servers zum Senden Ticket-bezogener E-Mails konfiguriert. Sie können optional einen externen SMTP-Server verwenden, müssen diesen

jedoch in den Netzwerkeinstellungen der Appliance konfigurieren. Weitere Informationen hierzu finden Sie unter Netzwerkeinstellungen der Appliance ändern.

1. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
2. Rufen Sie die Seite *Service Desk Warteschlange-E-Mail-Einstellungen* auf:
   a. Klicken Sie in der linken Navigationsleiste auf **Service Desk** und anschließend auf **Konfiguration**.
   b. Klicken Sie im Fensterbereich **Konfiguration** im Abschnitt *E-Mail-Konfiguration* auf **Service Desk Warteschlange-E-Mail-Einstellungen konfigurieren**.
   c. Wählen Sie auf der Seite *Service Desk Warteschlange-E-Mail-Einstellungen* eine Warteschlange aus.

   oder:

   a. Klicken Sie in der linken Navigationsleiste auf **Service Desk** und anschließend auf **Konfiguration**.
   b. Klicken Sie im Fensterbereich **Konfiguration** auf **Warteschlangen**.
   c. Klicken Sie rechts neben der E-Mail-Adresse der Warteschlange auf **Einstellungen für Warteschlange konfigurieren**.

   Die Seite *Service Desk Warteschlange-E-Mail-Einstellungen* wird angezeigt.
3. Legen Sie im Bereich *Integrierte E-Mail-Einstellung* die folgenden Optionen fest:

Feld	Beschreibung
E-Mail-Adresse	Eine voll qualifizierte E-Mail-Adresse für den Server. Benutzer antworten normalerweise nicht an diese Adresse. Wenn Sie Benutzern die Beantwortung von E-Mails der Appliance ermöglichen möchten, geben Sie im Feld *Alternative E-Mail-Adresse* eine E-Mail-Adresse ein.
Alternative E-Mail-Adresse	**Support@meinedomain.com** Die primäre E-Mail-Adresse, an die die Benutzer E-Mails senden. Die Appliance verwendet diese Adresse, um E-Mails vom Service Desk zu senden. Bestätigen Sie, dass der Domänenname für Ihren E-Mail-Service korrekt ist. **HINWEIS:** Diese gültige E-Mail-Adresse unterliegt den gleichen Spam- und Sicherheitsrisiken wie andere E-Mail-Adressen.
E-Mails von unbekannten Benutzern annehmen	Ermöglicht unerkannten Benutzern Tickets zu erstellen. Wenn diese Option in der Warteschlangenkonfiguration aktiviert ist, kann für das Feld *Absender* eines Tickets eine beliebige E-Mail-Adresse angegeben werden. Der Absender wird der Appliance als Benutzer mit der Rolle *Nur Benutzerkonsole* hinzugefügt. Sie enthält standardmäßig die Berechtigung, Service Desk-Tickets zu erstellen, anzuzeigen oder zu ändern und ausschließlich über die **Benutzerkonsole**

Feld	Beschreibung
	mit der Appliance zu interagieren. Sie können die Berechtigungsstufe für diese und andere Rollen nach Bedarf anpassen. Weitere Informationen hierzu finden Sie unter Einrichten von Rollen für Benutzerkonten. Wenn die Option deaktiviert ist, ist der oben genannte Vorgang nur möglich, wenn die E-Mail-Adresse des Absenders bereits mit einem Service Desk-Benutzerkonto verknüpft ist.

4. Wählen und konfigurieren Sie die Methode für den Empfang eingehender E-Mails mithilfe der Optionen im Abschnitt *Einstellungen für eingehende E-Mails*.

   - **SMTP-Server für eingehende E-Mails verwenden: Wählen Sie diese Option, wenn Sie einen internen SMTP-Server für eingehende E-Mails verwenden möchten. Sie können die erforderlichen Anmeldeinformationen im Abschnitt** *Outbound Email Setting (Einstellungen für ausgehende E-Mail)* **unten angeben. Siehe 5.**
   - **POP3-Server für eingehende E-Mails verwenden: Wählen Sie diese Option, wenn Sie einen POP3-Server für eingehende E-Mails verwenden möchten. Legen Sie die folgenden Optionen fest:**

Option	Beschreibung
POP3-Server	Geben Sie den Namen des POP3-Servers ein, den Sie für die Warteschlange verwenden möchten. Beispiel: **pop.example.com**.
SSL verwenden	Wählen Sie diese Option, wenn der POP3-Server eine sichere Verbindung verwenden soll.
POP3-Benutzername (E-Mail-Adresse) **POP3-Kennwort**	Geben Sie den Benutzernamen und das Kennwort eines Kontos ein, das Zugriff auf den POP3-Server hat.

   Klicken Sie auf **Verbindung testen**, um die POP3-Konfiguration zu testen. Das Dialogfeld „Verbindungstest POP3“ wird angezeigt und zeigt mehrere Protokollmeldungen mit dem Testergebnis. Wenn der Test erfolgreich ist, geben diese Meldungen beispielsweise an, ob das Benutzerkonto authentifiziert wurde. Sie enthalten zudem die Anzahl der ungelesenen Nachrichten und die Betreffzeile der letzten E-Mail-Nachricht. Wenn der Test fehlschlägt, überprüfen Sie Ihre Konfiguration und probieren es erneut.

   - **IMAP-Server für eingehende E-Mails verwenden: Wählen Sie diese Option, wenn Sie einen IMAP-Server für eingehende E-Mails verwenden möchten. Legen Sie die folgenden Optionen fest:**

Option	Beschreibung
IMAP-Server	Geben Sie den Namen des IMAP-Servers ein, den Sie für die Warteschlange verwenden möchten. Beispiel: **imap.beispiel.de** .
SSL verwenden	Wählen Sie diese Option, wenn der IMAP-Server eine sichere Verbindung verwenden soll.

Option	Beschreibung
IMAP-Server-Benutzername (E-Mail-Adresse) **IMAP-Server-Kennwort**	Geben Sie den Benutzernamen und das Kennwort eines Kontos ein, das Zugriff auf den IMAP-Server hat.

Klicken Sie auf **Verbindung testen**, um die IMAP-Konfiguration zu testen. Das Dialogfeld „Verbindungstest IMAP“ wird mit mehreren Protokollmeldungen und dem Testergebnis angezeigt. Wenn der Test erfolgreich ist, geben diese Meldungen beispielsweise an, ob das Benutzerkonto authentifiziert wurde. Sie enthalten zudem die Anzahl der ungelesenen Nachrichten und die Betreffzeile der letzten E-Mail-Nachricht. Wenn der Test fehlschlägt, überprüfen Sie Ihre Konfiguration und probieren es erneut.

- **Gmail für eingehende E-Mails verwenden: Wählen Sie diese Option, wenn Sie Google Gmail für eingehende E-Mails verwenden möchten. Klicken Sie auf Anmeldeinformationen auswählen.**
  - Um vorhandene Google OAuth-Anmeldeinformationen zu verwenden, wählen Sie diese in der Liste aus.

    HINWEIS: Sie müssen dedizierte Google OAuth-Anmeldeinformationen zum Abrufen von E-Mails erstellen. Sie können beispielsweise nicht dasselbe Konto für den Zugriff auf Chrome-Geräte und das Herunterladen von E-Mails verwenden.

  - Um neue Google OAuth-Zugangsdaten zu erstellen, klicken Sie auf **Anmeldeinformationen hinzufügen**. Das Dialogfeld *Anmeldeinformationen hinzufügen* wird angezeigt. Geben Sie die erforderlichen Optionen an. Weitere Informationen finden Sie unter Hinzufügen und Bearbeiten von Google OAuth-Anmeldeinformationen.
- **Office365 für eingehende E-Mails verwenden: Wählen Sie diese Option, wenn Sie Office 365 für eingehende E-Mails verwenden möchten. Legen Sie die folgenden Optionen fest:**

Option	Beschreibung
Anmeldeinformationen auswählen	• Um vorhandene Office 365 OAuth-Anmeldeinformationen zu verwenden, wählen Sie sie in der Liste aus. • Um neue Office 365 OAuth-Anmeldeinformationen zu erstellen, klicken Sie auf **Anmeldeinformationen hinzufügen**. Das Dialogfeld *Anmeldeinformationen hinzufügen* wird angezeigt. Geben Sie die erforderlichen Optionen an. Weitere Informationen finden Sie unter Microsoft Office 365 OAuth-Anmeldeinformationen hinzufügen und bearbeiten.
Microsoft 365 API Service (Microsoft 365 API-Dienst)	Wählen Sie den entsprechenden Microsoft 365 API-Dienst für Ihre Umgebung aus: • Wählen Sie für eine Azure AD-App in den USA je nach Bedarf eine der folgenden Optionen aus: ◦ **Microsoft 365 GCC**: Sie können auch weiterhin weltweite Endpunkte in Azure nutzen: https://graph.microsoft.com

Option	Beschreibung
	und https://portal.azure.com für die Registrierung verwenden. ◦ **Microsoft 365 GCC High**: Verwenden Sie https://portal.azure.us und https://graph.microsoft.us für die Registrierung. ◦ **Microsoft 365 DoD**: Verwenden Sie https://portal.azure.us und https://dod-graph.microsoft.us für die Registrierung. • Wählen Sie für eine Azure AD-App in Deutschland **Microsoft Office 365 Deutschland**. • Wählen Sie für eine Azure AD-App in China **Microsoft 365 China**.

5. Falls Sie einen externen SMTP-Server für eingehende E-Mails in Verbindung mit dieser Warteschlange verwenden möchten, verwenden Sie die Einstellungen im Abschnitt *Outbound Email Setting (Einstellungen für ausgehende E-Mail)*.
   a. Aktivieren Sie das Kontrollkästchen *Warteschlangen-spezifische SMTP-Einstellungen konfigurieren*.
   b. Legen Sie die folgenden Optionen fest:

Option	Beschreibung
SMTP-Server	Geben Sie den Hostnamen oder die IP-Adresse eines externen SMTP-Servers an, beispielsweise **smtp.gmail.com**. Externe SMTP-Server müssen die anonyme (nicht authentifizierte) Übermittlung ausgehender E-Mails unterstützen. Vergewissern Sie sich, dass es Ihre Netzwerkrichtlinien der Appliance gestatten, den SMTP-Server direkt zu kontaktieren. Der E-Mail-Server muss zudem für die Weiterleitung von E-Mails von der Appliance ohne Authentifizierung konfiguriert sein.
SMTP-Port	Geben Sie die für den externen SMTP-Server zu verwendende Port-Nummer ein. Für Standard-SMTP verwenden Sie Port 25. Für sicheres SMTP verwenden Sie Port 587.
SMTP-Benutzername	Geben Sie den Benutzernamen für ein Konto ein, das Zugriff auf den externen SMTP-Server hat, beispielsweise **Ihr_Kontoname**@gmail.com.
SMTP-Kennwort	Geben Sie das Kennwort für das angegebene Serverkonto ein.

6. Geben Sie im Abschnitt *Outgoing Email Embedded Images Setting (Einstellungen für eingebettete Bilder für ausgehende E-Mails)* an, wie Dateianhänge beim Versenden von Ticketdetails behandelt werden sollen.

Option	Beschreibung
Allow embedded images in emails (Eingebettete Bilder in E-Mails zulassen)	Wählen Sie diese Option aus, wenn Sie Grafikdateien in ticketbezogene E-Mails aufnehmen

Option	Beschreibung
	möchten. Wenn diese Option ausgewählt ist, werden die Grafiken als eingebettete Bilder angezeigt.
Maximum total embedded images limit per email (MB) (Maximale Gesamtanzahl eingebetteter Bilder pro E-Mail (MB))	Geben Sie die maximale Dateigröße aller Bilder zu einem Ticket, die in ticketbezogene E-Mails eingebettet werden können.

7. Wählen Sie auf der Seite *E-Mail-Einstellungen für Service Desk Warteschlange* im Abschnitt *E-Mail bei Ereignissen* die Optionen für das Senden von E-Mails aus, wenn die angegebenen Ereignisse eintreten. Jede Spalte entspricht einer Art von Service Desk-Benutzer(rolle) und jede Zeile entspricht einem Ticketereignis.

Service Desk-Benutzer(rolle)	Beschreibung
Besitzer	Die Person, die das Ticket lösen soll.
Absender	Die Person, deren Problem gelöst werden soll.
Genehmigt von	Die Person, die die Bearbeitung des Tickets genehmigen oder ablehnen kann.
Ticket CC	Eine oder mehrere E-Mail-Adressen, die im Feld *CC* des Tickets gespeichert sind.
Kategorie CC	Eine oder mehrere E-Mail-Adressen, die in der *CC-Liste* des *Kategoriewerts* des Tickets gespeichert sind. Siehe CC-Listen für Ticketkategorien konfigurieren.
Queue-Eigentümer	Ein oder mehrere Eigentümer der Ticketwarteschlange, wie vom Label *Eigentümer* angegeben. Dies gilt nur für die Ereignisse *Neues Ticket per E-Mail* und *Neues Ticket über Portal*.

Wenn ein Ticketereignis eintritt, werden an ausgewählte Rollen oder Benutzer E-Mails gesendet. Wenn Sie z. B. das Kontrollkästchen **Alle Änderungen** in der Spalte *Besitzer* aktivieren, wird bei jeder Ticketänderung eine E-Mail an den Ticketbesitzer gesendet. Für die Auslöser *Kommentar* und *Ticket abgeschlossen* werden sofort E-Mails versendet. Bei anderen Ticketänderungen werden E-Mails jedoch im Abstand von mehreren Minuten versendet, um eine E-Mail-Überlastung zu vermeiden.

HINWEIS: Wenn Benutzer die mobile App KACE GO auf ihrem Smartphone oder Tablet installiert haben, sendet das System Push-Benachrichtigungen für die ausgewählten Service Desk-Ticketereignisse.

Option	Beschreibung
Alle Änderungen	Eine beliebige Ticketinformation ist geändert worden.
Besitzeränderung	Das Ticketfeld *Besitzer* ist geändert worden.
Statusänderung	Das Ticketfeld *Status* ist geändert worden.
Kommentar	Im Abschnitt *Kommentare* des Tickets sind Informationen, Anhänge oder Screenshots

Option	Beschreibung
	hinzugefügt worden. Das System sendet E-Mail-Benachrichtigungen für Kommentare, wenn Benutzer auf dem Ticketformular Kommentare hinzufügen und auf **Senden** klicken. Wenn Benutzer auf dem Ticketformular Kommentare hinzufügen und auf **Speichern** klicken, wird jedoch nur die Benachrichtigung *Alle Änderungen* gesendet.
Genehmigungsänderung	Der Genehmigungsstatus des Tickets ist geändert worden.
Änderung der Lösung	Die Ticketauflösung ist geändert worden.
Eskalation	Das Ticket ist nicht innerhalb der durch die Ticketpriorität definierten Eskalationszeit aufgelöst worden.
SLA-Verstoß	Das Ticket ist nicht bis zum Fälligkeitsdatum aufgelöst worden.
Ticket abgeschlossen	Das Ticketfeld *Status* ist auf **Abgeschlossen** geändert worden. Dieses Ereignis wird für die Zusendung einer Zufriedenheitsumfrage an die Absender verwendet. Siehe Verwenden der Zufriedenheitsumfrage.
Neues Ticket per E-Mail	Ein Benutzer sendet eine E-Mail-Nachricht an den Service Desk und es wird ein Ticket erstellt.
Neues Ticket per E-Mail	Ein Ticket wird über die **Benutzerkonsole** erstellt.

8. Klicken Sie auf **Speichern**.

   Die Appliance ist nun für die Weiterleitung von E-Mails an den angegebenen SMTP-Server konfiguriert. Wenn Sie mehrere Warteschlangen haben, wiederholen Sie die vorherigen Schritte für jede Warteschlange.

Umbenennen von Service Desk-Titeln und Labels

Sie können die Service Desk-Titel und Label umbenennen, die in der **Administratorkonsole** und der **Benutzerkonsole** verwendet werden.

1. Rufen Sie die Seite *Einstellungen* des Service Desks auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Service Desk** und anschließend auf **Konfiguration**.
   c. Klicken Sie im Fensterbereich *Konfiguration* auf **Einstellungen**.
2. Legen Sie die folgenden Einstellungen fest:

Einstellung	Beschreibung
Hauptregisterkarte	Der Text, der auf der Registerkarte der Komponentenebene in der **Administratorkonsole** und der Registerkarte in der **Benutzerkonsole** angezeigt wird. Der Standardwert lautet **Service Desk**. Wenn Sie jedoch ein Upgrade von einer früheren Version der Appliance durchgeführt haben, wird standardmäßig die Bezeichnung **Helpdesk** angezeigt.
Warteschlange **Warteschlangen**	Der Text, der in der **Administratorkonsole** auf der Seite *Service Desk-Konfiguration* und in der Liste *Warteschlange* anstelle von **Warteschlange** und **Warteschlangen** angezeigt werden soll. Der Text erscheint auch als Option im Menü *Aktion auswählen* und als Überschrift auf der Seite *Ticket* in der **Benutzerkonsole**.
Ticket **Tickets**	Der Text, der in der **Administratorkonsole** auf der Registerkarte *Ticket* und auf der Seite *Ticket* anstelle von **Ticket** und **Tickets** angezeigt werden soll. Dieser Text wird auch in der **Benutzerkonsole** auf der Seite *Ticket* angezeigt.
Prozess **Prozesse**	Der Text, der in der **Administratorkonsole** auf der Seite *Service Desk-Konfiguration* und in der Liste *Prozess* anstelle von **Prozess** und **Prozesse** angezeigt werden soll.

3. Klicken Sie auf **Speichern**.

Aktivieren oder Deaktivieren der Konfliktwarnung

Wurde für eine Warteschlange ein Dialogfeld für Konfliktwarnungen aktiviert, erhalten Administratoren und Ticket-Besitzer eine Meldung, wenn mehrere Benutzer gleichzeitig Tickets bearbeiten. Das Dialogfeld ermöglicht Benutzern, von anderen vorgenommene Änderungen zu sehen und zu entscheiden, welche Änderungen sie übernehmen wollen.

Sie verfügen über Administratorrechte in der **Administratorkonsole**.

Administratoren können das Dialogfeld für Konfliktwarnungen für jede Warteschlange getrennt aktivieren oder deaktivieren.

1. Rufen Sie die Seite *Warteschlangen-Detail* des Service Desks auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Service Desk** und anschließend auf **Konfiguration**.
   c. Klicken Sie im Fensterbereich **Konfiguration** auf **Warteschlangen**.

d. Führen Sie zum Anzeigen der Seite *Warteschlangen-Detail* einen der folgenden Schritte aus:

- Klicken Sie auf den Namen einer Warteschlange.
- Wählen Sie **Aktion auswählen** > **Neu**.

2. Aktivieren oder deaktivieren Sie im Abschnitt *Benutzereinstellungen* die Konfliktwarnung:

Feld	Beschreibung
Ticket-Konfliktwarnung für Ticket-Eigentümer aktivieren	Zeigt ein Dialogfeld für Administratoren und Ticketbesitzer, das Konflikte zwischen abgesendeten Änderungen und von anderen Benutzern abgesendeten Änderungen zusammenfasst. Wenn Administratoren und Ticketbesitzer auf der Seite *Details zum Ticket* auf **Speichern** oder **Änderungen übernehmen** klicken, wird das Dialogfeld angezeigt, wenn das Ticket von anderen Benutzern bearbeitet und gespeichert wurde, während es zur Bearbeitung geöffnet war. Dies ermöglicht Administratoren und Ticketbesitzern im Konfliktfall zu entscheiden, ob sie ihre Änderungen verwerfen oder die Änderungen von anderen Benutzern überschreiben wollen. Das Dialogfeld wird nur dann angezeigt, wenn andere Benutzer das Ticket geändert haben. Nur Administratoren und Ticketbesitzer erhalten diese Warnung. Für andere Benutzer wird das Dialogfeld nicht angezeigt. **HINWEIS:** In dem Dialogfeld sind alle von anderen Benutzern durchgeführten Änderungen zusammengefasst. Die Änderungen des aktuellen Benutzers werden aber nur dann zusammengefasst, wenn ein Konflikt mit von anderen Benutzern vorgenommenen Änderungen besteht.

3. Klicken Sie auf **Speichern**.

Antwortvorlagen anzeigen und bearbeiten

Mit Antwortvorlagen können Sie häufige Antworten als Kommentare oder Auflösungen in Service Desk-Tickets speichern.

Jede Antwortvorlage ist einer bestimmten Ticket-Warteschlange zugeordnet und gehört zu dem Benutzer, der sie erstellt hat. Sie können die entsprechende Antwortvorlage auf der Seite *Ticket-Details* auswählen.

Der Vorlagentext unterstützt die Verwendung von E-Mail-Token. Tokenwerte werden dynamisch anhand der Feldwerte aus dem Ticket aktualisiert, in dem sie referenziert werden. Sie können dieselben Token verwenden, die in E-Mail-Vorlagen verfügbar sind. Weitere Informationen hierzu finden Sie unter E-Mail-Vorlagen konfigurieren.

Eine Antwortvorlage kann öffentlich oder privat sein. Private Antwortvorlagen können in entsprechenden Tickets nur von dem Benutzer, der sie erstellt hat, aktualisiert und referenziert werden. Eine öffentliche Antwortvorlage ist für die Auswahl in der zugeordneten Ticket-Warteschlange von anderen Benutzern verfügbar, doch nur der Benutzer, der sie erstellt hat, kann den Inhalt der Antwortnachricht bearbeiten. Andere Benutzer können den Inhalt der öffentlichen Antwortvorlagen anzeigen, können sie jedoch nicht bearbeiten.

1. Rufen Sie die Seite *Antwortvorlagen* des Service Desks auf:

   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen

Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.

b. Klicken Sie in der linken Navigationsleiste auf **Service Desk** und anschließend auf **Konfiguration**.

c. Klicken Sie im Fenster **Konfiguration** unter **Warteschlangen** auf **Antwortvorlagen**.

d. Führen Sie zum Anzeigen der Seite *Antwortvorlage-Detail* einen der folgenden Schritte aus:

- Klicken Sie auf den Namen einer Antwortvorlage.
- Wählen Sie **Aktion auswählen** > **Neu**.

HINWEIS: Diejenigen Warteschlangen-Eigentümer, die keinen Zugriff auf die *Warteschlangen*-Konfigurationsseiten haben, können auf die Seite *Antwortvorlagen* zugreifen, indem sie auf den Link *Verwalten* klicken, der direkt oberhalb der Option *Vordefinierte Antwort* auf der Seite *Ticket-Detail* angezeigt wird.

2. Legen Sie die folgenden Einstellungen fest:

Feld	Beschreibung
Name	Der Name der Antwortvorlage. Dieser Name ist im Feld *Vordefinierte Antwort* zur Auswahl verfügbar, wenn Sie eine automatisierte Antwort auf die entsprechenden Service Desk-Tickets konfigurieren möchten.
Öffentlich machen	Aktivieren Sie dieses Kontrollkästchen, wenn Sie diese Antwortvorlage zur Auswahl durch andere Benutzer verfügbar machen möchten. Andere Benutzer können den Inhalt der öffentlichen Antwortvorlagen anzeigen, können sie jedoch nicht bearbeiten.
Vorlage	Der Inhalt der Antwortnachricht. Dieses Feld unterstützt Nur-Text und Token.

3. Wenn Sie Änderungen an der Antwortvorlage vorgenommen haben, klicken Sie auf **Speichern**.
4. Um zur Liste der Antwortvorlagen zurückzukehren, klicken Sie auf **Abbrechen**.

Sie können eine Antwortvorlage als vordefinierte Antwort auf eine Service Desk-Ticket-Anfrage verwenden. Weitere Informationen hierzu finden Sie unter Tickets Kommentare hinzufügen.

Konfigurieren der Ticketeinstellungen

Für jede Service Desk-Ticketwarteschlange sind Standardeinstellungen für neue Tickets verfügbar. Sie können diese Einstellungen konfigurieren und nach Bedarf benutzerdefinierte Felder hinzufügen.

Typische benutzerdefinierte Felder:

- **Problembezogene Informationen**: Symptome, wie lange das Problem bereits auftritt oder andere Komponenten, die möglicherweise zum Problem beigetragen haben können.
- **Softwarebezogene Informationen**: Hersteller, Version, Zweck und Installationsdatum der Software.
- **Nur für die Service Desk-Mitarbeiter bestimmte Informationen**: Informationen, die zu Diagnose-, Berichterstellungs- oder Planungszwecken genutzt werden können, wie beispielsweise "Ansprechpartner beim Hersteller für Eskalation", "Grundlegende Ursache" oder "Zuvor behoben".
- **Benutzerdefinierte Ticketwerte**: Kategorien, Status, Prioritäten und Auswirkungen.

Sie können diese Felder jederzeit hinzufügen oder ändern und die Anzahl dieser Felder wird nur durch die Anzahl der maximal in der Datenbanktabelle möglichen Spalten beschränkt. Sie können jedoch keine Felder entfernen, wenn sie von Tickets verwendet werden. Um ein Feld zu entfernen, das benutzt wird, ändern Sie die Tickets auf ein anderes Feld und entfernen Sie dann das Feld.

Seite Details zum Ticket anpassen

Sie können die Seite *Details zum Ticket* für Warteschlangen nach Bedarf anpassen. Wenn Sie mehrere Warteschlangen haben, können Sie die Seite *Details zum Ticket* für jede Warteschlange individuell anpassen.

Der Service Desk umfasst die folgenden konfigurierbaren Ticketeinstellungen:

Einstellung	Verfügbare Werte
Kategorie	• Software • Hardware • Netzwerk • Andere (Standard)
Status	• Neu (Standard) • Offen • abgeschlossen • Weitere Infos erforderlich
Auswirkungen	• Viele Personen können nicht arbeiten • Viele Personen wurden beeinträchtigt • 1 Person kann nicht arbeiten (Standard) • 1 Person wurde belästigt
Priorität	• Hoch • Mittel (Standard) • Niedrig
Status	• Offen (Standard) • abgeschlossen • Angehalten

1. Rufen Sie die Seite *Warteschlangen-Detail* des Service Desks auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Service Desk** und anschließend auf **Konfiguration**.
   c. Klicken Sie im Fensterbereich **Konfiguration** auf **Warteschlangen**.

d. Führen Sie zum Anzeigen der Seite *Warteschlangen-Detail* einen der folgenden Schritte aus:

- Klicken Sie auf den Namen einer Warteschlange.
- Wählen Sie **Aktion auswählen** > **Neu**.

2. Fügen Sie das Label **Alle Ticketbesitzer** zum Feld *Besitzerlabel* hinzu:
   a. Klicken Sie im Feld *Besitzerlabel* auf **Verknüpfte Labels verwalten**.
   b. Ziehen Sie im Dialogfeld *Labels auswählen* die Schaltfläche **Alle Ticketbesitzer** mit der Maus ins Feld *Besitzer begrenzen auf* und klicken Sie dann auf **OK**.

   Weitere Informationen zu diesem Label finden Sie unter Label "Alle Ticketbesitzer" hinzufügen.

   c. Klicken Sie auf **Speichern**.
3. Klicken Sie im Abschnitt *Standardwerte für Tickets* auf **Diese Werte anpassen**, um die Seite *Anpassung von Warteschlange* anzuzeigen.
4. Klicken Sie im Abschnitt *Kategoriewerte* in der Spaltenüberschrift auf die Schaltfläche **Hinzufügen**, um eine Kategorie hinzuzufügen: +.

   Für den neuen Wert werden bearbeitbare Felder angezeigt.
5. Legen Sie die folgenden Einstellungen fest:

Feld	Beschreibung
Name	Der Text, der in der Dropdown-Liste angezeigt wird. Standardmäßig lautet dieser Text **Wählen Sie eine Kategorie**: Damit werden die Benutzer angewiesen, die Kategorie für das Ticket auszuwählen.
Standardbesitzer	Wählen Sie **DefaultTicketOwners** aus.
CC-Liste	Wenn Sie **keine** auswählen, wird die CC-Liste nicht auf Tickets angezeigt. Da **DefaultTicketOwners** der Standardbesitzer ist, erhalten alle potenziellen Ticketbesitzer beim Erstellen eines Tickets E-Mail-Benachrichtigungen.
Vom Benutzer einstellbar	Hierdurch wird diese Kategorie für die Benutzer sichtbar. Bei Deaktivierung erlaubt die Appliance nur den Service Desk-Mitarbeitern, diese Kategorie einzusehen. Verwenden Sie diese Einstellung, um Benutzern eine vereinfachte Werteliste anzuzeigen und den Administratoren und Service Desk-Mitarbeitern eine umfassendere Liste anzubieten. Benutzer sehen diese Kategorien möglicherweise, wenn ihre Tickets bearbeitet werden; sie können sie jedoch nicht einstellen oder ändern.

6. Klicken Sie auf **Speichern**.

   HINWEIS: Sie können Ticketkategorien jederzeit hinzufügen oder ändern. Siehe Erstellen von Ticketkategorien und -unterkategorien.
7. Klicken Sie für die übrigen Kategorien in *Kategoriewerte* auf die Schaltfläche **Bearbeiten**: .
8. Nehmen Sie die folgenden Änderungen vor:
   a. Wählen Sie in der Spalte *Standardbesitzer* die Option **DefaultTicketOwners** aus, um dieses Benutzerkonto als Standardbesitzer all dieser Kategorien festzulegen.

Weitere Informationen zu diesem Konto finden Sie unter Konto "DefaultTicketOwners" erstellen.

b. Entfernen Sie alle Einträge aus der **CC-Liste**.

c. Klicken Sie auf **Speichern**.

9. Erstellen Sie weitere Statuswerte:

   a. Klicken Sie im Abschnitt *Statuswerte* auf die Schaltfläche **Hinzufügen**: +.

      Für den neuen Wert werden editierbare Felder angezeigt.

   b. Geben Sie in der Spalte *Name* die Zeichenfolge Warten auf Benutzer ein und wählen Sie anschließend in der Spalte *Status* die Option **Angehalten** aus.

   c. Klicken Sie auf **Speichern**.

   d. Klicken Sie im Abschnitt *Statuswerte* auf die Schaltfläche **Hinzufügen**: +.

   e. Geben Sie in der Spalte *Name* Warten auf Service Desk-Mitarbeiter ein und wählen Sie dann in der Spalte *Status* die Option **Angehalten** aus. Klicken Sie dann auf **Speichern.**

   f. Klicken Sie im Abschnitt *Statuswerte* auf die Schaltfläche **Hinzufügen**: +.

   g. Geben Sie in der Spalte *Name* Erneut geöffnet ein und wählen Sie dann in der Spalte *Status* die Option **Geöffnet** aus. Klicken Sie dann auf **Speichern**.

   HINWEIS: Nur Tickets mit dem Status **Geöffnet** können eskaliert werden. Siehe Verwenden des Prozesses zur Eskalation von Tickets.

10. Erstellen Sie die Priorität **Kritisch** mit einer Eskalationszeit von 15 Minuten:

    a. Klicken Sie im Abschnitt *Prioritätswerte* auf die Schaltfläche **Hinzufügen**: +.

       Für den neuen Wert werden editierbare Felder angezeigt.

    b. Geben Sie in der Spalte *Name* Kritisch ein und wählen Sie anschließend in der Spalte *Eskalationszeit* die Option **15 Minuten** aus.

    c. Klicken Sie auf **Speichern**.

11. Ändern Sie die *Eskalationszeit* für die Priorität **Hoch** auf 1 Stunde und wählen Sie eine Farbe aus, die Sie für die Kennzeichnung von Tickets mit hoher Priorität verwenden möchten.

12. Klicken Sie unten auf der Seite auf die Schaltfläche **Speichern**.

Anpassen der Startseite der Benutzerkonsole

Sie können das Logo, den Titel, die Willkommensnachricht, die Ankündigungen und die Links auf der Startseite der **Benutzerkonsole** ändern, um die Benutzeroberfläche an das Branding, die Richtlinien und die Kommunikationsanforderungen Ihres Unternehmens anzupassen.

Benutzerkonsolen-Logo und -Text auf Systemebene ändern

Wenn auf der Appliance die Organisationskomponente aktiviert wurde, können Sie den Titel, den Begrüßungstext und das Logo der **Benutzerkonsole** auf Systemebene ändern.

Die auf Systemebene ausgewählten Logos werden für alle Organisationen verwendet, es sei denn, Sie konfigurieren die Organisationseinstellungen separat auf der Verwaltungsebene. Siehe Benutzerkonsole-Logo und Anmeldetext auf Verwaltungsebene ändern.

1. Rufen Sie die Seite *Allgemeine Einstellungen* auf Systemebene auf:

   a. Melden Sie sich bei der Systemadministratorkonsole der Appliance an: `http://`**appliance_hostname**`/system`. Oder wählen Sie in der Dropdown-Liste rechts oben auf der Seite den Eintrag **System** aus.

b. Klicken Sie in der linken Navigationsleiste auf **Einstellungen** und anschließend auf **Systemsteuerung**.

c. Klicken Sie in der *Systemsteuerung* auf **Allgemeine Einstellungen**.

2. Passen Sie im Abschnitt Benutzerkonsole den Text in den folgenden Feldern an:

Option	Beschreibung
Titel	Die Überschrift, die auf der Anmeldeseite der **Benutzerkonsole** angezeigt wird.
Begrüßungsmeldung	Ein Begrüßungshinweis oder eine Beschreibung der **Benutzerkonsole**. Dieser Text wird nach dem Titel auf der Anmeldeseite der **Benutzerkonsole** angezeigt.

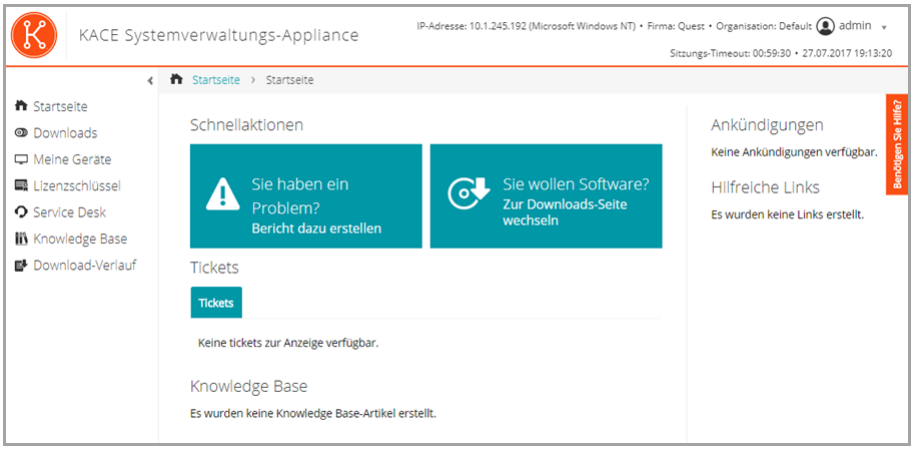
3. Um benutzerdefinierte Benutzerkonsole Logos und Hintergrundfarben zu verwenden, geben Sie in den Abschnitten *Login Screen Options (Optionen des Anmeldebildschirms)* die folgenden Informationen an.

Option	Beschreibung
User Console Login Background Color (Hintergrundfarbe für die Anmeldung an der Benutzerkonsole)	Klicken Sie auf die Farbauswahl und legen Sie damit die Farbe fest, die im Hintergrund der **Benutzerkonsole** angezeigt werden soll. Sie können die Farbe mit der Maus auswählen oder die RGB-Werte nach Bedarf angeben. Wenn Sie die Farbauswahl schließen, zeigt das Feld *HTML Color Code (HTML-Farbcode)* auf der rechten Seite den HTML-Code der ausgewählten Farbe an. Um die Auswahl rückgängig zu machen, klicken Sie auf **Zurücksetzen** und beginnen Sie von vorne. **HINWEIS:** Die Farbauswahl wird in Internet Explorer 11 nicht unterstützt.
Benutzerkonsolenlogo	Klicken Sie in jedem entsprechenden Abschnitt auf **Datei auswählen**, und geben Sie die Grafikdatei an, die Sie als benutzerdefiniertes Logo und in der **Benutzerkonsole** verwenden möchten. Die unterstützten Grafikdateiformate sind `.bmp`, `.gif`, `.jpg` und `.png`

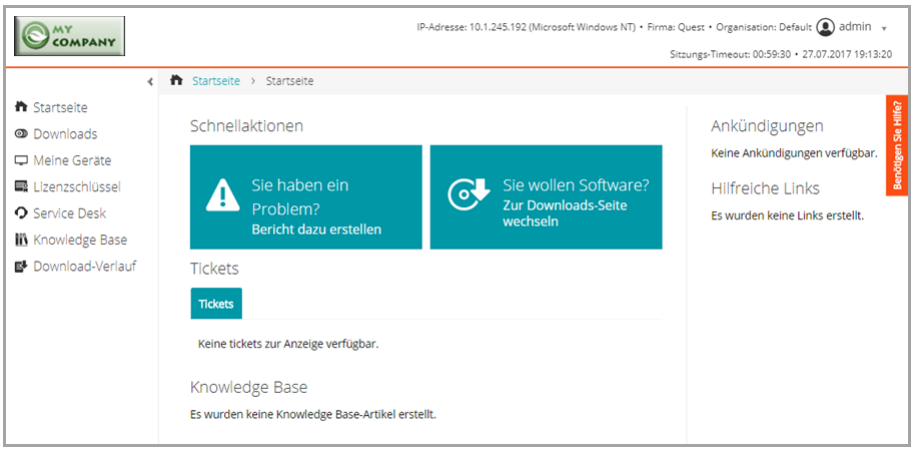
4. Klicken Sie auf **Dienste speichern und neu starten**.

   Die folgenden Abbildungen zeigen die Standardstartseite und eine benutzerdefinierte Version.

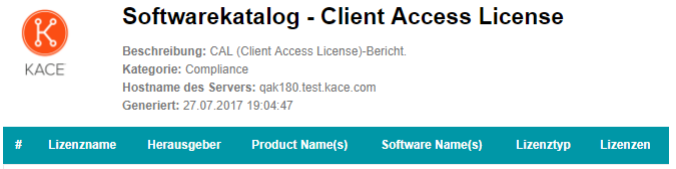
Standardlogo auf der Startseite der Benutzerkonsole



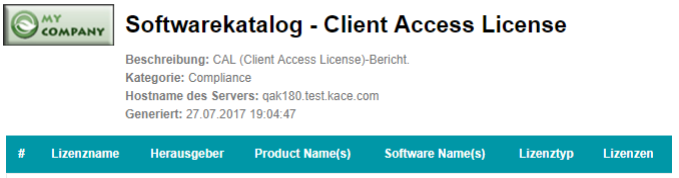
Benutzerdefiniertes Logo auf der Startseite der Benutzerkonsole



Standard-Berichtslogo



Benutzerdefiniertes Berichtslogo



Benutzerkonsole-Logo und Anmeldetext auf Verwaltungsebene ändern

Sie können den Titel, den Begrüßungstext und das Logo der **Benutzerkonsole** entsprechend den Branding-Anforderungen Ihres Unternehmens anpassen.

Wenn auf der Appliance die Organisationskomponente aktiviert wurde, können Sie benutzerdefinierte Logos sowohl auf Verwaltungsebene (Organisation) als auch auf Systemebene angeben. Logoeinstellungen auf Verwaltungsebene haben allerdings Vorrang vor Logoeinstellungen auf Systemebene, was die Angabe verschiedener Logos für jede Organisation ermöglicht. Wenn Sie für eine Organisation kein benutzerdefiniertes Logo auswählen, werden die Einstellungen für die Systemebene verwendet. Siehe Benutzerkonsolen-Logo und -Text auf Systemebene ändern.

1. Rufen Sie die Seite *Allgemeine Einstellungen* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`.
   b. Klicken Sie in der linken Navigationsleiste auf **Einstellungen** und anschließend auf **Systemsteuerung**.
   c. Klicken Sie in der *Systemsteuerung* auf **Allgemeine Einstellungen**.
2. Passen Sie im Abschnitt Benutzerkonsole den Text in den folgenden Feldern an:

   HINWEIS: Wenn die Organisationskomponente auf Ihrer Appliance aktiviert wurde, sind diese **Benutzerkonsole**-Einstellungen auf Systemebene verfügbar. Siehe Benutzerkonsolen-Logo und -Text auf Systemebene ändern.

Option	Beschreibung
Titel	Die Überschrift, die auf der Anmeldeseite der **Benutzerkonsole** angezeigt wird.
Begrüßungsmeldung	Ein Begrüßungshinweis oder eine Beschreibung der **Benutzerkonsole**. Dieser Text wird nach dem Titel auf der Anmeldeseite der **Benutzerkonsole** angezeigt.

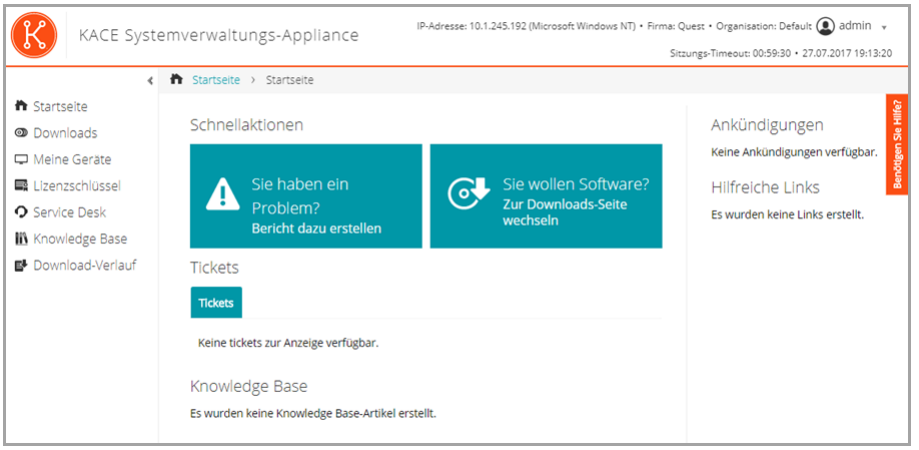
3. Um benutzerdefinierte Benutzerkonsole Logos und Hintergrundfarben zu verwenden, geben Sie in den Abschnitten *Login Screen Options (Optionen des Anmeldebildschirms)* die folgenden Informationen an.

Option	Beschreibung
User Console Login Background Color (Hintergrundfarbe für die Anmeldung an der Benutzerkonsole)	Klicken Sie auf die Farbauswahl und legen Sie damit die Farbe fest, die im Hintergrund der **Benutzerkonsole** angezeigt werden soll. Sie können die Farbe mit der Maus auswählen oder die RGB-Werte nach Bedarf angeben. Wenn Sie die Farbauswahl schließen, zeigt das Feld *HTML Color Code (HTML-Farbcode)* auf der rechten Seite den HTML-Code der ausgewählten Farbe an. Um die Auswahl rückgängig zu machen, klicken Sie auf **Zurücksetzen** und beginnen Sie von vorne. **HINWEIS:** Die Farbauswahl wird in Internet Explorer 11 nicht unterstützt.
Benutzerkonsolenlogo	Klicken Sie in jedem entsprechenden Abschnitt auf **Datei auswählen**, und geben Sie die Grafikdatei an, die Sie als benutzerdefiniertes Logo und in der **Benutzerkonsole** verwenden möchten. Die unterstützten Grafikdateiformate sind `.bmp`, `.gif`, `.jpg` und `.png`

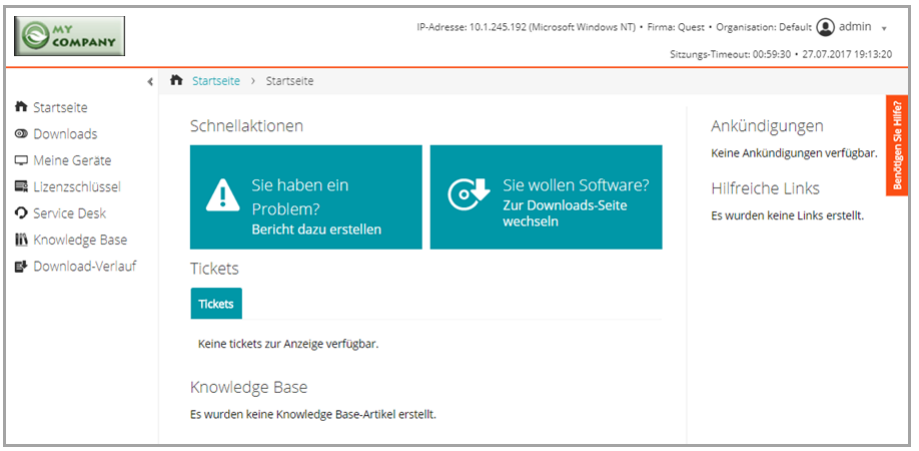
4. Klicken Sie auf **Dienste speichern und neu starten**.

   Die folgenden Abbildungen zeigen die Standardstartseite und eine benutzerdefinierte Version.

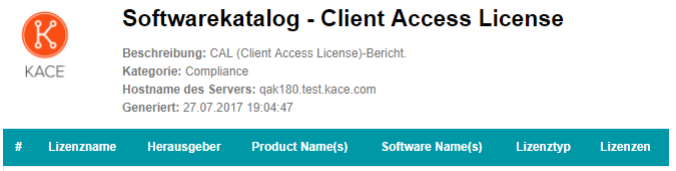
Standardlogo auf der Startseite der Benutzerkonsole



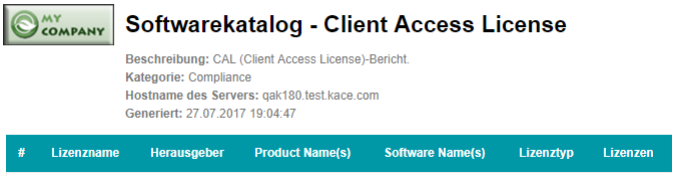
Benutzerdefiniertes Logo auf der Startseite der Benutzerkonsole



Standard-Berichtslogo



Benutzerdefiniertes Berichtslogo



Interaktive Schaltflächen und Widgets auf der Startseite der Benutzerkonsole ein- oder ausblenden

Sie können die interaktiven Schaltflächen und Widgets auf der Startseite der **Benutzerkonsole** ein- oder ausblenden. Mit interaktiven Schaltflächen können Benutzer schnell auf die Seiten zugreifen, auf denen Service Desk-Tickets angelegt und Software über die **Benutzerkonsole** heruntergeladen werden können. Mit Widgets können Sie benutzerdefinierte Links und Ankündigungen zur Startseite der **Benutzerkonsole** hinzufügen.

Interaktive Schaltflächen werden unabhängig von den Ticketwarteschlangen-Berechtigungen des Benutzers in der **Benutzerkonsole** für jeden Service Desk global angezeigt. Wenn jedoch in Ihrem System die Organisationskomponente aktiviert ist, werden interaktive Schaltflächen für den Service Desk jeder Organisation separat verwaltet.

1. Rufen Sie die Seite *Einstellungen der Startseite der Benutzerkonsole* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Service Desk** und anschließend auf **Konfiguration**.
   c. Klicken Sie im Fensterbereich **Konfiguration** im Abschnitt *Startseite der Benutzerkonsole* auf **Startseite der Benutzerkonsole konfigurieren**.
2. Wählen Sie die Anzeigeoptionen für jedes Element aus. Aktivieren Sie die Kontrollkästchen der Elemente, die angezeigt werden sollen. Deaktivieren Sie die Kontrollkästchen der Elemente, die ausgeblendet werden sollen.

Option	Beschreibung
Schnellaktionen anzeigen • Ticket-Schnellaktionen • Schnellaktionen "Download-Seite"	Ein- oder Ausblenden der Schnellaktion-Links, die auf der Download-Seite der **Benutzerkonsole** angezeigt werden. Der Text für diese Links beinhaltet: • **Ticket-Schnellaktionen**: Probleme melden • **Schnellaktionen "Download-Seite"**: Sie brauchen Software? Rufen Sie die Download-Seite auf. **HINWEIS:** Der Link-Text kann nicht geändert werden. Sie können aber das Label für Service Desk Tickets ändern, das in diesem Link verwendet wird. Wenn Sie beispielsweise Ihren Service Desk so ändern, dass das Label **Vorfälle** statt **Ticket** verwendet wird, heißt der Link für Schnellaktionen dann *Vorfälle-Schnellaktionen*. Siehe Umbenennen von Service Desk-Titeln und Labels.
Hauptfenster-Widgets • Tickets-Widget • Knowledge Base-Widget	Ein- oder Ausblenden der Widgets für: • **Tickets**: Links zu vom Benutzer eingereichten Tickets und der Link "Eigene Tickets

Option	Beschreibung
	anzeigen", mit dem der Benutzer zur Tickets-Liste gelangt • **Knowledge Base**: Links zu Knowledge Base-Artikeln, die dem Benutzer zur Verfügung stehen
Widgets im rechten Bereich • Widget "Ankündigungen" • Widget "Hilfreiche Links"	Ein- oder Ausblenden der Widgets für: • **Ankündigungen**: Meldungen, die dem Benutzer angezeigt werden sollen • **Hilfreiche Links**: HTML-Links zu Ihrem Intranet, Wiki, Cloud-Anwendungen oder jeder anderen Webressource

3. Klicken Sie auf **Speichern**.

   Schnellaktionen und Widgets werden auf der Startseite der **Benutzerkonsole** sofort ein- oder ausgeblendet. Wenn Benutzer angemeldet sind und die Startseite der **Benutzerkonsole** geöffnet haben, wird der Link nach der Aktualisierung der Seite angezeigt.

   HINWEIS: Widgets sind leer, bis Ankündigungen, Links oder Knowledge Base-Artikel hinzugefügt wurden.

Fügen Sie Ankündigungen, Links und Knowledge Base-Artikel hinzu. Siehe:

- Benutzerkonsole-Ankündigungen hinzufügen, bearbeiten, ausblenden oder löschen
- Benutzerdefinierte Links auf der Startseite der Benutzerkonsole hinzufügen, bearbeiten oder löschen
- Knowledge Base-Artikel hinzufügen, bearbeiten oder duplizieren

Links zu Knowledge Base-Artikeln auf der Startseite der Benutzerkonsole ein- oder ausblenden

Sie können Links zu Knowledge Base-Artikeln auf der Startseite der **Benutzerkonsole** ein- oder ausblenden. Außerdem können Sie Labels verwenden, um Knowledge Base-Artikel für verschiedene Benutzergruppen ein- oder auszublenden.

Um Links zu Knowledge Base-Artikeln verwalten zu können, müssen Sie mindestens einen Knowledge Base-Artikel erstellen. Siehe Knowledge Base-Artikel hinzufügen, bearbeiten oder duplizieren.

Um Labels für das Ein- oder Ausblenden von Links zu Knowledge Base-Artikeln verwenden zu können, müssen Sie mindestens ein Benutzerlabel erstellen. Siehe Manuelle Labels hinzufügen oder bearbeiten.

1. Rufen Sie die Seite *Einstellungen der Startseite der Benutzerkonsole* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Service Desk** und anschließend auf **Konfiguration**.
   c. Klicken Sie im Fensterbereich **Konfiguration** im Abschnitt *Startseite der Benutzerkonsole* auf **Startseite der Benutzerkonsole konfigurieren**.
2. Aktivieren Sie im Abschnitt *Hauptfenster-Widgets* das Kontrollkästchen neben **Knowledge Base-Widget**.
3. Klicken Sie auf **Speichern**.

Die Einstellung wird gespeichert und der Fensterbereich *Service Desk-Konfiguration* wird angezeigt.

4. Um den Zugriff auf Knowledge Base-Artikel zu steuern, rufen Sie die Seite *Artikeldetail* auf und weisen den Artikeln Benutzerlabels zu:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Service Desk** und anschließend auf **Knowledge Base**.
   c. Führen Sie zum Anzeigen der Seite *Artikeldetail* einen der folgenden Schritte aus:
      - Klicken Sie auf den Namen eines Artikels.
      - Wählen Sie **Aktion auswählen** > **Neu**.
   d. Wählen Sie im Abschnitt *Zuweisen zu Labels* das Label aus, dass Sie mit dem Artikel verknüpfen möchten. Klicken Sie dann auf **Speichern**.

   Der Zugriff auf die Knowledge Base-Artikel ist auf Benutzer beschränkt, denen das entsprechende Label zugewiesen ist.
5. Rufen Sie die Liste *Benutzer* auf und weisen Sie den Benutzerkonten das Label zu:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie auf der linken Navigationsleiste auf **Einstellungen** und anschließend auf **Benutzer**.
   c. Aktivieren Sie in der Liste *Benutzer* die Kontrollkästchen neben den Benutzern, die den Artikel anzeigen können sollen.
   d. Wählen Sie **Aktion auswählen** > **Labels zuweisen**.
   e. Ziehen Sie das mit dem Knowledge Base-Artikel verknüpfte Label in das Feld *Diese Labels übernehmen* und klicken Sie dann auf **Labels zuweisen**.

   Benutzer, denen das Label zugewiesen worden ist, können auf den Knowledge Base-Artikel zugreifen.

Benutzerkonsole-Ankündigungen hinzufügen, bearbeiten, ausblenden oder löschen

Sie können Ankündigungen hinzufügen, die auf der Startseite der**Benutzerkonsole** angezeigt werden sollen, und vorhandene Ankündigungen nach Bedarf bearbeiten, ausblenden oder löschen.

Um Ankündigungen anzuzeigen, müssen Sie den Service Desk so konfigurieren, dass das Widget *Ankündigungen* angezeigt wird. Siehe Anpassen der Startseite der Benutzerkonsole.

Ankündigungen werden unabhängig von den Ticketwarteschlangen-Berechtigungen des Benutzers in der **Benutzerkonsole** für jeden Service Desk global angezeigt. Wenn jedoch in Ihrem System die Organisationskomponente aktiviert ist, werden Ankündigungen für den Service Desk jeder Organisation separat verwaltet.

HINWEIS: Die ersten 140 Zeichen jeder Ankündigung werden auf der Startseite der **Benutzerkonsole** angezeigt. Bei Ankündigungen, die länger als 140 Zeichen sind, können die Benutzer über den Link **Mehr anzeigen** die gesamte Ankündigung lesen.

1. Rufen Sie die Seite *Benutzerkonsolenankündigungen* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen*

aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.

b. Klicken Sie in der linken Navigationsleiste auf **Service Desk** und anschließend auf **Ankündigungen**.

2. So fügen Sie eine Ankündigung hinzu:

   a. Klicken Sie auf **Ankündigung hinzufügen**.

   b. Geben Sie die folgenden Informationen an:

Option	Beschreibung
Nachrichtentitel	(Erforderlich) Der Titel, den Sie für die Ankündigung verwenden möchten. **HINWEIS:** Im Feld *Nachrichtentitel* können keine Links verwendet werden.
Nachrichtentext	(Optional) Weitere Informationen, die Sie anzeigen möchten, einschließlich Links. Diese Informationen werden unter dem Titel angezeigt. Verwenden Sie beim Erstellen von Links für Ankündigungsnachrichten die folgenden Formate: • http://example.com • https://example.com • http://www.example.com • www.example.com
Ausgeblendet	(Optional) Ein- oder Ausblenden der Ankündigung auf der Startseite der **Benutzerkonsole**. Diese Aktion ist hilfreich, wenn Sie bestimmte Nachrichten in regelmäßigen Abständen ein- oder ausblenden möchten, z. B. Ankündigungen zum Systemstatus oder zu geplanten Wartungen. Aktivieren Sie das Kontrollkästchen, um die Ankündigung auszublenden. Deaktivieren Sie das Kontrollkästchen, um die Ankündigung einzublenden.
Zu Labels zugewiesen	(Optional) Die Benutzer-Labels, für die die Ankündigung gilt. Wenn Sie ein Label auswählen, wird die Ankündigung nur Benutzern angezeigt, deren Benutzerkonto das Label zugewiesen ist. Diese Aktion ist hilfreich, wenn Ankündigungen Gruppen von Benutzern angezeigt werden sollen, z. B. Benutzern an verschiedenen geografischen Standorten, und Sie für diese Benutzer Label erstellt und zugewiesen haben.

   c. Klicken Sie auf **Speichern**.

   Wenn das Widget "Ankündigungen" für den Service Desk aktiviert ist, wird die Ankündigung auf der Startseite der **Benutzerkonsole** je nach von Ihnen ausgewählten Einstellungen angezeigt.

3. Um eine Ankündigung zu bearbeiten, klicken Sie unter dem Ankündigungstitel auf **Bearbeiten** und dann auf **Speichern**.

Die Änderungen werden auf der Startseite der **Benutzerkonsole** sofort angezeigt. Wenn Benutzer angemeldet sind und die Startseite der **Benutzerkonsole** geöffnet haben, wird die Ankündigung nach der Aktualisierung der Seite gelöscht.

4. So blenden Sie eine Ankündigung aus:
   a. Klicken Sie unter dem Ankündigungstitel auf **Bearbeiten**.
   b. Aktivieren Sie das Kontrollkästchen neben *Ausgeblendet*.
   c. Klicken Sie auf **Speichern**.

   Die Ankündigung wird auf der Startseite der **Benutzerkonsole** sofort verborgen. Wenn Benutzer angemeldet sind und die Startseite der **Benutzerkonsole** geöffnet haben, wird die Ankündigung nach der Aktualisierung der Seite verborgen.
5. Die Priorität der Ankündigung kann mit dem Ziehen-Symbol auf der linken Seite der Ankündigung geändert werden. Siehe Benutzerkonsole Ankündigungen priorisieren oder Ankündigung als dringend kennzeichnen.

   Die Ankündigung wird auf der Startseite der **Benutzerkonsole** sofort verborgen. Wenn Benutzer angemeldet sind und die Startseite der **Benutzerkonsole** geöffnet haben, wird die Ankündigung nach der Aktualisierung der Seite verborgen.
6. Um eine Ankündigung zu löschen, klicken Sie unter dem Ankündigungstitel auf **Löschen** und dann im Bestätigungsfenster auf **Ja**.

   Die Ankündigung wird sofort von der Startseite der **Benutzerkonsole** entfernt. Wenn Benutzer angemeldet sind und die Startseite der **Benutzerkonsole** geöffnet haben, wird die Ankündigung nach der Aktualisierung der Seite gelöscht.

Benutzerkonsole Ankündigungen priorisieren oder Ankündigung als dringend kennzeichnen

Sie können festlegen, in welcher Reihenfolge die Ankündigungen auf der Startseite der **Benutzerkonsole** angezeigt werden sollen. Zusätzlich können Sie eine dringende Ankündigung in einem markierten Banner anzeigen lassen, um mehr Aufmerksamkeit zu erhalten.

Um Ankündigungen Priorität zu verleihen, müssen Sie den Service Desk so konfigurieren, dass das Widget *Ankündigungen* angezeigt wird. Auch müssen Sie Ankündigungen hinzufügen. Siehe:

- Interaktive Schaltflächen und Widgets auf der Startseite der Benutzerkonsole ein- oder ausblenden
- Benutzerkonsole-Ankündigungen hinzufügen, bearbeiten, ausblenden oder löschen

1. Rufen Sie die Seite *Benutzerkonsolenankündigungen* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Service Desk** und anschließend auf **Ankündigungen**.
2. Um einer Ankündigung Priorität zu verleihen, verwenden Sie das Ziehen-Symbol auf der linken Seite der Ankündigung ( ) wie folgt:
   - Zum Ändern der Priorität einer Ankündigung ziehen Sie diese in der Liste nach oben oder nach unten. Ankündigungen werden auf der Startseite der **Benutzerkonsole** in der Reihenfolge angezeigt, die auf der Seite *Benutzerkonsolenankündigungen* festgelegt ist.
   - Um einer Ankündigung Dringlichkeit zu verleihen, ziehen Sie sie in das Feld *Dringende Ankündigung*. Die dringende Ankündigung wird auf der Startseite der **Benutzerkonsole** ganz oben in einem Banner angezeigt.

> **HINWEIS:** In dem Banner *Dringende Ankündigung* kann immer nur eine Ankündigung auf einmal angezeigt werden.

- Um die dringende Ankündigung zu ändern, ziehen Sie eine andere Ankündigung in das Feld *Dringende Ankündigung*.
- Um aus der dringenden eine normale Ankündigung zu machen, ziehen Sie sie aus dem Feld *Dringende Ankündigung*.

Die Priorität der Ankündigungen wird sofort von der Startseite der **Benutzerkonsole** übernommen. Wenn Benutzer angemeldet sind und die Startseite der **Benutzerkonsole** geöffnet haben, wird die Ankündigungspriorität nach der Aktualisierung der Seite übernommen.

Benutzerdefinierte Links auf der Startseite der Benutzerkonsole hinzufügen, bearbeiten oder löschen

Sie können benutzerdefinierte Links hinzufügen, die auf der Startseite der **Benutzerkonsole** angezeigt werden sollen, und vorhandene benutzerdefinierte Links nach Bedarf bearbeiten oder löschen.

Um benutzerdefinierte Links anzuzeigen, müssen Sie den Service Desk so konfigurieren, dass das Widget *Hilfreiche Links* angezeigt wird. Siehe Anpassen der Startseite der Benutzerkonsole.

Benutzerdefinierte Links werden unabhängig von den Ticketwarteschlangen-Berechtigungen des Benutzers in der **Benutzerkonsole** für jeden Service Desk global angezeigt. Wenn jedoch in Ihrem System die Organisationskomponente aktiviert ist, werden benutzerdefinierte Links für den Service Desk jeder Organisation separat verwaltet.

1. Rufen Sie die Seite *Links auf Startseite der Benutzerkonsole* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Service Desk** und anschließend auf **Konfiguration**.
   c. Klicken Sie im Fensterbereich **Konfiguration** im Abschnitt *Startseite der Benutzerkonsole* auf **Hilfreiche Links definieren**.
2. So fügen Sie einen Link hinzu:
   a. Klicken Sie auf +.
   b. Geben Sie die folgenden Informationen an:

Option	Beschreibung
Titel	Der als Linktext anzuzeigende Text. Sie können die URL selbst oder eine beliebige Textzeichenfolge verwenden.
URL	Die URL des Links. Zulässige Linkformate sind: • http://example.com • https://example.com • http://www.example.com **HINWEIS:** Die gleiche URL kann nicht in mehreren Links verwendet werden.

c. Klicken Sie rechts neben dem Feld *URL* auf **Speichern** und anschließend unten auf der Seite auf **Speichern**.

Der Link wird auf der Startseite der **Benutzerkonsole** sofort angezeigt. Wenn Benutzer angemeldet sind und die Startseite der **Benutzerkonsole** geöffnet haben, wird der Link nach der Aktualisierung der Seite angezeigt.

3. So bearbeiten Sie einen Link:
   a. Klicken Sie auf .
   b. Ändern Sie den *Titel* oder die *URL* nach Bedarf.
   c. Klicken Sie rechts neben dem Feld *URL* auf **Speichern** und anschließend unten auf der Seite auf **Speichern**.

   Die Änderung wird auf der Startseite der **Benutzerkonsole** sofort angezeigt. Wenn Benutzer angemeldet sind und die Startseite der **Benutzerkonsole** geöffnet haben, wird der Link nach der Aktualisierung der Seite angezeigt.
4. So ändern Sie die Reihenfolge, in der die Links auf der Startseite der Benutzerkonsole angezeigt werden:
   a. Ziehen Sie den Link mit nach oben oder unten.
   b. Klicken Sie unten auf der Seite auf **Speichern**.

   Die Änderung wird auf der Startseite der **Benutzerkonsole** sofort angezeigt. Wenn Benutzer angemeldet sind und die Startseite der **Benutzerkonsole** geöffnet haben, wird die Reihenfolge der Links nach der Aktualisierung der Seite geändert.
5. So löschen Sie einen Link:
   a. Klicken Sie auf .
   b. Klicken Sie im Dialogfenster auf **Ja**.
   c. Klicken Sie rechts neben dem Feld *URL* auf **Speichern** und anschließend unten auf der Seite auf **Speichern**.

   Der Link wird auf der Startseite der **Benutzerkonsole** sofort gelöscht. Wenn Benutzer angemeldet sind und die Startseite der **Benutzerkonsole** geöffnet haben, wird der Link nach der Aktualisierung der Seite gelöscht.

Ticket-Links zur Startseite der Benutzerkonsole hinzufügen

Sie können den Service Desk so konfigurieren, dass auf der Startseite der **Benutzerkonsole** automatisch Links zu den Tickets des Benutzers hinzugefügt werden. Dieser Link ermöglicht den Benutzern den Zugriff auf die Ticketdetails mit nur einem Klick.

Ticket-Links werden nur angezeigt, wenn der Benutzer mindestens ein Ticket erstellt hat.

1. Rufen Sie die Seite *Links auf Startseite der Benutzerkonsole* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Service Desk** und anschließend auf **Konfiguration**.
   c. Klicken Sie im Fensterbereich **Konfiguration** im Abschnitt *Startseite der Benutzerkonsole* auf **Startseite der Benutzerkonsole konfigurieren**.
2. Aktivieren Sie im Abschnitt *Hauptfenster-Widgets* das Kontrollkästchen neben **Tickets-Widget**.
3. Klicken Sie auf **Speichern**.

Die Einstellung wird gespeichert und der Fensterbereich *Service Desk-Konfiguration* wird angezeigt. Auf der Startseite der **Benutzerkonsole** werden vom Benutzer abgelegte Tickets sowie der Link **Eigene Tickets** angezeigt, über den die Benutzer direkt zur Seite *Tickets* gelangen.

HINWEIS: Wenn der Benutzer keine Tickets erstellt hat, wird das Widget *Tickets* mit einem Hinweis angezeigt, dass keine Tickets für die Anzeige zur Verfügung stehen.

Schnellaktions-Link für die Meldung von Problemen auf der Startseite der Benutzerkonsole hinzufügen

Sie können der Seite *Neues Ticket* auf der Startseite der **Benutzerkonsole** einen Schnellaktions-Link hinzufügen. Dieser ermöglicht Benutzern den Zugriff auf das Formular "Neues Ticket" mit nur einem Klick.

1. Rufen Sie die Seite *Einstellungen der Startseite der Benutzerkonsole* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Service Desk** und anschließend auf **Konfiguration**.
   c. Klicken Sie im Fensterbereich **Konfiguration** im Abschnitt *Startseite der Benutzerkonsole* auf **Startseite der Benutzerkonsole konfigurieren**.
2. Aktivieren Sie im Abschnitt *Schnellaktionen anzeigen* das Kontrollkästchen neben **Ticket Schnellaktion**.
3. Klicken Sie auf **Speichern**.

   Die Einstellung wird gespeichert und der Fensterbereich *Service Desk-Konfiguration* wird angezeigt. Die Schaltfläche *Probleme Melden* wird auf der Startseite der **Benutzerkonsole** angezeigt. Wenn Benutzer auf diese Schaltfläche klicken, wird die Seite *Neues Ticket* angezeigt.

Informationen zur Zeitspanne für den Sitzungs-Timeout

Standardmäßig meldet die Appliance Benutzer nach einer Stunde Inaktivität automatisch von der **Administratorkonsole** oder **Benutzerkonsole** ab. **(Sitzungs-Timeout)**.

Die Sitzung beginnt bei jeder Serverinteraktion von neuem, zum Beispiel wenn die aktuelle Seite erneut geladen, Änderungen gespeichert oder zu einer anderen Seite gewechselt wird. Wenn die Zeitspanne für den Timeout ohne Interaktion verstreicht, gehen ungespeicherte Änderungen verloren und die Anmeldeseite wird angezeigt. Der Timeout-Zähler der Sitzung wird in der oberen rechten Ecke jeder Konsole angezeigt.

Informationen zum Ändern des Sitzungs-Timeouts finden Sie hier:

- Allgemeine Appliance-Einstellungen bei aktivierter Organisationskomponente konfigurieren
- Allgemeine Appliance-Einstellungen ohne aktivierte Organisationskomponente konfigurieren

Verwenden der Zufriedenheitsumfrage

Mithilfe der Zufriedenheitsumfrage können Absender von Service-Desk-Tickets Feedback zur Behandlung von Tickets geben.

Wenn die Zufriedenheitsumfrage aktiviert ist, wird sofort nach dem Schließen von Tickets eine E-Mail-Nachricht versendet, die die Umfrage beschreibt. Für diese E-Mail-Nachricht wird die E-Mail-Vorlage **Ticket abgeschlossen** verwendet.

Die Umfrage wird dem Absender standardmäßig angezeigt, wenn er zum ersten Mal auf ein abgeschlossenes Ticket zugreift. Sie wird danach so lange angezeigt, bis die Umfrage ausgefüllt wurde. Nachdem die Umfrage

ausgefüllt wurde, wird sie ausgeblendet. Umfragepunkte und -kommentare werden im Ticket gespeichert und können von den Service Desk-Mitarbeitern nicht bearbeitet werden.

Sie können verschiedene Berichte ausführen, um die Umfragedaten mit Service Desk-Berichten anzuzeigen und zu analysieren. Darüber hinaus können Sie die E-Mail-Vorlage *Ticket abgeschlossen*, die die Umfrage beschreibt, sowie das Umfrage-Label ändern oder die Anzeige der Umfrage deaktivieren. Siehe:

- Ausführen von Service Desk-Berichten
- E-Mail-Vorlagen konfigurieren
- Label für die Zufriedenheitsumfrage ändern
- Feld "Zufriedenheitsumfrage" aus den Tickets entfernen

Standardverhalten der Zufriedenheitsumfrage ändern

Die Zufriedenheitsumfrage kann durch Bearbeiten der Standardeingabeaufforderung im Umfragefeld geändert oder entfernt und nicht für den Ticketabsender angezeigt werden.

Label für die Zufriedenheitsumfrage ändern

Sie können das Einführungslabel für die Zufriedenheitsumfrage entsprechend Ihren Anforderungen ändern.

1. Rufen Sie die Seite *Warteschlangen-Detail* des Service Desks auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Service Desk** und anschließend auf **Konfiguration**.
   c. Klicken Sie im Fensterbereich **Konfiguration** auf **Warteschlangen**.
   d. Klicken Sie auf den Namen einer Warteschlange.
2. Klicken Sie oben auf der Seite auf Felder und Layout anpassen, um die Seite *Anpassung von Warteschlange* anzuzeigen.
3. Klicken Sie im Abschnitt *Layout Ticket-Felder* in der Zeile *SAT_SURVEY* auf die Schaltfläche **Bearbeiten**: .
4. Geben Sie im Abschnitt *Label* den neuen Text für das Umfragefeld ein.
5. Klicken Sie rechts neben dem Element auf die Schaltfläche **Speichern**.
6. Klicken Sie unten auf der Seite auf die Schaltfläche **Speichern**.

Feld "Zufriedenheitsumfrage" aus den Tickets entfernen

Sie können verhindern, dass Ticketabsendern die Zufriedenheitsumfrage angezeigt wird.

1. Rufen Sie die Seite *Warteschlangen-Detail* des Service Desks auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Service Desk** und anschließend auf **Konfiguration**.
   c. Klicken Sie im Fensterbereich **Konfiguration** auf **Warteschlangen**.

   d. Klicken Sie auf den Namen einer Warteschlange.
2. Klicken Sie oben auf der Seite auf Felder und Layout anpassen, um die Seite *Anpassung von Warteschlange* anzuzeigen.
3. Klicken Sie im Abschnitt *Layout Ticket-Felder* in der Zeile *SAT_SURVEY* auf die Schaltfläche **Bearbeiten**: .
4. Wählen Sie im Abschnitt *Berechtigungen* den Eintrag **Ausgeblendet** aus der Dropdown-Liste aus.
5. Klicken Sie rechts neben dem Element auf die Schaltfläche **Speichern**.
6. Klicken Sie unten auf der Seite auf die Schaltfläche **Speichern**.

   Die Zufriedenheitsumfrage ist nun deaktiviert und wird den Ticketabsendern nicht mehr angezeigt, wenn die Tickets abgeschlossen wurden.

Aktivieren oder Deaktivieren der Sicherheitsfunktionen für Service Desk-Anhänge

Sie können die Sicherheitsfunktionen für Service Desk-Anhänge aktivieren oder deaktivieren, um zu verhindern, dass außerhalb der **Administratorkonsole** oder **Benutzerkonsole** auf Dateien zugegriffen wird.

Die Sicherheitseinstellungen für Service Desk-Anhänge sind standardmäßig aktiviert. Deaktivieren Sie diese Funktion, wenn Benutzer auch außerhalb der **Administratorkonsole** oder **Benutzerkonsole** auf Ticket-Anhänge über Ticket-Links zugreifen können sollen. Die Sicherheitseinstellungen für Service Desk-Anhänge sind Einstellungen auf Appliance-Ebene. Wenn die Organisationskomponente auf Ihrem System aktiviert ist, gelten die gewählten Einstellungen für alle Organisationen.

1. Navigieren Sie zur *Systemsteuerung* der Appliance:
   - **Wenn die Organisationskomponente nicht für die Appliance aktiviert ist, melden Sie sich bei der Administratorkonsole an: `https://appliance_hostname/admin`, und wählen Sie dann Einstellungen > Systemsteuerung aus.**
   - **Wenn die Organisationskomponente für die Appliance aktiviert ist, melden Sie sich bei der Systemverwaltungskonsole der Appliance an: `https://appliance_hostname/system`. Oder wählen Sie in der Dropdown-Liste rechts oben auf der Seite den Eintrag System aus, und klicken Sie dann auf Einstellungen > Systemsteuerung.**
2. Klicken Sie auf **Sicherheitseinstellungen**, um die Seite *Sicherheitseinstellungen* anzuzeigen.
3. Wählen Sie im Abschnitt *Sichere Anhänge für Service Desk*, ob Sie die Sicherheitseinstellungen für an Service Desk Tickets angehängte Dateien hinzufügen wollen:
   - **Wählen Sie das Kontrollkästchen aus, um die Sicherheitseinstellungen für an Tickets angehängte Dateien zu aktivieren. Wenn Sie diese Option wählen, können Benutzer nur innerhalb der Administratorkonsole oder Benutzerkonsole der Appliance auf an Tickets angehängte Dateien zugreifen.**
   - **Deaktivieren Sie das Kontrollkästchen, wenn Benutzer auch außerhalb der Administratorkonsole oder Benutzerkonsole durch Klicken auf Links auf Ticket-Dateianhänge zugreifen dürfen.**
4. Klicken Sie auf **Dienste speichern und neu starten**, um die Änderungen zu übernehmen und die Appliance neu zu starten.

Verwenden des Service Desk-Dashboards

Das Service Desk-Dashboard bietet einen Überblick über Service Desk-Tickets für die ausgewählte Organisation (falls zutreffend) oder das Gerät.

Wenn auf der Appliance die Organisationskomponente aktiviert ist und Sie bei der Administratorkonsole angemeldet sind (`http://`**appliance_hostname**`/admin`), zeigt das *Service Desk-Dashboard* Informationen zur ausgewählten Organisation an. Wenn Sie an der Systemverwaltungskonsole angemeldet sind (`http://`**appliance_hostname**`/system`), zeigt das Dashboard Informationen zur Appliance an, einschließlich aller Organisationen.

Sie können auf das *Service Desk-Dashboard* zugreifen, wenn eine oder mehrere Rollen, die mit Ihrem Benutzerkonto verknüpft sind, Zugriff auf dieses Dashboard haben. Wenn Sie es ausblenden möchten, bearbeiten Sie Ihre Benutzerrollen nach Bedarf. Weitere Informationen hierzu finden Sie unter Benutzerrollen hinzufügen oder bearbeiten.

TIPP: Die Appliance aktualisiert die Übersichtswidgets regelmäßig. Um die meisten Widgets zu aktualisieren, klicken Sie auf die Schaltfläche **Aktualisieren** in der oberen rechten Seite: . Um die meisten einzelne Widgets zu aktualisieren, zeigen Sie mit dem Mauszeiger auf das Widget und klicken Sie oberhalb des Widgets auf die Schaltfläche **Aktualisieren**. Einige Widgets erfordern möglicherweise zusätzliche Schritte.

Info über die Service Desk-Dashboard-Widgets

Die Service Desk-Dashboard-Widgets bieten einen Überblick über Service Desk-Tickets für die ausgewählte Organisation oder Appliance.

In diesem Abschnitt werden die im *Service Desk-Dashboard* verfügbaren Widgets beschrieben. Wenn die Organisationskomponente in Ihrer Appliance aktiviert ist, zeigen die Widgets die Informationen für die ausgewählte Organisation auf Administratorebene und die Informationen für das Gerät auf Systemebene.

Dieses Dashboard bietet einen groben Überblick über Ihre Gerätenutzung. Verwenden Sie es, um schnell den Status Ihrer Geräte zu überprüfen und nach Indikatoren zu suchen, mit denen Sie Ihre Ticketverwaltung verbessern können. Beispielsweise können Sie die Anzahl aktiver oder überfälliger Tickets pro Besitzer sehen.

Titel, Diagrammtyp und die Gruppierung der Elemente in einigen Widgets können aktualisiert werden. Die Gruppierungsoptionen unterscheiden sich geringfügig zwischen diesen Widgets.

Widget	Beschreibung
Verknüpfungen	Dieses Widget enthält Links zu allgemeinen Service Desk-Aktionen. Verwenden Sie es, um bestimmte Aufgaben schnell zu initiieren, z. B. das Erstellen eines neuen KB-Artikels (Knowledge Base), die Planung eines Berichts usw.
Ansichten	Dieses Widget enthält Links zu allgemeinen Service Desk-Seiten und -Assistenten, einschließlich benutzerdefinierten Ansichten, die Sie erstellt haben. Verwenden Sie es, um schnell zu bestimmten Seiten zu navigieren, wie z. B. *Meine letzten Tickets*, *Nicht zugewiesene Tickets* und *Heute fällige Tickets.* Außerdem wird der Link zu

Widget	Beschreibung
	benutzerdefinierten Ansichten angezeigt. Die Liste der benutzerdefinierten Ansichten ist alphabetisch sortiert. Wenn die benutzerdefinierten Ansichten in einer bestimmten Reihenfolge angezeigt werden sollen, können Sie ihre Namen bei Bedarf mit Nummern versehen.
Berichte	Dieses Widget enthält Links zu allgemeinen Service Desk-Berichten. Verwenden Sie sie, um schnell einen bestimmten Bericht zu erstellen, z. B. *Offene Tickets der letzten 7 Tagen nach Eigentümer*, *Blockierte/offene Tickets nach Eigentümer* und andere.
Heute geöffnete Tickets	Dieser Assistent enthält die Anzahl der heute geöffneten Service-Desk-Tickets.
Aktive Tickets nach Benutzer Aktive Tickets nach Kategorie Aktive Tickets nach Priorität Aktive Tickets Abgeschlossene Tickets Überfällige Tickets Überfällige Tickets nach Benutzer Heute überfällige Tickets Heute fällige Tickets Erneut geöffnete Tickets	Diese Widgets zeigen die Anzahl der aktiven, geschlossenen, überfälligen, heute überfälligen, fälligen, heute fälligen oder erneut geöffneten Service-Desk-Tickets, die nach einem der folgenden Parameter gruppiert sind: • Kategorie • Priorität • Besitzer • Warteschlange • Bereich Die resultierenden Daten können in einem *Balkendiagramm* oder einem *Ringdiagramm* angezeigt werden. Um den Widget-Titel zu ändern, wählen Sie, wie Sie die Tickets gruppieren möchten, oder wählen Sie den Diagrammtyp aus und klicken Sie auf im Widget. Nehmen Sie im daraufhin angezeigten Dialogfeld Ihre Änderungen vor und klicken Sie auf **Speichern**.
Durchschnittliche Ticket-Auflösungszeit	Dieses Widget zeigt die durchschnittlichen Auflösungszeiten eines Tickets nach einer der folgenden Kategorien an: • Kategorie • Priorität • Besitzer • Warteschlange • Monat Die resultierenden Daten können in einem *Balkendiagramm* oder einem *Ringdiagramm* angezeigt werden.

Widget	Beschreibung
	Um den Widget-Titel zu ändern, wählen Sie, wie Sie die Tickets gruppieren möchten, oder wählen Sie den Diagrammtyp aus und klicken Sie auf im Widget. Nehmen Sie im daraufhin angezeigten Dialogfeld Ihre Änderungen vor und klicken Sie auf **Speichern**.
Überfällige Tickets	Dieses Widget zeigt die Anzahl der derzeit überfälligen Service-Desk-Tickets an.

Anpassen des Service Desk-Dashboards

Sie können das Service Desk-Dashboard anpassen und Widgets nach Bedarf ein- oder ausblenden.

Diese Widgets sind auch im Home-Dashboard verfügbar, wenn sie installiert sind.

1. Rufen Sie die Seite *Service Desk-Dashboard* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Service Desk** und anschließend auf **Dashboard**.
2. Fahren Sie mit dem Mauszeiger über das Widget und verwenden Sie anschließend die folgenden Schaltflächen:
   - : Die Informationen im Widget aktualisieren
   - : Die Informationen zum Widget anzeigen
   - : Das Widget ausblenden
   - : Die Größe des Widgets ändern
   - : Das Widget an eine andere Position auf der Seite ziehen.
3. Titel, Diagrammtyp und die Gruppierung der Elemente in einigen Widgets können aktualisiert werden.

   Klicken Sie dazu auf im Widget. Nehmen Sie im daraufhin angezeigten Dialogfeld Ihre Änderungen vor und klicken Sie auf **Speichern**.
4. Klicken Sie auf die Schaltfläche **Anpassen** in der oberen rechten Ecke der Seite, um die verfügbaren Widgets anzuzeigen.
5. Um ein Widget anzuzeigen, das derzeit ausgeblendet ist, klicken Sie auf **Installieren**.

Verwalten von Service Desk-Tickets, -Prozessen und -Berichten

Zum Verwalten von Service Desk-Tickets, -Prozessen und -Berichten verwenden Sie die **Administratorkonsole**. Tickets können auch in der **Benutzerkonsole** und per E-Mail verwaltet werden.

Tickets können erst verwaltet werden, nachdem der Service Desk konfiguriert wurde. Siehe Einrichten des Service Desks.

Übersicht über den Lebenszyklus von Service Desk-Tickets

Service Desk-Tickets durchlaufen während ihres Lebenszyklus mehrere Phasen.

Zu diesen Phasen zählen:

1. Das Ticket wird über die Benutzerkonsole, die Administratorkonsole oder per E-Mail gesendet. Siehe Erstellen von Tickets über die Administratorkonsole und Benutzerkonsole und Erstellen und Verwalten von Tickets per E-Mail.
2. Das Ticket wird entsprechend den Ticketregeln einem Besitzer zugewiesen. Siehe Konfigurieren der Ticketeinstellungen und Verwenden von Ticketregeln.
3. Der Ticketbesitzer prüft das Ticket, korrigiert gegebenenfalls die Auswirkung und weist ihm eine Priorität zu.
4. Sind für die Warteschlange, in der sich das Ticket befindet, Service Level-Vereinbarungen aktiviert, wird das Ticket-Fälligkeitsdatum auf Grundlage der Priorität berechnet.
5. Falls es sich um ein einfaches Problem handelt, löst und schließt der Besitzer das Ticket und des werden E-Mail-Benachrichtigungen gesendet. Siehe Konfigurieren der E-Mail-Einstellungen.
6. Ein komplexes Ticket bleibt möglicherweise länger geöffnet und kann mehrere Besitzer haben.
7. Ist der Besitzer nicht in der Lage, das Ticket während der Eskalationsfrist zu lösen, wird das Ticket eskaliert. Siehe Verwenden des Prozesses zur Eskalation von Tickets.
8. Wenn Tickets geschlossen werden, können Benutzer eine Zufriedenheitsumfrage ausfüllen, um Feedback zum Umgang mit dem Ticket zu geben. Siehe Verwenden der Zufriedenheitsumfrage.
9. Das Ticket wird archiviert Siehe Archivieren, Wiederherstellen und Löschen von Tickets.

Erstellen von Tickets über die Administratorkonsole und Benutzerkonsole

Sie können Service Desk Tickets in der **Administratorkonsole** oder der **Benutzerkonsole** erstellen.

Tickets können auch per E-Mail erstellt werden. Siehe Erstellen und Verwalten von Tickets per E-Mail.

Erstellen von Tickets in der Benutzerkonsole

Sie können Service-Desk-Tickets in der **Benutzerkonsole** erstellen.

Wenn Sie Tickets in der **Benutzerkonsole** erstellen, werden Ihre Benutzerinformationen automatisch zum Feld *Absender* auf der Seite *Neues Ticket* hinzugefügt.

1. Rufen Sie die Seite *Neues Ticket* der Benutzerkonsole auf:
    a. Rufen Sie die Benutzerkonsole auf: `http://`**appliance_hostname**`/user`, wobei **appliance_hostname** der Hostname der Appliance ist.
    b. Klicken Sie in der linken Navigationsleiste auf **Service Desk** und anschließend auf **Tickets**.

c. Führen Sie zum Anzeigen der Seite *Neues Ticket* einen der folgenden Schritte aus:

- Wählen Sie **Aktion auswählen** > **Neu**.
- Klicken Sie auf **Aktion auswählen** > **Neues Ticket aus Warteschlange** > **Warteschlangenname**.
- Klicken Sie auf **Aktion auswählen** > **Neues Ticket aus Warteschlange** > **Warteschlangenname** > **Name der Ticketvorlage**
- Klicken Sie auf **Aktion auswählen** > **Neues Ticket aus Prozess** > **Prozessname**.

2. Wenn Sie ein neues Ticket aus einem Prozess erstellen und die Prozessvorlage zur Anzeige der Prozessbeschreibungsseite konfiguriert ist, überprüfen Sie die Informationen auf der Beschreibungsseite und klicken Sie auf **Fortfahren**.

   Diese Seite zeigt normalerweise einige wichtige Voraussetzungen, die Sie zunächst abschließen müssen, damit Sie mit der Erstellung eines Tickets fortfahren können. Wenn zum Beispiel die Prozessvorlage definiert, wie ein neuer Mitarbeiter zum System hinzuzufügen ist, können Sie Benutzer anweisen, zu überprüfen, ob der Mitarbeiter-Erfassungsvorgang abgeschlossen ist und ob die Mitarbeiter-ID erstellt wurde. Weitere Informationen zum Erstellen und Konfigurieren Prozessvorlagen finden Sie unter Hinzufügen, Bearbeiten und Aktivieren von Prozessvorlagen.

3. **Nur warteschlangenbasierte und Prozesstickets**. Geben Sie die folgenden Informationen an:

Option	Beschreibung
Titel	(Erforderlich) Eine kurze Beschreibung des Problems. Wenn dieses Feld in der zugeordneten Service Desk-Warteschlange angezeigt wird, wird einige Sekunden nach dem Beenden der Eingabe eine Liste mit Knowledge Base-Artikeln eingeblendet, die mit den in diesem Feld bereitgestellten Informationen verknüpft sind. Die vorgeschlagenen Artikel können Ihnen helfen, mehr über das Problem zu erfahren, und Ihr Problem zu lösen, bevor Sie ein Service Desk-Ticket erstellen.
Übersicht	Eine ausführlichere Beschreibung des Problems. Dieses Feld umfasst eine umfassende Reihe von Bearbeitungsoptionen zum Formatieren Ihrer Inhalte, wie Schaltflächen für fettgedruckten Text, Hyperlinks, Listen oder Textfarbe. Beispiel: • Um Fettdruck auf eine Textfolge anzuwenden, wählen Sie diese im Editor aus und klicken auf B. • Um Bilder hinzuzufügen, klicken Sie auf ▣, und geben Sie die URL der Bilddatei oder einen lokalen Dateipfad an, oder legen Sie das Bild einfach in dem angegebenen Bereich ab. ◦ Sie können Screenshots auch kopieren und direkt in das Textfeld einfügen. ◦ Alle Bilder, die Sie auf diese Weise einfügen, werden als Dateianhänge zum Ticket hinzugefügt. Sie sind

Option	Beschreibung
	gegebenenfalls auch in der E-Mail-Kommunikation enthalten. ◦ Wenn Sie ein Bild aus dem Textfeld löschen, wird der zugehörige Dateianhang nicht entfernt. Dateianhänge können Sie im Abschnitt *Anlage* der Ticket-Seite verwalten. Weitere Informationen hierzu finden Sie unter Screenshots und Anhänge zu Service-Desk-Tickets hinzufügen oder aus ihnen löschen. • Um externe Links hinzuzufügen, klicken Sie auf . • Um extern gehostete Videos einzubetten, klicken Sie auf .
Absender	Der Anmeldename des Benutzers, der das Ticket sendet. Der Absender kann durch Auswahl eines anderen Anmeldenamens in der Dropdown-Liste geändert werden.
Auswirkungen	Die Anzahl der Benutzer, die bei der Arbeit beeinträchtigt sind oder nicht arbeiten können.
Kategorie	Eine Klassifizierung des Problems.
Anhänge	Dateien, die zum Ticket hinzugefügt werden sollen. Sie können bis zu fünf Dateien einfügen. Siehe Screenshots und Anhänge zu Service-Desk-Tickets hinzufügen oder aus ihnen löschen.
Bildschirmaufnahmen	Bildschirmaufnahmen, die zum Ticket hinzugefügt werden sollen. Sie können bis zu fünf Bildschirmaufnahmen einfügen. Siehe Screenshots und Anhänge zu Service-Desk-Tickets hinzufügen oder aus ihnen löschen.

4. **Nur vorlagenbasierte Tickets.** Geben Sie die Informationen zu diesem Ticket an. Ticketfelder werden in der zugehörigen Ticketvorlage definiert.

   Weitere Informationen über Ticketvorlagen finden Sie unter Ticketvorlage konfigurieren.

5. Führen Sie einen der folgenden Schritte aus:
   - Klicken Sie auf **Speichern**, um das Ticket zu speichern und zur Liste *Ticket* zurückzukehren.
   - Klicken Sie auf **Änderungen übernehmen**, um das Ticket zu speichern und mit der Bearbeitung fortzufahren.
   - Klicken Sie auf **Abbrechen**, um die Änderungen am Ticket zu verwerfen.

   Wenn andere Benutzer das Ticket gleichzeitig geändert haben, wird das Dialogfeld *Aktualisierungsbenachrichtigung* angezeigt, wenn das Dialogfeld für die Warteschlange aktiviert ist und Sie der Ticketbesitzer oder ein Administrator sind. Dieses Dialogfeld wird nur Administratoren und Ticketbesitzern angezeigt. Anderen Benutzern wird es nicht angezeigt. Administratoren können die Konfliktwarnungsmeldung für jede Warteschlange separat aktivieren/deaktivieren. Siehe Aktivieren oder Deaktivieren der Konfliktwarnung.

Erstellen von Tickets auf der Ticketseite der Administratorkonsole

Sie können auf der Seite *Ticket* der **Administratorkonsole** nach Bedarf Service Desk-Tickets erstellen.

Wenn Sie auf der Seite *Ticket* der **Administratorkonsole** Tickets erstellen, werden Ihre Benutzerinformationen automatisch zum Feld *Absender* der Seite *Neues Ticket* hinzugefügt.

1. Rufen Sie die Seite *Neues Ticket* des Service Desks auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Service Desk** und anschließend auf **Tickets**.
   c. Führen Sie zum Anzeigen der Seite *Neues Ticket* einen der folgenden Schritte aus:
   - Wählen Sie **Aktion auswählen** > **Neu**.
   - Klicken Sie auf **Aktion auswählen** > **Neues Ticket aus Warteschlange** > **Warteschlangenname**.
   - Klicken Sie auf **Aktion auswählen** > **Neues Ticket aus Warteschlange** > **Warteschlangenname** > **Name der Ticketvorlage**
   - Klicken Sie auf **Aktion auswählen** > **Neues Ticket aus Prozess** > **Prozessname**.
2. Wenn Sie ein neues Ticket aus einem Prozess erstellen und die Prozessvorlage zur Anzeige der Prozessbeschreibungsseite konfiguriert ist, überprüfen Sie die Informationen auf der Beschreibungsseite und klicken Sie auf **Fortfahren**.

   Diese Seite zeigt normalerweise einige wichtige Voraussetzungen, die Sie zunächst abschließen müssen, damit Sie mit der Erstellung eines Tickets fortfahren können. Wenn zum Beispiel die Prozessvorlage definiert, wie ein neuer Mitarbeiter zum System hinzuzufügen ist, können Sie Benutzer anweisen, zu überprüfen, ob der Mitarbeiter-Erfassungsvorgang abgeschlossen ist und ob die Mitarbeiter-ID erstellt wurde. Weitere Informationen zum Erstellen und Konfigurieren Prozessvorlagen finden Sie unter Hinzufügen, Bearbeiten und Aktivieren von Prozessvorlagen.
3. **Nur warteschlangenbasierte und Prozesstickets**. Geben Sie die folgenden Informationen an:

Option	Beschreibung
Titel	(Erforderlich) Eine kurze Beschreibung des Problems.
Übersicht	Eine ausführlichere Beschreibung des Problems. Dieses Feld umfasst eine umfassende Reihe von Bearbeitungsoptionen zum Formatieren Ihrer Inhalte, wie Schaltflächen für fettgedruckten Text, Hyperlinks, Listen oder Textfarbe. Beispiel: • Um Fettdruck auf eine Textfolge anzuwenden, wählen Sie diese im Editor aus und klicken auf . • Um Bilder hinzuzufügen, klicken Sie auf , und geben Sie die URL der Bilddatei oder einen lokalen Dateipfad an, oder legen Sie

Option	Beschreibung
	das Bild einfach in dem angegebenen Bereich ab. ◦ Sie können Screenshots auch kopieren und direkt in das Textfeld einfügen. ◦ Alle Bilder, die Sie auf diese Weise einfügen, werden als Dateianhänge zum Ticket hinzugefügt. Sie sind gegebenenfalls auch in der E-Mail-Kommunikation enthalten. ◦ Wenn Sie ein Bild aus dem Textfeld löschen, wird der zugehörige Dateianhang nicht entfernt. Dateianhänge können Sie im Abschnitt *Anlage* der Ticket-Seite verwalten. Weitere Informationen hierzu finden Sie unter Screenshots und Anhänge zu Service-Desk-Tickets hinzufügen oder aus ihnen löschen. • Um externe Links hinzuzufügen, klicken Sie auf . • Um extern gehostete Videos einzubetten, klicken Sie auf .
Absender	Der Anmeldename des Benutzers, der das Ticket sendet. Der Absender kann durch Auswahl eines anderen Anmeldenamens in der Dropdown-Liste geändert werden. Klicken Sie auf , um die Kontaktinformationen des Absenders anzuzeigen. Wenn Sie ein untergeordnetes Ticket aus einer Prozessvorlage erstellen oder bearbeiten, haben Sie die Option, dieses Feld auf *Übergeordneter Eigentümer* oder *Übergeordneten Absender* des zugeordneten übergeordneten Tickets einzurichten.
Asset	Das Asset, auf das sich die Informationen im Ticket beziehen. Wählen Sie ein Asset aus der Dropdown-Liste aus. Klicken Sie auf , um die Asset-Details anzuzeigen.
Nach den dem Absender zugewiesenen Assets filtern	Filtern Sie die Asset-Liste basierend auf den Assets, die dem Absender zugewiesen sind. Dieses Kontrollkästchen ist standardmäßig aktiviert.
Gerät	Das Gerät, auf das sich die Informationen im Ticket beziehen. Falls irgendwelche Geräte dem Ticketabsender zugeordnet sind, werden sie hier aufgelistet, und das primäre Gerät des Absenders ist standardmäßig ausgewählt. Wählen Sie nach Bedarf ein Gerät aus der Dropdown-Liste aus. Klicken Sie auf , um die Gerätedetails anzuzeigen.

Option	Beschreibung
Nach den dem Absender zugewiesenen Geräten filtern	Filtern Sie die Geräte-Liste basierend auf den Geräten, die dem Absender zugewiesen sind. Falls irgendwelche Geräte dem Ticketabsender zugeordnet sind, erscheint diese Option auf dieser Seite standardmäßig als ausgewählt. Wenn Sie dieses Ticket jedoch auf der Seite *Ticketdetail* öffnen, ist diese Option nicht ausgewählt, und im Feld „Gerät“ ist das beim erstmaligen Erstellen des Tickets ausgewählte Gerät ausgewählt. Dies ist das standardmäßige Verhalten. Indem Sie dieses Kontrollkästchen deaktiviert lassen, verhindern Sie, dass Sie versehentlich ein Gerät auswählen, das eventuell in keiner Verbindung mit dem durch das Ticket angegebenen Problem steht.
Auswirkungen	Die Anzahl der Benutzer, die bei der Arbeit beeinträchtigt sind oder nicht arbeiten können.
Kategorie	Eine Klassifizierung des Problems.
Status	Der aktuelle Status des Tickets. Dieses Feld wird nicht angezeigt, wenn Sie ein Ticket aus einer Prozessvorlage erstellen oder bearbeiten.
Priorität	Die Bedeutung des Tickets.
Besitzer	Der Benutzer, der während des Lebenszyklus des Tickets für dessen Verwaltung verantwortlich ist. Wenn Sie ein untergeordnetes Ticket aus einer Prozessvorlage erstellen oder bearbeiten, haben Sie die Option, dieses Feld auf *Übergeordneter Eigentümer* oder *Übergeordneten Absender* des zugeordneten übergeordneten Tickets einzurichten. **TIPP:** Um sich selbst schnell ein Ticket zuzuweisen, klicken Sie auf der Listenseite *Tickets* in der Zeile mit dem Ticket auf .
Fällig	Datum und Uhrzeit für den geplanten Abschluss des Tickets. Falls keine Service Level-Vereinbarungen aktiviert sind, wird als Fälligkeitsdatum standardmäßig Kein(e) festgelegt. Sind Service Level-Vereinbarungen aktiviert, wird das Fälligkeitsdatum automatisch gemäß den SLA-Einstellungen berechnet. Das Fälligkeitsdatum wird basierend auf der Priorität berechnet, die beim Übermitteln des Tickets festgelegt wurde. Wurde die Priorität nach der Ticketübermittlung geändert, wird das berechnete Datum gemäß der neuen Priorität, jedoch basierend auf dem Datum und der Uhrzeit der ursprünglichen Übermittlung neu berechnet. Wird die Konfiguration der SLA-Auflösungszeit geändert, gilt sie nur für neue Tickets. Alte Tickets

Option	Beschreibung
	sind davon nicht betroffen. Siehe Konfigurieren von Service Level-Vereinbarungen. Wählen Sie **Manuelles Datum** aus, um Fälligkeitsdatum und -uhrzeit manuell festzulegen. Wenn Service Level-Vereinbarungen aktiviert sind, werden in diesem Fall Fälligkeitsdatum und -uhrzeit berechnet und als Option angezeigt, jedoch nicht ausgewählt.
CC-Liste	Eine Liste der Benutzer, die im Fall eines Ticketereignisses eine Benachrichtigungs-E-Mail erhalten. Die Empfänger in der CC-Liste erhalten eine E-Mail auf der Grundlage des Ticketereignisses und der für die Warteschlange **E-Mail bei Ereignissen** konfigurierten Einstellung **Ticket CC**.
Lösung	Die Lösung des mit dem Ticket verknüpften Problems. Dieses Feld umfasst eine umfassende Reihe von Bearbeitungsoptionen zum Formatieren Ihrer Inhalte, wie Schaltflächen für fettgedruckten Text, Hyperlinks, Listen oder Textfarbe. Beispiel: • Um Fettdruck auf eine Textfolge anzuwenden, wählen Sie diese im Editor aus und klicken auf B. • Um Bilder hinzuzufügen, klicken Sie auf , und geben Sie die URL der Bilddatei oder einen lokalen Dateipfad an, oder legen Sie das Bild einfach in dem angegebenen Bereich ab. ◦ Sie können Screenshots auch kopieren und direkt in das Textfeld einfügen. ◦ Alle Bilder, die Sie auf diese Weise einfügen, werden als Dateianhänge zum Ticket hinzugefügt. Sie sind gegebenenfalls auch in der E-Mail-Kommunikation enthalten. ◦ Wenn Sie ein Bild aus dem Textfeld löschen, wird der zugehörige Dateianhang nicht entfernt. Dateianhänge können Sie im Abschnitt *Anlage* der Ticket-Seite verwalten. Weitere Informationen hierzu finden Sie unter Screenshots und Anhänge zu

Option	Beschreibung
	Service-Desk-Tickets hinzufügen oder aus ihnen löschen. • Um externe Links hinzuzufügen, klicken Sie auf 🔗. • Um extern gehostete Videos einzubetten, klicken Sie auf 🎥.
Vordefinierte Antwort	Wenn Sie eine automatische Antwort als Lösung für dieses Ticket hinzufügen möchten, klicken Sie auf **Vordefinierte Antwort** und wählen Sie eine Antwortvorlage aus. Die ausgewählte Antwortvorlage wird im Feld **Auflösung** angezeigt. Sie können mehrere Antwortvorlagen als Auflösungseinträge hinzufügen. Sie werden in der Reihenfolge angezeigt, in der Sie sie ausgewählt haben. **TIPP:** Um eine Antwortvorlage zu erstellen oder zu bearbeiten, speichern Sie Ihre Änderungen und klicken Sie auf **Verwalten**. Dadurch gelangen Sie zur Seite *Antwortvorlagen*. Weitere Informationen über Antwortvorlagen finden Sie unter Antwortvorlagen anzeigen und bearbeiten.
Zugehörige Ticketinformationen	Dieser Abschnitt wird nicht angezeigt, wenn Sie ein Ticket aus einer Prozessvorlage erstellen.
Ticket hinzufügen	Um ein zusätzliches Ticket zu der zugehörigen Ticketinformation hinzuzufügen, klicken Sie.
Referrer	**Referrer** ist ein schreibgeschütztes Feld mit einem Ticketverweis auf ein Ticket, das mithilfe des Abschnitts **Siehe auch** auf dieses Ticket verweist.
Zusammengeführte Tickets	In diesem Abschnitt können Sie die Liste der Tickets bearbeiten, die mit diesem Ticket zusammengeführt wurden. Alle Tickets, die Sie zusammenführen möchten, müssen derselben Warteschlange angehören. Wenn Sie Tickets auf der Seite *Ticketdetails* zusammenführen, wird das offene Ticket zum Hauptticket. Alle anderen zusammengeführten Tickets werden archiviert, wenn Sie sie zusammenführen. Weitere Informationen finden Sie unter Zusammenführen von Tickets. Um ein zusammengeführtes Ticket hinzuzufügen, klicken Sie auf **Tickets zum Zusammenführen hinzufügen/Zusammengeführte Tickets bearbeiten** und wählen Sie ein Ticket aus der angezeigten Liste aus.
Prozessinformationen	Dieser Abschnitt wird nur angezeigt, wenn Sie ein Ticket aus einer Prozessvorlage erstellen. Alle Einstellungen in diesem Abschnitt sind

Option	Beschreibung
	schreibgeschützt. Umfassende Informationen zum Erstellen und Konfigurieren von Prozessvorlagen finden Sie unter Hinzufügen, Bearbeiten und Aktivieren von Prozessvorlagen.
Prozess	Der Name der diesem Ticket zugeordneten Prozessvorlage.
Prozesstyp	Der Prozesstyp. In einer Standardinstallation sind nur die Prozesstypen*Service Desk* und *Softwareanforderung: Genehmigung erforderlich* enthalten. Sie können falls erforderlich neue Prozesstypen erstellen. Sie können beispielsweise einen Prozesstyp für den Zugriff auf eine bestimmte Anwendung oder eine Gruppe von Anwendungen erstellen. Weitere Informationen hierzu finden Sie unter Prozesstypen definieren.
Prozessstatus	Der Status des dieser Prozessvorlage zugeordneten Workflows. Zum Beispiel *Genehmigung ausstehend*.
Übergeordnet	Der Name der diesem übergeordneten Ticket, wie in der Prozessvorlage, die diesem Ticket zugeordnet ist, definiert wurde.
Prozessgenehmigungen	Eine Liste aller Benutzer, die als Genehmiger für dieses Ticket zugordnet sind, falls zutreffend. • Wenn alle Genehmigungen für das Ticket eingegangen sind, wird dieser Abschnitt standardmäßig reduziert. Um die Genehmigungen zu prüfen, klicken Sie auf **Erweitern**. • Wenn eine oder mehrere Genehmigungen für dieses Ticket noch ausstehen, wird dieser Abschnitt angezeigt. Um sie auszublenden, klicken Sie auf **Reduzieren**. Die Genehmiger werden in Stufen aufgeführt, wie in der Prozessvorlage definiert. Jede Stufe kann je nach Bedarf einen oder mehrere Genehmiger haben. Die Einstellungen für Genehmiger und Stufe werden auch in diesem Abschnitt aufgeführt, wie z. B. Zeitlimit für Genehmigungen und die Benachrichtigungen. Wenn Sie einen Prozessticket erstellen, beginnt das Zeitlimit für den ersten Genehmiger. Wenn dieser Benutzer das Ticket genehmigt, beginnt das Zeitlimit für den nächsten usw. Wenn die mit diesem Prozess verbundene Prozessvorlage angibt, dass der Manager des Ticketabsenders ein Genehmiger für eine oder mehrere Stufen ist, und der angemeldete Benutzer ein Managerkonto damit verknüpft hat, erscheint der Benutzername des Managers in der Liste.

Option	Beschreibung
	Wenn das angemeldete Benutzerkonto nicht mit einem Manager verknüpft ist und die verbundene Prozessvorlage angibt, dass der Manager des Ticketabsenders die zugehörigen Prozesstickets genehmigen muss, wird beim Versuch, das Ticket zu speichern, eine Fehlermeldung angezeigt. Wenn jedoch der Manager des Ticketabsenders nur einer der Genehmiger ist, werden im Abschnitt *Prozessgenehmiger* die anderen Genehmiger aufgelistet, und Sie können das Ticket ohne Fehlermeldung speichern.
Prozessaktivitäten	Eine Liste der Prozessaktivitäten von denen jede ein untergeordnetes Ticket repräsentiert und in Stufen aufgeführt wird, wie in der Prozessvorlage definiert. Mehrere Tickets können der gleichen Stufe zugewiesen werden, falls das erforderlich sein sollte. Wenn z. B. die erste Stufe die Bestellung von Ausstattungen und Verbrauchsmaterialien für eine Neueinstellung ist, könnten mehrere separate untergeordnete Tickets für die Bestellung von Geräten, Büroausstattungen und Verbrauchsmaterialien sinnvoll sein, die alle Stufe 1 zugewiesen sind. Bei der Erstellung eines Prozesstickets werden alle der Stufe 1 zugewiesenen Prozesstickets automatisch erstellt. Tickets der Stufe 2 werden erstellt, wenn alle Tickets der Stufe 1 abgeschlossen sind. Tickets der Stufe 3 werden erstellt, wenn alle Tickets der Stufe 2 abgeschlossen sind usw. Wenn für eine der Genehmigungen eine Zeitüberschreitung eintritt, wird keines der untergeordneten Tickets in Bezug zu dieser oder einer späteren Stufe erstellt.
Ticket hinzufügen	Um ein zusätzliches Ticket zu der zugehörigen Ticketinformation hinzuzufügen, klicken Sie.
Referrer	**Referrer** ist ein schreibgeschütztes Feld mit einem Ticketverweis auf ein Ticket, das mithilfe des Abschnitts **Siehe auch** auf dieses Ticket verweist.
Kommentare	Kommentare, die zum Ticket hinzugefügt werden sollen. Außerdem können Sie Dateianhänge, Screenshots, automatische Antworten oder Inhalte aus Artikeln der Wissensdatenbank als Ticket-Kommentare hinzufügen. Weitere Informationen hierzu finden Sie unter: • Tickets Kommentare hinzufügen • Screenshots und Anhänge zu Service-Desk-Tickets hinzufügen oder aus ihnen löschen Wenn Sie eine automatische Antwort als Lösung für dieses Ticket hinzufügen möchten, klicken Sie auf **Vordefinierte Antwort** und wählen Sie eine Antwortvorlage aus.

Option	Beschreibung
	Die ausgewählte Antwortvorlage wird im Feld **Auflösung** angezeigt. Sie können mehrere Antwortvorlagen als Auflösungseinträge hinzufügen. Sie werden in der Reihenfolge angezeigt, in der Sie sie ausgewählt haben. **TIPP:** Um eine Antwortvorlage zu erstellen oder zu bearbeiten, speichern Sie Ihre Änderungen und klicken Sie auf **Verwalten**. Dadurch gelangen Sie zur Seite *Antwortvorlagen*. Weitere Informationen über Antwortvorlagen finden Sie unter Antwortvorlagen anzeigen und bearbeiten.
Knowledge Base-Artikel	Rufen Sie einen Wissensdatenbank-Artikel auf und fügen Sie seinen Inhalt zu den Ticket-Kommentaren hinzu. Weitere Informationen zu Knowledge Base-Artikeln finden Sie unter Verwalten von Knowledge Base-Artikeln.

4. **Nur vorlagenbasierte Tickets.** Geben Sie die Informationen zu diesem Ticket an. Ticketfelder werden in der zugehörigen Ticketvorlage definiert.

   Weitere Informationen über Ticketvorlagen finden Sie unter Ticketvorlage konfigurieren.

5. Führen Sie einen der folgenden Schritte aus:
   - Klicken Sie auf **Speichern**, um das Ticket zu speichern und zur Liste *Ticket* zurückzukehren.
   - Klicken Sie auf **Änderungen übernehmen**, um das Ticket zu speichern und mit der Bearbeitung fortzufahren.
   - Klicken Sie auf **Abbrechen**, um die Änderungen am Ticket zu verwerfen.

   Wenn andere Benutzer das Ticket gleichzeitig geändert haben, wird das Dialogfeld *Aktualisierungsbenachrichtigung* angezeigt, wenn das Dialogfeld für die Warteschlange aktiviert ist und Sie der Ticketbesitzer oder ein Administrator sind. Dieses Dialogfeld wird nur Administratoren und Ticketbesitzern angezeigt. Anderen Benutzern wird es nicht angezeigt. Administratoren können die Konfliktwarnungsmeldung für jede Warteschlange separat aktivieren/deaktivieren. Siehe Aktivieren oder Deaktivieren der Konfliktwarnung.

6. Überprüfen Sie alle im Dialogfeld *Aktualisierungsbenachrichtigung* angezeigten Änderungen:

Option	Beschreibung
Änderungen anderer Benutzer	Eine Übersicht der Änderungen, die von anderen Benutzern gesendet worden sind, während Sie das Ticket bearbeitet haben.
Ihre Änderungen	Eine Übersicht der Änderungen, die Sie für die gleichen in der Spalte *Änderungen anderer Benutzer* aufgeführten Felder senden. Diese Änderungen können zu Konflikten mit den von anderen Benutzern gesendeten Änderungen führen.

Option	Beschreibung
	HINWEIS: In dem Dialogfeld sind alle von anderen Benutzern durchgeführten Änderungen zusammengefasst. Ihre Änderungen werden jedoch nur zusammengefasst, wenn sie mit Änderungen anderer Benutzer in Konflikt stehen. Wenn ein anderer Benutzer ein Feld geändert hat, z. B. *Kategorie*, und Sie haben dieses Feld nicht geändert, wird die Änderung außerdem im Abschnitt *Geändert!* angezeigt. In der Spalte *Ihre Änderungen* wird „- -“ angezeigt. Das bedeutet, dass Sie keine Änderungen am Inhalt vorgenommen haben und die Änderungen der anderen Benutzer beibehalten werden.
Konflikt!	Bestimmte Änderungen widersprechen sich. Wenn Sie z. B. das Ticket *Kategorie* auf **Software** geändert haben und ein anderer Benutzer das Ticket *Kategorie* auf **Netzwerk** geändert hat, werden die Änderungen im Abschnitt *Konflikt!* zusammengefasst.
Geändert!	Eine Übersicht der Änderungen, die nicht in Konflikt stehen. Wenn Sie z. B. zum Ticket *Übersicht* Informationen hinzugefügt haben und ein anderer Benutzer **Auswirkungen** geändert hat, werden die Änderungen im Abschnitt *Geändert!* zusammengefasst.

7. Führen Sie einen der folgenden Schritte aus:
   - Klicken Sie auf **Speichern**, um das Ticket zu speichern und zur Liste *Ticket* zurückzukehren.
   - Klicken Sie auf **Änderungen übernehmen**, um das Ticket zu speichern und mit der Bearbeitung fortzufahren.
   - Klicken Sie auf **Abbrechen**, um die Änderungen am Ticket zu verwerfen.

   Wenn andere Benutzer das Ticket gleichzeitig geändert haben, wird das Dialogfeld *Aktualisierungsbenachrichtigung* angezeigt, wenn das Dialogfeld für die Warteschlange aktiviert ist und Sie der Ticketbesitzer oder ein Administrator sind. Dieses Dialogfeld wird nur Administratoren und Ticketbesitzern angezeigt. Anderen Benutzern wird es nicht angezeigt. Administratoren können die Konfliktwarnungsmeldung für jede Warteschlange separat aktivieren/deaktivieren. Siehe Aktivieren oder Deaktivieren der Konfliktwarnung.
8. Überprüfen Sie alle im Dialogfeld *Aktualisierungsbenachrichtigung* angezeigten Änderungen:

Option	Beschreibung
Änderungen anderer Benutzer	Eine Übersicht der Änderungen, die von anderen Benutzern gesendet worden sind, während Sie das Ticket bearbeitet haben.
Ihre Änderungen	Eine Übersicht der Änderungen, die Sie für die gleichen in der Spalte *Änderungen anderer Benutzer* aufgeführten Felder senden. Diese Änderungen können zu Konflikten mit den von anderen Benutzern gesendeten Änderungen führen.

Option	Beschreibung
	HINWEIS: In dem Dialogfeld sind alle von anderen Benutzern durchgeführten Änderungen zusammengefasst. Ihre Änderungen werden jedoch nur zusammengefasst, wenn sie mit Änderungen anderer Benutzer in Konflikt stehen. Wenn ein anderer Benutzer ein Feld geändert hat, z. B. *Kategorie*, und Sie haben dieses Feld nicht geändert, wird die Änderung außerdem im Abschnitt *Geändert!* angezeigt. In der Spalte *Ihre Änderungen* wird „- -“ angezeigt. Das bedeutet, dass Sie keine Änderungen am Inhalt vorgenommen haben und die Änderungen der anderen Benutzer beibehalten werden.
Konflikt!	Bestimmte Änderungen widersprechen sich. Wenn Sie z. B. das Ticket *Kategorie* auf **Software** geändert haben und ein anderer Benutzer das Ticket *Kategorie* auf **Netzwerk** geändert hat, werden die Änderungen im Abschnitt *Konflikt!* zusammengefasst.
Geändert!	Eine Übersicht der Änderungen, die nicht in Konflikt stehen. Wenn Sie z. B. zum Ticket *Übersicht* Informationen hinzugefügt haben und ein anderer Benutzer **Auswirkungen** geändert hat, werden die Änderungen im Abschnitt *Geändert!* zusammengefasst.

9. Führen Sie im Dialogfeld *Aktualisierungsbenachrichtigung* einen der folgenden Schritte aus:
   - Klicken Sie auf **Änderungen behalten**, um die von Ihnen vorgenommenen Änderungen zu speichern. Diese Option wird angezeigt, wenn Ihre Änderungen nicht mit den Änderungen anderer Benutzer in Konflikt stehen.

     HINWEIS: Wenn ein anderer Benutzer ein Feld geändert hat, z. B. *Kategorie*, und Sie haben das Feld nicht geändert, wird die Änderung im Abschnitt *Geändert!* angezeigt. In der Spalte *Ihre Änderungen* wird „- -“ angezeigt. Das bedeutet, dass Sie keine Änderungen am Inhalt vorgenommen haben und die Änderungen der anderen Benutzer beibehalten werden.
   - Klicken Sie auf **Konflikte überschreiben**, um die von Ihnen am Ticket vorgenommenen Änderungen zu speichern. Bei allen mit **Konflikt!** markierten Änderungen setzen Ihre Änderungen die Änderungen anderer Benutzer außer Kraft.
   - Klicken Sie auf **Abbrechen**, um zur Seite *Details zum Ticket* zurückzugelangen und das Ticket weiter zu bearbeiten.

Tickets über die Seite "Gerätedetail" erstellen

Sie können Service Desk-Tickets für Geräte nach Bedarf auf der Seite *Gerätedetail* erstellen.

Wenn Sie Service Desk-Tickets auf der Seite *Gerätedetail* erstellen, werden Benutzer- und Geräteinformationen automatisch zum Ticket hinzugefügt.

1. Rufen Sie die *Gerätedetailseite* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen

Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.

b. Klicken Sie in der linken Navigationsleiste auf **Inventar** und anschließend auf **Dashboard**.

c. Klicken Sie auf den Namen eines Geräts.

2. Klicken Sie im Abschnitt *Aktivitäten* auf **Service Desk-Tickets**, um eine Tabelle mit Tickets in Zusammenhang mit dem Gerät anzuzeigen.
3. Klicken Sie auf **Neu**, um die Seite *Neu* anzuzeigen.
   - Wenn Sie ein Ticket basierend auf einer Warteschlange erstellen möchten, wenn es mehrere Ticket-Warteschlangen in der Organisation gibt, wählen Sie eine Warteschlange aus der Dropdown-Liste **Ticket** aus.
   - Wenn Sie ein Ticket basierend auf einer Prozessvorlage erstellen möchten, wählen Sie den Prozess aus der Dropdown-Liste **Prozess** aus.

   Die Seite *Ticketdetail* wird angezeigt.
4. Geben Sie die erforderlichen Informationen ein. Eine Beschreibung der Ticketfelder finden Sie unter Erstellen von Tickets auf der Ticketseite der Administratorkonsole.
5. Führen Sie einen der folgenden Schritte aus:
   - Klicken Sie auf **Speichern**, um das Ticket zu speichern und zur Liste *Ticket* zurückzukehren.
   - Klicken Sie auf **Änderungen übernehmen**, um das Ticket zu speichern und mit der Bearbeitung fortzufahren.
   - Klicken Sie auf **Abbrechen**, um die Änderungen am Ticket zu verwerfen.

   Wenn andere Benutzer das Ticket gleichzeitig geändert haben, wird das Dialogfeld *Aktualisierungsbenachrichtigung* angezeigt, wenn das Dialogfeld für die Warteschlange aktiviert ist und Sie der Ticketbesitzer oder ein Administrator sind. Dieses Dialogfeld wird nur Administratoren und Ticketbesitzern angezeigt. Anderen Benutzern wird es nicht angezeigt. Administratoren können die Konfliktwarnungsmeldung für jede Warteschlange separat aktivieren/deaktivieren. Siehe Aktivieren oder Deaktivieren der Konfliktwarnung.

Tickets über die Seite "Asset-Detail" erstellen

Sie können Service Desk-Tickets für Assets nach Bedarf auf der Seite *Asset-Detail* erstellen.

Wenn Sie Service Desk-Tickets auf der Seite *Asset-Detail* erstellen, werden Benutzer- und Geräteinformationen automatisch zum Ticket hinzugefügt.

1. Rufen Sie die Seite *Asset-Detail* auf:

   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.

   b. Klicken Sie in der linken Navigationsleiste auf **Asset Management** und anschließend auf **Assets**.

   c. Klicken Sie auf den Namen eines Assets.

   Im Abschnitt **Service Desk-Tickets** wird eine Tabelle mit Tickets in Zusammenhang mit dem Asset angezeigt.
2. Klicken Sie auf **Neu**, um die Seite *Neu* anzuzeigen.
   - Wenn Sie ein Ticket basierend auf einer Warteschlange erstellen möchten, wenn es mehrere Ticket-Warteschlangen in der Organisation gibt, wählen Sie eine Warteschlange aus der Dropdown-Liste **Ticket** aus.
   - Wenn Sie ein Ticket basierend auf einer Prozessvorlage erstellen möchten, wählen Sie den Prozess aus der Dropdown-Liste **Prozess** aus.

Die Seite *Ticketdetail* wird angezeigt.

3. Geben Sie die erforderlichen Informationen ein. Eine Beschreibung der Ticketfelder finden Sie unter Erstellen von Tickets auf der Ticketseite der Administratorkonsole.
4. Führen Sie einen der folgenden Schritte aus:
   - Klicken Sie auf **Speichern**, um das Ticket zu speichern und zur Liste *Ticket* zurückzukehren.
   - Klicken Sie auf **Änderungen übernehmen**, um das Ticket zu speichern und mit der Bearbeitung fortzufahren.
   - Klicken Sie auf **Abbrechen**, um die Änderungen am Ticket zu verwerfen.

   Wenn andere Benutzer das Ticket gleichzeitig geändert haben, wird das Dialogfeld *Aktualisierungsbenachrichtigung* angezeigt, wenn das Dialogfeld für die Warteschlange aktiviert ist und Sie der Ticketbesitzer oder ein Administrator sind. Dieses Dialogfeld wird nur Administratoren und Ticketbesitzern angezeigt. Anderen Benutzern wird es nicht angezeigt. Administratoren können die Konfliktwarnungsmeldung für jede Warteschlange separat aktivieren/deaktivieren. Siehe Aktivieren oder Deaktivieren der Konfliktwarnung.

Service-Desk-Tickets aus Warnungen erstellen

Sie können anhand einer Serverüberwachungswarnung ein Service Desk-Ticket erstellen. Die Felder im Ticketformular werden dabei automatisch mit den Informationen aus der Warnung ausgefüllt.

1. Führen Sie zum Anzeigen der Liste *Überwachungswarnungen* einen der folgenden Schritte aus:
   - **Wenn das Widget** *Überwachungswarnungen* **installiert und das** *Dashboard* **geöffnet ist, klicken Sie auf Überwachungswarnungen.**
   - **Klicken Sie in der linken Navigationsleiste auf Überwachung > Warnungen.**
2. Aktivieren Sie das Kontrollkästchen für die Zeile mit der Warnmeldung und klicken Sie anschließend auf **Aktion auswählen** > **Neues Ticket**.
   - Wenn Sie ein Ticket basierend auf einer Warteschlange erstellen möchten, wenn es mehrere Ticket-Warteschlangen in der Organisation gibt, wählen Sie eine Warteschlange aus der Dropdown-Liste **Ticket** aus.
   - Wenn Sie ein Ticket basierend auf einer Prozessvorlage erstellen möchten, wählen Sie den Prozess aus der Dropdown-Liste **Prozess** aus.

   Die Felder *Titel*, *Übersicht*, *Absender* und *Gerät* enthalten Informationen aus der Warnung.
3. **Optional**: Ändern Sie die Angaben in den Feldern *Titel* und *Übersicht* entsprechend den Verfahrensweisen Ihres Unternehmens.
4. Füllen Sie das Formular mit den weiteren erforderlichen Informationen aus und klicken Sie anschließend auf **Speichern**, um das Ticket zu speichern und die Seite *Details zum Ticket* zu schließen. Oder klicken Sie auf **Änderungen übernehmen**, um das Ticket zu speichern und seine Bearbeitung fortzusetzen.

Option	Beschreibung
Titel	(Erforderlich) Eine kurze Beschreibung des Problems. Sie können den von der Überwachungsfunktion generierten Titel durch einen Titel Ihrer Wahl ersetzen.
Übersicht	Eine ausführlichere Beschreibung des Problems. Dieses Feld umfasst eine umfassende Reihe von Bearbeitungsoptionen zum Formatieren Ihrer Inhalte, wie Schaltflächen für fettgedruckten Text, Hyperlinks, Listen oder Textfarbe.

Option	Beschreibung

	Beispiel:
	• Um Fettdruck auf eine Textfolge anzuwenden, wählen Sie diese im Editor aus und klicken auf B.
	• Um Bilder hinzuzufügen, klicken Sie auf, und geben Sie die URL der Bilddatei oder einen lokalen Dateipfad an, oder legen Sie das Bild einfach in dem angegebenen Bereich ab.
	  ◦ Sie können Screenshots auch kopieren und direkt in das Textfeld einfügen.
	  ◦ Alle Bilder, die Sie auf diese Weise einfügen, werden als Dateianhänge zum Ticket hinzugefügt. Sie sind gegebenenfalls auch in der E-Mail-Kommunikation enthalten.
	  ◦ Wenn Sie ein Bild aus dem Textfeld löschen, wird der zugehörige Dateianhang nicht entfernt. Dateianhänge können Sie im Abschnitt *Anlage* der Ticket-Seite verwalten. Weitere Informationen hierzu finden Sie unter Screenshots und Anhänge zu Service-Desk-Tickets hinzufügen oder aus ihnen löschen.
	• Um externe Links hinzuzufügen, klicken Sie auf.
	• Um extern gehostete Videos einzubetten, klicken Sie auf.

Absender	Der Anmeldename des Benutzers, der das Ticket sendet. Der Absender kann durch Auswahl eines anderen Anmeldenamens in der Dropdown-Liste geändert werden. Klicken Sie auf, um die Kontaktinformationen des Absenders anzuzeigen.
Asset	Das Asset, auf das sich die Informationen im Ticket beziehen. Wählen Sie ein Asset aus der Dropdown-Liste aus. Klicken Sie auf, um die Asset-Details anzuzeigen.
Nach den dem Absender zugewiesenen Assets filtern	Filtern Sie die Asset-Liste basierend auf den Assets, die dem Absender zugewiesen sind.
Gerät	Das Gerät, auf das sich die Informationen im Ticket beziehen. Diese Informationen werden von der Überwachungsfunktion bereitgestellt. Klicken Sie auf, um die Gerätedetails anzuzeigen.

Option	Beschreibung
Nach den dem Absender zugewiesenen Geräten filtern	Filtern Sie die Asset-Liste basierend auf den Geräten, die dem Absender zugewiesen sind.
Auswirkungen	Die Anzahl der Benutzer, die bei der Arbeit beeinträchtigt sind oder nicht arbeiten können.
Kategorie	Eine Klassifizierung des Problems.
Status	Der aktuelle Status des Tickets. Dieses Feld wird nicht angezeigt, wenn Sie ein Ticket aus einer Prozessvorlage erstellen oder bearbeiten.
Priorität	Die Bedeutung des Tickets.
Besitzer	Der Benutzer, der während des Lebenszyklus des Tickets für dessen Verwaltung verantwortlich ist.
Fällig	Datum und Uhrzeit für den geplanten Abschluss des Tickets. Falls keine Service Level-Vereinbarungen aktiviert sind, wird als Fälligkeitsdatum standardmäßig Kein(e) festgelegt. Sind Service Level-Vereinbarungen aktiviert, wird das Fälligkeitsdatum automatisch gemäß den SLA-Einstellungen berechnet. Das Fälligkeitsdatum wird basierend auf der Priorität berechnet, die beim Übermitteln des Tickets festgelegt wurde. Wurde die Priorität nach der Ticketübermittlung geändert, wird das Fälligkeitsdatum gemäß der neuen Priorität, jedoch basierend auf dem Datum und der Uhrzeit der ursprünglichen Übermittlung neu berechnet. Wird die Konfiguration der SLA-Auflösungszeit geändert, gilt sie nur für neue Tickets. Alte Tickets sind davon nicht betroffen. Siehe Konfigurieren von Service Level-Vereinbarungen. Wählen Sie **Manuelles Datum** aus, um Fälligkeitsdatum und -uhrzeit manuell festzulegen. Wenn Service Level-Vereinbarungen aktiviert sind, werden in diesem Fall Fälligkeitsdatum und -uhrzeit berechnet und als Option angezeigt, jedoch nicht ausgewählt.
CC-Liste	Eine Liste der Benutzer, die im Fall eines Ticketereignisses eine Benachrichtigungs-E-Mail erhalten. Die Empfänger in der CC-Liste erhalten eine E-Mail auf der Grundlage des Ticketereignisses und der für die Warteschlange **E-Mail bei Ereignissen** konfigurierten Einstellung **Ticket CC**.
Lösung	Die Lösung des mit dem Ticket verknüpften Problems.

Option	Beschreibung

	Dieses Feld umfasst eine umfassende Reihe von Bearbeitungsoptionen zum Formatieren Ihrer Inhalte, wie Schaltflächen für fettgedruckten Text, Hyperlinks, Listen oder Textfarbe.
	Beispiel:
	• Um Fettdruck auf eine Textfolge anzuwenden, wählen Sie diese im Editor aus und klicken auf B.
	• Um Bilder hinzuzufügen, klicken Sie auf , und geben Sie die URL der Bilddatei oder einen lokalen Dateipfad an, oder legen Sie das Bild einfach in dem angegebenen Bereich ab.
	  ◦ Sie können Screenshots auch kopieren und direkt in das Textfeld einfügen.
	  ◦ Alle Bilder, die Sie auf diese Weise einfügen, werden als Dateianhänge zum Ticket hinzugefügt. Sie sind gegebenenfalls auch in der E-Mail-Kommunikation enthalten.
	  ◦ Wenn Sie ein Bild aus dem Textfeld löschen, wird der zugehörige Dateianhang nicht entfernt. Dateianhänge können Sie im Abschnitt *Anlage* der Ticket-Seite verwalten. Weitere Informationen hierzu finden Sie unter Screenshots und Anhänge zu Service-Desk-Tickets hinzufügen oder aus ihnen löschen.
	• Um externe Links hinzuzufügen, klicken Sie auf .
	• Um extern gehostete Videos einzubetten, klicken Sie auf .

Zugehörige Ticketinformationen	Dieser Abschnitt wird nicht angezeigt, wenn Sie ein Ticket aus einer Prozessvorlage erstellen.
Ticket hinzufügen	Um ein zusätzliches Ticket zu der zugehörigen Ticketinformation hinzuzufügen, klicken Sie.
Referrer	**Referrer** ist ein schreibgeschütztes Feld mit einem Ticketverweis auf ein Ticket, das mithilfe des Abschnitts **Siehe auch** auf dieses Ticket verweist.
Zusammengeführte Tickets	In diesem Abschnitt können Sie die Liste der Tickets bearbeiten, die mit diesem Ticket zusammengeführt wurden. Alle Tickets, die Sie zusammenführen möchten, müssen derselben Warteschlange angehören. Wenn Sie Tickets auf der Seite *Ticketdetails* zusammenführen, wird das offene Ticket zum Hauptticket. Alle anderen zusammengeführten Tickets werden archiviert, wenn

Option	Beschreibung
	Sie sie zusammenführen. Weitere Informationen finden Sie unter Zusammenführen von Tickets. Um ein zusammengeführtes Ticket hinzuzufügen, klicken Sie auf **Tickets zum Zusammenführen hinzufügen/Zusammengeführte Tickets bearbeiten** und wählen Sie ein Ticket aus der angezeigten Liste aus.
Prozessinformationen	Dieser Abschnitt wird nur angezeigt, wenn Sie ein Ticket aus einer Prozessvorlage erstellen. Alle Einstellungen in diesem Abschnitt sind schreibgeschützt. Umfassende Informationen zum Erstellen und Konfigurieren von Prozessvorlagen finden Sie unter Hinzufügen, Bearbeiten und Aktivieren von Prozessvorlagen
Prozess	Der Name der diesem Ticket zugeordneten Prozessvorlage.
Prozesstyp	Der Prozesstyp.
Prozessstatus	Der Status des dieser Prozessvorlage zugeordneten Workflows. Zum Beispiel *Genehmigung ausstehend*.
Übergeordnet	Der Name der diesem übergeordneten Ticket, wie in der Prozessvorlage, die diesem Ticket zugeordnet ist, definiert wurde.
Prozessgenehmigungen	Eine Liste aller Benutzer, die als Genehmiger für dieses Ticket zugordnet sind, falls zutreffend. Die Genehmiger werden in Stufen aufgeführt, wie in der Prozessvorlage definiert. Jede Stufe kann je nach Bedarf einen oder mehrere Genehmiger haben. Die Einstellungen für Genehmiger und Stufe werden auch in diesem Abschnitt aufgeführt, wie z. B. Zeitlimit für Genehmigungen und die Benachrichtigungen. Wenn Sie einen Prozessticket erstellen, beginnt das Zeitlimit für den ersten Genehmiger. Wenn dieser Benutzer das Ticket genehmigt, beginnt das Zeitlimit für den nächsten usw.
Prozessaktivitäten	Eine Liste der Prozessaktivitäten von denen jede ein untergeordnetes Ticket repräsentiert und in Stufen aufgeführt wird, wie in der Prozessvorlage definiert. Mehrere Tickets können der gleichen Stufe zugewiesen werden, falls das erforderlich sein sollte. Wenn z. B. die erste Stufe die Bestellung von Ausstattungen und Verbrauchsmaterialien für eine Neueinstellung ist, könnten mehrere separate untergeordnete Tickets für die Bestellung von Geräten, Büroausstattungen und Verbrauchsmaterialien sinnvoll sein, die alle Stufe 1 zugewiesen sind. Bei der Erstellung eines Prozesstickets werden alle der Stufe 1 zugewiesenen Prozesstickets automatisch erstellt.

Option	Beschreibung
	Tickets der Stufe 2 werden erstellt, wenn alle Tickets der Stufe 1 abgeschlossen sind. Tickets der Stufe 3 werden erstellt, wenn alle Tickets der Stufe 2 abgeschlossen sind usw.
Ticket hinzufügen	Um ein zusätzliches Ticket zu der zugehörigen Ticketinformation hinzuzufügen, klicken Sie.
Referrer	**Referrer** ist ein schreibgeschütztes Feld mit einem Ticketverweis auf ein Ticket, das mithilfe des Abschnitts **Siehe auch** auf dieses Ticket verweist.
Kommentare	Kommentare, die zum Ticket hinzugefügt werden sollen. Außerdem können Sie Dateianhänge, Screenshots, automatische Antworten oder Inhalte aus Artikeln der Wissensdatenbank als Ticket-Kommentare hinzufügen. Weitere Informationen hierzu finden Sie unter: • Tickets Kommentare hinzufügen • Screenshots und Anhänge zu Service-Desk-Tickets hinzufügen oder aus ihnen löschen Wenn Sie eine automatische Antwort als Lösung für dieses Ticket hinzufügen möchten, klicken Sie auf **Vordefinierte Antwort** und wählen Sie eine Antwortvorlage aus. Die ausgewählte Antwortvorlage wird im Feld **Auflösung** angezeigt. Sie können mehrere Antwortvorlagen als Auflösungseinträge hinzufügen. Sie werden in der Reihenfolge angezeigt, in der Sie sie ausgewählt haben. **TIPP:** Um eine Antwortvorlage zu erstellen oder zu bearbeiten, speichern Sie Ihre Änderungen und klicken Sie auf **Verwalten**. Dadurch gelangen Sie zur Seite *Antwortvorlagen*. Weitere Informationen über Antwortvorlagen finden Sie unter Antwortvorlagen anzeigen und bearbeiten.
Knowledge Base-Artikel	Rufen Sie einen Wissensdatenbank-Artikel auf und fügen Sie seinen Inhalt zu den Ticket-Kommentaren hinzu. Weitere Informationen zu Knowledge Base-Artikeln finden Sie unter Verwalten von Knowledge Base-Artikeln.

Verwandte Themen

Verwalten von Service Desk-Tickets, -Prozessen und -Berichten

Erstellen und Verwalten von Tickets per E-Mail

Sie können Benutzern die Möglichkeit geben, Tickets per E-Mail zu erstellen und zu verwalten. Dies ist nützlich für Benutzer, die keinen Zugriff auf die **Administratorkonsole** oder **Benutzerkonsole** der Appliance haben.

Informationen zu Anhängen für per E-Mail erstellte Tickets

Benutzer können Dateien an Service-Desk-Tickets anhängen, die per E-Mail übermittelt werden. Die maximale Dateigröße für Anhänge beträgt 8 MB.

E-Mails mit Anhängen, die größer als 8 MB sind, werden abgelehnt. Für den Benutzer wird in einem solchen Fall keine Fehlermeldung angezeigt.

Ticketerstellung per E-Mail aktivieren

Sie können Benutzern die Möglichkeit geben, Service-Desk-Tickets per E-Mail zu erstellen und zu verwalten.

1. Rufen Sie die Seite *Details zum Ticket* des Service Desks auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Service Desk** und anschließend auf **Konfiguration**.
   c. Klicken Sie im Fensterbereich **Konfiguration** auf **Warteschlangen**.
   d. Klicken Sie auf den Namen einer Warteschlange.
2. Richten Sie ein gültiges E-Mail-Konto ein, beispielsweise Support@meinedomäne.com, ein, an das Benutzer E-Mails senden können, um Tickets zu erstellen.
3. Fügen Sie die E-Mail-Adresse dem Feld *Alternative E-Mail-Adresse* hinzu.
4. Aktivieren Sie das Kontrollkästchen **Alle Benutzer als Absender zulassen**.
5. Aktivieren Sie das Kontrollkästchen **E-Mails von unbekannten Benutzern annehmen**.

   Wenn **E-Mails von unbekannten Benutzern annehmen** in der Warteschlangenkonfiguration aktiviert ist, kann in allen zum Erstellen eines Tickets an die Service Desk-Warteschlange gesendeten E-Mails das Feld *Absender* festgelegt werden. In diesem Fall muss der Benutzername im Token **@submitter** übergeben werden und es muss sich dabei um den Namen eines vorhandenen Benutzers bzw. bei einem unbekannten Benutzer um die aktuelle E-Mail-Adresse handeln.

   Wenn die Option **E-Mails von unbekannten Benutzern annehmen** deaktiviert ist, ist der oben genannte Vorgang nur möglich, wenn die E-Mail-Adresse des Absenders bereits mit einem Service Desk-Benutzerkonto verknüpft ist.
6. Klicken Sie auf **Speichern**.

Aus E-Mails erstellte Tickets erhalten die auf der Seite *Warteschlangen-Detail* festgelegten Standardwerte für Auswirkung, Kategorie und Priorität. Der Text der E-Mail-Nachricht wird als Kommentar hinzugefügt. Das Feld *Absender* wird von der E-Mail-Adresse des Absenders abgeleitet.

Ticket per E-Mail erstellen

Sie können ein Ticket schnell per E-Mail erstellen, wenn Sie den Namen der Ticketvorlage in der Betreffzeile der E-Mail angeben.

1. Melden Sie sich bei Ihrem E-Mail-Konto an und erstellen Sie eine neue E-Mail-Nachricht.
2. Geben Sie in der Betreffzeile der E-Mail den Namen der Ticketvorlage in Klammern an. Beispiel: `{Druckerprobleme}`.

   Wenn Sie die Ticketvorlage nicht angeben, verwendet die Appliance die Standardticketvorlage, die mit der Warteschlange verknüpft ist.
3. Beschreiben Sie Ihr Problem in der E-Mail-Nachricht und senden Sie sie an die E-Mail-Adresse, die mit der Warteschlange verknüpft ist, zu der die angegebene Ticketvorlage gehört.

Informationen zum Konfigurieren der Warteschlangen-E-Mail-Einstellungen finden Sie unter Warteschlangen-spezifische E-Mail-Einstellungen konfigurieren.

4. Wenn Sie eine E-Mail-Bestätigung vom Service Desk erhalten, klicken Sie auf den Link in der E-Mail, um den Inhalt des Tickets zu überprüfen, und

   Die Seite *Ticketdetails* wird mit dem neu erstellten Ticket angezeigt.

5. Nehmen Sie die gewünschten Änderungen vor.

   Weitere Informationen zum Bearbeiten der Ticketseite finden Sie unter Erstellen von Tickets auf der Ticketseite der Administratorkonsole.

Ticketattribute per E-Mail ändern

Sie können Ticketattribute per E-Mail mithilfe der E-Mail-Variablen mit dem Symbol **@** ändern, die sich am Anfang von E-Mails befinden.

Text nach der letzten E-Mail-Variablen wird zum Feld *Kommentar* des Tickets hinzugefügt.

Wenn Sie beispielsweise den folgenden E-Mail-Text senden, wird das Ticket abgeschlossen, der Ticketbesitzer geändert und ein Kommentar hinzugefügt:

```
status=abgeschlossen
@owner=joe
Ich habe das Problem behoben. Falls es erneut auftritt, wenden Sie sich an Joe.
```

Wenn Sie ungültige Felder oder Feldwerte eingeben, werden Fehler ausgegeben. Diese werden Ihnen über die E-Mail-Fehlervorlage gemeldet. Weitere Informationen zu E-Mail-Vorlagen finden Sie unter E-Mail-Auslöser und E-Mail-Vorlagen konfigurieren.

Ticketfeld per E-Mail löschen

Sie können jedes Feld löschen, indem Sie eine E-Mail mit der entsprechenden Syntax senden.

Die Syntax lautet wie folgt: @Feldname=. Beispielsweise löscht der folgende Eintrag das Feld *Fälligkeitsdatum*:

```
@due_date=
```

Ticketfelder per E-Mail ändern

Sie können die folgenden Ticketattribute mithilfe von E-Mail-Nachrichten ändern, wenn der Wert des Ticketfelds auf *Vom Benutzer änderbar* festgelegt ist.

Informationen zum Ändern der Berechtigungen für Ticketfelder finden Sie unter Verwenden von Ticketgenehmigern.

Feld	Beschreibung
@category	Eine gültige Kategorie.
@cc_list	Eine durch Kommas getrennte Liste von E-Mail-Adressen oder E-Mail-Verteiler.
@due_date	Ein Fälligkeitsdatum. Das Datum kann in einem beliebigen Format angegeben werden, beispielsweise 03.04.2014, 3. April 2014 oder nächsten Freitag.
@impact	Eine gültige Ticketauswirkung.

Feld	Beschreibung
@owner	Benutzername, vollständiger Name oder die E-Mail-Adresse des Besitzers.
@priority	Eine gültige Ticketpriorität.
@resolution	Eine Lösung.
@status	Ein gültiger Ticketstatus.
@submitter	Benutzername, vollständiger Name oder die E-Mail-Adresse des Absenders. Diese E-Mail-Adresse wird für die Felder "Benutzername" und "E-Mail-Adresse" verwendet. Der vollständige Name wird auf den Teil *Name* der E-Mail-Adresse festgelegt. Beispiel: **name**@domain.com.
@title	Ein Titel für das Ticket.
@summary	Eine ausführlichere Beschreibung des Problems.
@asset	Das mit der Lizenz verknüpfte Asset.
@machine	Das mit dem Ticket verknüpfte Gerät.
@approval	Der Status des Ticket-Genehmigungsprozesses. Sie können dieses Feld auf einen der folgenden Werte festlegen: `Genehmigt`, `Abgelehnt`, `Kein(e)` oder `Weitere Informationen erforderlich`.
@approval_note	Eine mit der Genehmigung verknüpfte Notiz.
@owners_only	Gibt an, ob nur Inhaber das Ticket per E-Mail kommentieren können. Bei Einstellung auf `1` ist die Kennzeichnung `True`. Jeder andere numerische Wert setzt diesen Indikator auf `False`.
@custom_<number>	Der Wert eines benutzerdefinierten Ticketfelds, wobei `<number>` die ID des benutzerdefinierten Felds ist. Beispielsweise weist `$custom_2=ABC` den Wert `ABC` dem benutzerdefinierten Ticketfeld `CUSTOM_2` zu.

Ticketgenehmigungsfelder per E-Mail ändern

Als Ticketgenehmiger definierte Benutzer können die folgenden Genehmigungsfelder mithilfe von E-Mail-Nachrichten ändern.

Genehmiger können die folgenden Genehmigungsfelder ändern:

Feld	Beschreibung
@approval	Damit ändern Sie das Ticket. Verwenden Sie eine der folgenden Optionen: **Genehmigt**, **Abgelehnt**, **Kein(e)** oder **Weitere Informationen erforderlich**.
@approver	Damit ändern Sie den Ticketgenehmiger. Geben Sie einen Benutzernamen aus dem Ticketgenehmigungslabel ein. Anweisungen zum Einrichten des Labels mit Genehmigern finden Sie unter Verwenden von Ticketgenehmigern.
@approval_note	Geben Sie einen Kommentar ein.

Benutzerdefinierte Felder per E-Mail festlegen oder ändern

Sie können benutzerdefinierte Felder für Service-Desk-Tickets festlegen, indem Sie eine E-Mail mit der entsprechenden Syntax senden.

Die Syntax lautet wie folgt: @benutzerdefinierter_feldname=neuer_wert.

Benutzerdefinierte Felder dürfen keine Leerzeichen enthalten. Verwenden Sie zwischen Wörtern einen Unterstrich. Beispiel: neuer_Wert.

Außerdem haben Sie folgende Möglichkeiten:

- @priority = hoch
- @priority = sehr_dringend

Verwenden Sie für benutzerdefinierte Mehrfachauswahlfelder eine durch Kommas getrennte Liste der Werte. Ungültige Werte in benutzerdefinierten Auswahl- oder Mehrfachauswahlfeldern verursachen Fehler.

Anzeigen von Tickets und Verwalten von Kommentaren, Arbeit und Anhängen

Über Links auf Detailseiten können Sie zwischen Tickets und den dazugehörigen Geräten und Assets navigieren. Darüber hinaus können Sie Arbeitsinformationen, Kommentare und Anhänge wie z. B. Screenshots hinzufügen.

Auf den Detailseiten für Tickets sind die zugehörigen Geräte und Assets aufgeführt und für den schnellen Zugriff verknüpft. Auf ähnliche Weise können Sie auf den Detailseiten für Geräte und Assets auf die dazugehörigen Tickets zugreifen. Außerdem können Sie über die Detailseiten für Geräte und Assets Tickets anzeigen und erstellen.

Zwischen Tickets, dazugehörigen Geräten und Assets navigieren

Auf den Ticketdetailseiten sind Links verfügbar, die Ihnen die Navigation zwischen zugehörigen Service Desk-Tickets sowie den zugehörigen Geräten und Assets ermöglichen.

1. Rufen Sie die Seite *Details zum Ticket* des Service Desks auf:
    a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.

b. Klicken Sie in der linken Navigationsleiste auf **Service Desk** und anschließend auf **Tickets**.
c. Klicken Sie auf den Titel eines Tickets.

2. Zeigen Sie Tickets nach Absender, Asset oder Gerät an.
   - **Klicken Sie auf Ticket-Verlauf - Absender.**
   - **Klicken Sie auf Ticket-Verlauf - Asset.**
   - **Klicken Sie auf Ticket-Verlauf - Gerät.**

   In einem neuen Fenster werden alle Tickets für das Asset mit Ticketnummer, Titel und Status angezeigt.

   Klicken Sie auf den Link in der Spalte *Nummer* oder *Titel*, um die Seite *Details zum Ticket* anzuzeigen.
3. Zeigen Sie zugehörige Tickets im Abschnitt *Zugehörige Ticket-Informationen* an.
   - **Klicken Sie auf ein Ticket mit dem Verweis** *Siehe auch***.**
   - **Klicken Sie auf ein Ticket mit dem Verweis** *Referrer***.**
   - **Klicken Sie auf ein Ticket mit dem Verweis** *Zusammengeführtes Ticket***.**
   - **Klicken Sie auf ein Ticket mit dem Verweis** *Untergeordnetes Ticket***.**
   - **Klicken Sie auf ein Ticket mit dem Verweis** *Übergeordnetes Ticket***.**

   Für das ausgewählte Ticket wird das Fenster *Details zum Ticket* angezeigt.

Arbeitsinformationen zu Tickets hinzufügen

Sie können Service Desk-Tickets Arbeitsinformationen hinzufügen, beispielsweise das Datum des Beginns oder Endes der Arbeit, die Gesamtzahl der für das Ticket aufgewendeten Stunden sowie Notizen zu den durchgeführten Arbeiten. Diese Informationen stehen Ticketabsendern und -besitzern zur Verfügung.

1. Rufen Sie die Seite *Details zum Ticket* des Service Desks auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Service Desk** und anschließend auf **Tickets**.
   c. Klicken Sie auf den Titel eines Tickets.
2. Klicken Sie unten auf der Seite auf die Registerkarte **Arbeit**.
3. Klicken Sie auf **Hinzufügen**.
4. Geben Sie die folgenden Informationen an:

Option	Beschreibung
Datum	Das Datum, an dem die Arbeit beginnt. Um dieses Datum zu ändern, klicken Sie ins Datumsfeld und wählen ein anderes Datum aus. Klicken Sie zum Entfernen des Datums auf **Löschen**.
Start	Die Uhrzeit, zu der die Arbeit beginnt (24-Stunden-Format).
Ende	Die Uhrzeit, zu der die Arbeitet endet (24-Stunden-Format).
Anpassung	Der zu den protokollierten Stunden zu addierende oder zu subtrahierende Zeitraum. Dies kann zu Abrechnungs- oder Verfolgungszwecken nützlich

Option	Beschreibung
	sein. So kann beispielsweise die Arbeit an einem Ticket um 08:00 beginnen und um 12:00 enden. Die tatsächliche Zeit, die ein Administrator für die Arbeit an dem Ticket aufgewendet hat, beträgt jedoch möglicherweise 2 Stunden. Sie können dann in dieses Feld -2,0 eingeben, um die tatsächlich aufgewendete Zeit genau zu melden.
Hinweis	Geben Sie nach Bedarf beliebige weitere Informationen ein.

5. Klicken Sie auf **Tätigkeit hinzufügen**.

Benutzerdefinierte Ansichten für Tickets verwenden

Es sind mehrere integrierte Systemansichten verfügbar, mit denen Sie die auf der Seite *Tickets* angezeigten Tickets einschränken können.

1. Rufen Sie die Seite *Ticket* des Service Desks auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Service Desk** und anschließend auf **Tickets**.

   Die Seite *Tickets* zeigt die Tickets in der Standardwarteschlange.
2. Wählen Sie zum Einschränken der in der Warteschlange angezeigten Tickets eine Ansicht in der Dropdown-Liste **Anzeigen nach** aus.

   Folgende integrierte Ansichten sind verfügbar:

Gruppe	Ansicht
Eigene Tickets	Alle meine Tickets **HINWEIS:** Diese Ansicht enthält alle Tickets, die vom jeweiligen Benutzer gesendet wurden, deren Besitzer er ist oder für die er als Genehmiger festgelegt ist. Meine aktiven Tickets **HINWEIS:** Diese Ansicht enthält alle Tickets, die vom jeweiligen Benutzer gesendet wurden oder ihm zugewiesen sind und den Status Geöffnet oder Angehalten aufweisen. Meine heute übermittelten Tickets Meine heute fälligen Tickets Meine überfälligen Tickets Meine letzten Tickets
Meine Tickets nach Zustand	Meine Tickets mit Status "Eröffnet" Meine Tickets mit Status "Angehalten" Meine Tickets mit Status "Abgeschlossen"

Gruppe	Ansicht
	Meine Tickets mit Status "Nicht abgeschlossen"
Meine Tickets nach Status	**HINWEIS:** Diese Option ist nur beim Anzeigen einer bestimmten Warteschlange vorhanden. Meine Neu-Tickets Meine Offen-Tickets Meine Abgeschlossen-Tickets Meine Weitere Infos erforderlich-Tickets
Alle Tickets	Alle Tickets Alle aktiven nicht zugewiesenen Tickets **HINWEIS:** Diese Ansicht enthält alle Tickets, denen kein Besitzer zugewiesen ist und die den Status Geöffnet oder Angehalten aufweisen. Die Ansicht ist nur verfügbar, wenn der angemeldete Benutzer ein Besitzer der ausgewählten Warteschlange ist. Alle heute übermittelten Tickets Alle heute fälligen Tickets Alle überfälligen Tickets
Alle Tickets nach Zustand	Alle Tickets mit Status "Eröffnet" Alle Tickets mit Status "Angehalten" Alle Tickets mit Status "Geschlossen" Alle Tickets mit Status "Nicht abgeschlossen"
Alle Tickets nach Status	**HINWEIS:** Diese Option ist nur beim Anzeigen einer bestimmten Warteschlange vorhanden. Alle Neu-Tickets Alle Geöffnet-Tickets Alle Abgeschlossen-Tickets Alle Weitere Infos erforderlich-Tickets
Meine Mitarbeiter-Tickets nach Zustand	**HINWEIS:** Diese Option wird nur angezeigt, wenn: • Ihr Benutzerkonto eine Managerrolle hat und ein oder mehrere Mitarbeiterkonten damit verknüpft sind. • Sie die **Benutzerkonsole** verwenden. **HINWEIS:** Administratoren können diese Funktion auf der Seite *Warteschlangen-Einstellungen* ausschalten. Meine Mitarbeiter-Tickets: Geöffnet

Gruppe	Ansicht
	Meine Mitarbeiter-Tickets: Angehalten Meine Mitarbeiter-Tickets: abgeschlossen Meine Mitarbeiter-Tickets: Nicht geschlossen
Label "Absender"	<Label "Absender">
Benutzerdefinierte Ansicht	Liste der verfügbaren benutzerdefinierten Ansichten. **HINWEIS:** Diese Option wird nur angezeigt, wenn benutzerdefinierte Ansichten vorhanden sind, die vom angemeldeten Benutzer erstellt wurden.

Legen Sie die benutzerdefinierte Ansicht als Standardeinstellung fest. Siehe Ansicht als Standardeinstellung für Tickets festlegen.

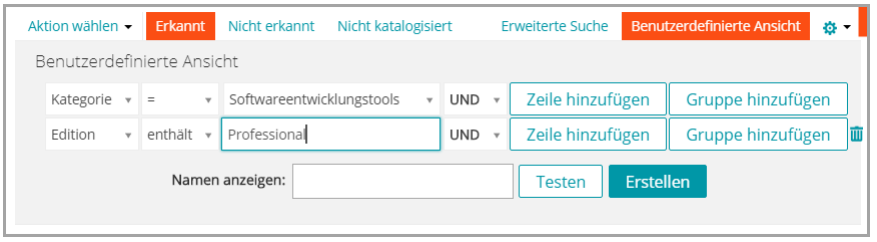
Benutzerdefinierte Ansichten für Tickets erstellen

Sie können benutzerdefinierte Ansichten erstellen, um den Typ oder die Anzahl der auf der Seite *Tickets* angezeigten Service-Desk-Tickets zu beschränken. Auf diese Weise werden Ihnen nur die gewünschten Tickets angezeigt.

HINWEIS: Benutzerdefinierte Ansichten stehen nur für die Benutzerkonten zur Verfügung, in denen sie erstellt wurden. Sie stehen nicht für mehrere Benutzerkonten zur Verfügung. Wenn Sie anderen Benutzern den Zugriff auf eine von Ihnen erstellte benutzerdefinierte Ansicht ermöglichen möchten, senden Sie ihnen die URL der benutzerdefinierten Ansicht.

1. Rufen Sie die Seite *Ticket* des Service Desks auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Service Desk** und anschließend auf **Tickets**.
2. Klicken Sie oberhalb der Liste rechts auf die Registerkarte **Benutzerdefinierte Ansicht**.

   Der Bereich *Benutzerdefinierte Ansicht* wird angezeigt.



3. Geben Sie die Kriterien an, die für die benutzerdefinierte Ansicht verwendet werden sollen. Sie könnten beispielsweise eine benutzerdefinierte Ansicht erstellen, in der offene Tickets mit der Priorität Hoch angezeigt werden:
4. Klicken Sie auf **Testen**, um die Ergebnisse zu überprüfen.
5. Klicken Sie auf **Erstellen**, um die benutzerdefinierte Ansicht zu speichern.

Legen Sie die benutzerdefinierte Ansicht als Standardeinstellung fest. Siehe Ansicht als Standardeinstellung für Tickets festlegen.

Ansicht als Standardeinstellung für Tickets festlegen

Sie können eine Ansicht als Standardeinstellung für die Seite *Tickets* des Service Desks anpassen. Die Standardansicht ist benutzerspezifisch und muss für jeden Benutzer einzeln konfiguriert werden.

1. Rufen Sie die Seite *Tickets* des Service Desks auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Service Desk** und anschließend auf **Tickets**.
2. **Optional**: Klicken Sie rechts über der Liste auf die Registerkarte **Benutzerdefinierte Ansicht** und wählen Sie die Einstellungen für die benutzerdefinierte Ansicht aus. Siehe Benutzerdefinierte Ansichten für Tickets erstellen.
3. Wählen Sie **Aktion auswählen** > **Standardansicht festlegen** > **Aktuelle Ansicht als Standard festlegen** aus.

   Die aktuelle Ansicht wird als Standardansicht für den angemeldeten Benutzer für die Liste *Tickets* gespeichert.

Tickets Kommentare hinzufügen

Einem Ticket können während der Bearbeitung Kommentare hinzugefügt werden, um zusätzliche Informationen zum Ticket bereitzustellen.

1. Rufen Sie die Seite *Details zum Ticket* des Service Desks auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Service Desk** und anschließend auf **Tickets**.
   c. Klicken Sie auf den Titel eines Tickets.
2. Klicken Sie unten auf der Seite "Details zum Ticket" auf die Registerkarte **Kommentare**, sofern sie noch nicht geöffnet ist.
3. Geben Sie den Kommentar in das Textfeld **Kommentar** ein.

   Dieses Feld umfasst eine umfassende Reihe von Bearbeitungsoptionen zum Formatieren Ihrer Inhalte, wie Schaltflächen für fettgedruckten Text, Hyperlinks, Listen oder Textfarbe.

   Beispiel:

   - Um Fettdruck auf eine Textfolge anzuwenden, wählen Sie diese im Editor aus und klicken auf B.
   - Um Bilder hinzuzufügen, klicken Sie auf , und geben Sie die URL der Bilddatei oder einen lokalen Dateipfad an, oder legen Sie das Bild einfach in dem angegebenen Bereich ab.
     - Sie können Screenshots auch kopieren und direkt in das Textfeld einfügen.
     - Alle Bilder, die Sie auf diese Weise einfügen, werden als Dateianhänge zum Ticket hinzugefügt. Sie sind gegebenenfalls auch in der E-Mail-Kommunikation enthalten.
     - Wenn Sie ein Bild aus dem Textfeld löschen, wird der zugehörige Dateianhang nicht entfernt. Dateianhänge können Sie im Abschnitt *Anlage* der Ticket-Seite verwalten. Weitere Informationen

hierzu finden Sie unter Screenshots und Anhänge zu Service-Desk-Tickets hinzufügen oder aus ihnen löschen.

- Um externe Links hinzuzufügen, klicken Sie auf .
- Um extern gehostete Videos einzubetten, klicken Sie auf .

4. Aktivieren Sie das Kontrollkästchen **Nur Besitzer**, wenn der Kommentar für andere Personen als Besitzer (beispielsweise Absender) ausgeblendet und nur für Ticketbesitzer angezeigt werden soll.
5. Wenn Sie dem Ticket einen Anhang hinzufügen möchten, klicken Sie auf **Anhang hinzufügen** und wählen Sie die anzuhängende Datei aus.

   Sie können einem Ticket bis zu fünf Dateianhänge hinzufügen. Weitere Informationen hierzu finden Sie unter Screenshots und Anhänge zu Service-Desk-Tickets hinzufügen oder aus ihnen löschen
6. Wenn Sie dem Ticket einen Screenshot hinzufügen möchten, klicken Sie auf **Screenshot einfügen** und fügen Sie den Screenshot in das angezeigte Dialogfeld ein.

   Sie können bis zu fünf Bildschirmaufnahmen hinzufügen. Weitere Informationen hierzu finden Sie unter Screenshots und Anhänge zu Service-Desk-Tickets hinzufügen oder aus ihnen löschen
7. Wenn Sie eine automatische Antwort als Kommentar zu diesem Ticket hinzufügen möchten, klicken Sie auf **Vordefinierte Antwort** und wählen Sie eine Antwortvorlage aus.

   Die ausgewählte Antwortvorlage wird im Feld **Kommentare** angezeigt. Sie können mehrere Antwortvorlagen als Kommentare hinzufügen. Sie werden in der Reihenfolge angezeigt, in der Sie sie ausgewählt haben.

   TIPP: Um eine Antwortvorlage zu erstellen oder zu bearbeiten, speichern Sie Ihre Änderungen und klicken Sie auf **Verwalten**. Dadurch gelangen Sie zur Seite *Antwortvorlagen*.

   Weitere Informationen über Antwortvorlagen finden Sie unter Antwortvorlagen anzeigen und bearbeiten.
8. Wenn Sie den Inhalt eines Knowledge Base-Artikels als Kommentar zu diesem Ticket hinzufügen möchten, klicken Sie auf **Knowledge Base-Artikel** und wählen Sie ein gültiges Thema aus.

   Die ausgewählte Antwortvorlage wird im Feld **Kommentare** angezeigt.

   Weitere Informationen zu Knowledge Base-Artikeln finden Sie unter Verwalten von Knowledge Base-Artikeln.
9. Falls Sie ein Ticket anzeigen, für das Sie bereits Kommentare bereitgestellt haben und Ihre eigenen Kommentare bearbeiten möchten, so können Sie das tun, falls die mit dem Ticket verknüpfte Warteschlange so konfiguriert ist, dass Benutzer ihre eigenen Kommentare bearbeiten können. Informationen zum Konfigurieren der Warteschlangen-Voreinstellungen Sie unter Ticketwarteschlangen konfigurieren.
10. Falls Sie ein Ticket anzeigen, das Sie eingesendet haben und die Kommentare anderer Benutzer bearbeiten möchten, so können Sie das tun, falls die mit dem Ticket verknüpfte Warteschlange so konfiguriert ist, dass Techniker die von anderen Benutzern eingesendeten Kommentare bearbeiten können. Informationen zum Konfigurieren der Warteschlangen-Voreinstellungen Sie unter Ticketwarteschlangen konfigurieren.
11. Falls Ihr Konto eine Managerrolle hat, wird die mit dem Ticket verknüpfte Warteschlange so konfiguriert, dass Manager Kommentare zu Mitarbeitertickets bearbeiten können. Falls Sie also ein Ticket anzeigen, das von Ihrem Mitarbeiter eingesendet wurde, können Sie Kommentare hinzufügen und bearbeiten oder auch nach Bedarf Dateianhänge oder Screenshots zum Ticket hinzufügen. Informationen zum Konfigurieren der Warteschlangen-Voreinstellungen Sie unter Ticketwarteschlangen konfigurieren.
12. Wenn ein verwandter Knowledge Base-Artikel an die Ticketkommentare angehängt werden soll, wählen Sie den Artikel in der Dropdown-Liste aus. Sie können einen Suchbegriff eingeben, um nach einem bestimmten Artikel zu suchen.
13. Klicken Sie auf **Senden**, um den neuen Kommentar zu speichern.

HINWEIS: Kommentare werden unabhängig von allen anderen Ticketinformationen gespeichert. Falls auf Kommentaren basierende E-Mail-Benachrichtigungen aktiviert sind, erhalten die festgelegten Empfänger umgehend eine E-Mail für den hinzugefügten Kommentar. Wenn Benutzer auf eine E-Mail-Benachrichtigung im Zusammenhang mit einem vorhandenen Ticket antworten, wird nur der neue Text, den sie über der Antwortzeile eingeben, als Kommentar hinzugefügt.

Tickets Kommentare nur für Besitzer hinzufügen

Sie können Ticket-Kommentare hinzufügen, die für andere Personen als die Besitzer (beispielsweise Absender) nicht angezeigt werden und nur für Ticketbesitzer sichtbar sind.

Beim Hinzufügen von Kommentaren, die nur für Besitzer bestimmt sind, ist zu berücksichtigen, dass andere Ticketbesitzer zur Änderung dieser Einstellung berechtigt sind. Kommentare nur für Besitzer werden bei der Änderung der Einstellung für andere Benutzer sichtbar.

Quest empfiehlt für Kommentare nur für Besitzer die folgenden Best Practices:

- Gehen Sie beim Hinzufügen von Kommentaren immer umsichtig vor.
- Legen Sie eine eindeutige, gut dokumentierte Richtlinie für das Ändern der Einstellung *Nur Besitzer* fest.

1. Rufen Sie die Seite *Details zum Ticket* des Service Desks auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Service Desk** und anschließend auf **Tickets**.
   c. Klicken Sie auf den Titel eines Tickets.
2. Klicken Sie unten auf der Seite "Details zum Ticket" auf die Registerkarte **Kommentare**, sofern sie noch nicht geöffnet ist.
3. Aktivieren Sie das Kontrollkästchen **Nur Besitzer** und fügen Sie dann den Kommentar, den Verweis auf einen Knowledge Base-Artikel oder den Anhang hinzu.

   HINWEIS: Das Kontrollkästchen **Nur Besitzer** kann durch Aktivieren des Kontrollkästchens **Standardmäßige Ticket-Besitzerkommentare für die Anzeige "Nur Besitzer"** auf der Seite "Warteschlangen-Detail" standardmäßig aktiviert werden. Siehe Ticketwarteschlangen konfigurieren.
4. Klicken Sie auf **Senden**.

   HINWEIS: Kommentare werden unabhängig von allen anderen Ticketinformationen gespeichert.

   Der Kommentar wird zum Ticket hinzugefügt. Die Anzeige erfolgt nur für Ticketbesitzer, es sei denn, ein Benutzer mit den entsprechenden Berechtigungen deaktiviert das Kontrollkästchen *Nur Besitzer*.

Ticket-Kommentare anzeigen

Bei der Bearbeitung eines Tickets werden Kommentare angezeigt, wenn Sie die Registerkarte **Kommentar** auswählen. Die Kommentare werden auch zusammen mit anderen Verlaufseinträgen auf der Registerkarte **Verlauf** angezeigt.

1. Rufen Sie die Seite *Details zum Ticket* des Service Desks auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Service Desk** und anschließend auf **Tickets**.

c. Klicken Sie auf den Titel eines Tickets.

2. Klicken Sie unten auf der Seite *Details zum Ticket* auf die Registerkarte **Kommentare**.

   Eine Liste der Kommentare, die dem Ticket hinzugefügt wurden, wird unter der Registerkarte **Kommentare** angezeigt.

3. Aktivieren Sie das Kontrollkästchen **Nur Anhänge anzeigen**, um die Kommentarliste zu filtern und nur Kommentare mit Anhängen anzuzeigen.

Screenshots und Anhänge zu Service-Desk-Tickets hinzufügen oder aus ihnen löschen

In jedes Service Desk-Ticket können bis zu fünf Screenshots eingefügt werden. Darüber hinaus können Sie jedem Ticket bis zu fünf Dateien als Anhang hinzufügen.

So fügen Sie Screenshots in Tickets ein:

- Der zu erfassende Inhalt muss auf dem Bildschirm sichtbar sein und Sie müssen in der Zwischenablage Ihres Computers einen Screenshot speichern können.
- Für den Zugriff auf die **Administratorkonsole** benötigen Sie einen unterstützten Browser, außer Safari. Eine vollständige Liste der unterstützten Browser finden Sie in den *Technischen Daten*.

> **HINWEIS:** Die Funktion zum Einfügen von Screenshots ist verborgen, wenn Sie eine frühere Version oder einen nicht unterstützten Browser verwenden. Sie können aber trotzdem Screenshots als Dateien an Tickets anhängen.

Um Dateien anhängen zu können, müssen Sie von der **Administratorkonsole** aus nach Dateien suchen können. Sie können Dateien mit einer Größe von bis zu 8 MB anhängen.

Wenn Sie Screenshots und Anhänge zu einem Ticket hinzufügen, werden diese in einem separaten Abschnitt des Ticketbildschirms angezeigt. Sie können auch Bilder (einschließlich Screenshots) direkt zu den Feldern *Zusammenfassung* und *Kommentar* hinzufügen. Weitere Informationen hierzu finden Sie unter Erstellen von Tickets auf der Ticketseite der Administratorkonsole.

1. Führen Sie eine der folgenden Aktionen aus, um in der Zwischenablage Ihres Computers einen Screenshot zu speichern (der zu erfassende Inhalt muss dabei auf dem Bildschirm sichtbar sein):
   - Drücken Sie unter Windows die Taste **Druck**.
   - Drücken Sie auf einem Mac gleichzeitig die folgenden Tasten: **Befehlstaste**, **Umschalttaste** und **3**.

   Der Screenshot wird in die Zwischenablage Ihres Computers kopiert.

2. Rufen Sie die Seite *Details zum Ticket* des Service Desks auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Service Desk** und anschließend auf **Tickets**.
   c. Führen Sie zum Anzeigen der Seite *Details zum Ticket* einen der folgenden Schritte aus:
      - Wählen Sie **Aktion auswählen** > **Neu**.
      - Klicken Sie auf **Aktion auswählen** > **Neues Ticket aus Warteschlange** > **Warteschlangenname**.
      - Klicken Sie auf den Namen eines Tickets.

3. So hängen Sie einen Screenshot an das Ticket an:
   a. Blättern Sie auf der Seite *Ticketdetail* zum Abschnitt *Anlagen* der Registerkarte *Kommentare*, und klicken Sie auf **Anlage hinzufügen**.

b. Wählen Sie im daraufhin angezeigten Dialogfeld des Dateibrowsers die Datei aus, die Sie dem Ticket zuordnen möchten, und öffnen Sie sie.

   Der Dateibrowser wird geschlossen und der Dateiname der Anlage wird im Abschnitt *Anlage* unter **Anlage hinzufügen** angezeigt. Sie können einem Ticket bis zu fünf Dateianhänge hinzufügen.

c. Klicken Sie unten auf der Seite auf **Senden** und dann zur Bestätigung auf **Änderungen übernehmen**.

   Der Kommentar wird zum Ticket hinzugefügt.

4. So hängen Sie einen Screenshot an das Ticket an:
   a. Scrollen Sie auf der Seite *Ticketdetail* zum Ende der Seite und klicken Sie auf der Registerkarte *Kommentare* im Abschnitt *Anlage* auf **Screenshot einfügen**.

      Das Dialogfeld *Live-Chat* wird angezeigt.

   b. Erfassen Sie einen Screenshot, kopieren Sie ihn in die Zwischenablage.
   c. Verwenden Sie eine der folgenden Tastenkombinationen, um den Screenshot in das Dialogfenster einzufügen:

   - Halten Sie unter Windows die Taste **Strg** gedrückt und drücken Sie dann die Taste **V**.
   - Halten Sie beim Mac die **Befehlstaste** gedrückt und drücken Sie dann die Taste **V**.

      Der Screenshot wird im Dialogfeld *Screenshot einfügen* angezeigt.

   d. Klicken Sie auf **Screenshot hinzufügen**.

      Das Dialogfeld *Screenshot einfügen* wird geschlossen und der dem Screenshot zugewiesene Dateiname wird im Abschnitt *Anlage* unter **Screenshot einfügen** angezeigt. Sie können einem Ticket bis zu fünf Screenshots hinzufügen.

   e. Klicken Sie unten auf der Seite auf **Änderungen übernehmen**.

      Der Screenshot wird zum Ticket hinzugefügt.

5. So löschen Sie einen Screenshot oder eine Anlage von einem Ticket:
   a. Scrollen Sie auf der Seite *Details zum Ticket* nach unten zum Abschnitt *Anhänge* der Registerkarte *Kommentare*.
   b. Um eine Dateianlage zu löschen, suchen Sie unter **Anlage hinzufügen** die zu löschende Datei und klicken Sie auf rechts neben dem Dateinamen.
   c. Um einen Screenshot zu löschen, suchen Sie unter **Screenshot einfügen** die Datei mit dem Screenshot, den Sie löschen möchten, und klicken Sie auf rechts neben dem Dateinamen.
   d. Klicken Sie unten auf der Seite auf **Änderungen übernehmen**.

      Die Datei wird von dem Ticket entfernt.

6. Klicken Sie unten auf der Seite auf **Speichern**, um die Änderungen zu übernehmen.

Ticketaktivitätsverlauf anzeigen

Auf der Registerkarte Verlauf wird ein Verlauf aller für das Ticket ausgeführten Aktivitäten angezeigt. Der Verlauf enthält auch Änderungen an Ticketdetailfeldern und Kommentaren.

1. Rufen Sie die Seite *Details zum Ticket* des Service Desks auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Service Desk** und anschließend auf **Tickets**.

c. Klicken Sie auf den Titel eines Tickets.

2. Klicken Sie unten auf der Seite "Details zum Ticket" auf die Registerkarte **Verlauf**.

Ticketinformationen per E-Mail senden

Service Desk-Ticketinformationen können bei Bedarf manuell an Empfänger per E-Mail gesendet werden.

Der Inhalt und das Format der E-Mail werden durch die Benachrichtigungsvorlage *Ticket manuell per E-Mail senden* **vorgegeben. Auch zeigt der Token** *$ticket_fields_visible* **in der Vorlage alle Felder, die der angemeldete Benutzer beim Senden der E-Mail sehen kann. Siehe E-Mail-Auslöser und E-Mail-Vorlagen konfigurieren.**

1. Rufen Sie die Seite *Details zum Ticket* des Service Desks auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Service Desk** und anschließend auf **Tickets**.
   c. Klicken Sie auf den Titel eines Tickets.
2. Wählen Sie **Aktion auswählen > Ticket per E-Mail senden** aus.
3. Geben Sie auf der Seite *Ticket per E-Mail senden* die **E-Mail-Adresse** des Empfängers an und ändern Sie ggf. den **Betreff**.
4. Klicken Sie auf **Senden**.

   Die Ticketinformationen werden per E-Mail an den angegebenen Empfänger gesendet.

Geräteaktionen über Tickets ausführen

Für Geräte, die Service Desk Tickets zugewiesen sind, können Sie die Geräteaktionen über die Seite *Ticket Detail* ausführen.

- Geräteaktionen wurden hinzugefügt. Siehe Abschnitt *Geräteaktionen* unter Allgemeine Appliance-Einstellungen ohne aktivierte Organisationskomponente konfigurieren.
- Geräte wurden Tickets zugewiesen.
- Sie greifen mit einem zulässigen Browser auf die **Administratorkonsole** zu. Siehe https://support.quest.com/kb/148787.

1. Rufen Sie die Seite *Details zum Ticket* des Service Desks auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Service Desk** und anschließend auf **Tickets**.
   c. Klicken Sie auf den Titel eines Tickets.
2. Wählen Sie direkt unter der Dropdown-Liste *Gerät* in der Dropdown-Liste *Aktion* eine Geräteaktion aus.

   Es wird sofort versucht, die ausgewählte Geräteaktion auf dem Remotegerät auszuführen.

Zusammenführen von Tickets

Wenn Sie eine Reihe verwandter Tickets haben, die noch aktiv sind, müssen Sie diese nicht separat verwalten, sondern können sie zu einem einzigen Ticket zusammenführen und dieses eine Ticket verwalten, ohne die Ticket-Spuren aller zusammengeführten Tickets zu verlieren.

Wenn Sie Tickets zusammenführen, müssen Sie ein Hauptticket auswählen. Die anderen Tickets werden automatisch archiviert. Der gesamte Verlauf der zusammengeführten Tickets bleibt unverändert. Der Ticketverlauf zeigt auch an, wenn ein Ticket zusammengeführt wird.

Sie können nur Tickets zusammenführen, die in derselben Warteschlange vorhanden sind. Tickets, die zur gleichen Warteschlange gehören, aber mit verschiedenen Vorlagen erstellt wurden, können zusammengeführt werden. Die mit der Hauptticketvorlage verknüpften Felder bleiben erhalten, während die untergeordneten Ticketfelder entfernt und archiviert werden. Diese Funktion ist nur verfügbar, wenn die Ticketarchivierung aktiviert ist.

Service-, übergeordnete, untergeordnete und bereits zusammengeführte Tickets können nicht zusammengeführt werden. Nur Tickets ohne übergeordnetes bzw. untergeordnetes Element können zusammengeführt werden.

Sie können die Zusammenführung von Tickets nach Bedarf löschen. Alle Benutzer auf der CC-Liste eines Tickets, die während des Zusammenführungsprozesses hinzugefügt werden, bleiben auf der Liste, wenn die Zusammenführung des Tickets aufgehoben wird.

Tickets über die Seite „Ticketliste“ zusammenführen

Sie können die Seite *Ticketliste* verwenden, um Tickets zusammenzuführen und ein Hauptticket festzulegen.

1. Wählen Sie die Tickets aus, die Sie zusammenführen möchten.
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie auf **Service Desk**, um die Seite *Tickets* anzuzeigen.
   c. Klicken Sie auf der Seite *Ticketliste* auf **Warteschlange** und wählen Sie die Warteschlange mit den Tickets aus, die Sie zusammenführen möchten.
   d. Wählen Sie alle Tickets aus, die Sie zusammenführen möchten.
2. Führen Sie die ausgewählten Tickets zusammen.
   a. Klicken Sie im Menü *Aktion auswählen* auf **Tickets zusammenführen**.

      Das Dialogfeld *Tickets zusammenführen* wird angezeigt.

   b. Geben Sie im Dialogfeld *Tickets zusammenführen* das Ticket an, das Sie als Hauptticket auswählen möchten, und klicken Sie auf **Speichern**.

      Das Dialogfeld *Tickets zusammenführen* wird geschlossen und das Dialogfeld *Bestätigen* wird angezeigt, das darauf hinweist, dass alle Tickets (mit Ausnahme der Haupttickets) archiviert werden.

   c. Klicken Sie im Meldungsfeld *Bestätigen* auf **Ja**, um mit der Zusammenführung fortzufahren.

Tickets über die Seite „Ticketdetail“ zusammenführen

Sie können ein oder mehrere Tickets mit dem angezeigten Ticket auf der Seite *Ticketdetail* zusammenführen. Alle Tickets, die Sie zusammenführen möchten, müssen derselben Warteschlange angehören.

Wenn Sie Tickets auf der Seite *Ticketdetails* zusammenführen, wird das offene Ticket zum Hauptticket. Alle anderen zusammengeführten Tickets werden archiviert, wenn Sie sie zusammenführen. Weitere Informationen finden Sie unter Zusammenführen von Tickets.

1. Öffnen Sie ein Ticket, das Sie mit einem oder mehreren anderen Tickets zusammenführen möchten.
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Service Desk** und anschließend auf **Tickets**.
   c. Klicken Sie auf den Titel eines Tickets.

   Die Seite *Ticketdetail* wird angezeigt.
2. Führen Sie ein oder mehrere Tickets mit dem ausgewählten Ticket zusammen.
   a. Klicken Sie auf der Seite *Ticketdetails* unter *Zusammengeführte Tickets* auf **Tickets zum Zusammenführen hinzufügen/Zusammengeführte Tickets bearbeiten** und wählen Sie ein Ticket aus der angezeigten Liste aus.
   b. Fügen Sie bei Bedarf weitere zusammengeführte Tickets hinzu.
3. Überprüfen Sie, ob der Vorgang der Zusammenführung von Tickets im Ticketverlauf angezeigt wird.
   a. Öffnen Sie auf der Seite *Ticketdetails* die Registerkarte *Verlauf* und aktivieren Sie das Kontrollkästchen **Verlauf des zusammengeführten Tickets anzeigen**.
   b. Prüfen Sie auf der Registerkarte *Verlauf* ggf. die Einträge zu den zusammengeführten Tickets.

Verwenden des Prozesses zur Eskalation von Tickets

Der Eskalationsprozess für Service-Desk-Tickets soll Service Desk-Mitarbeiter und ihre Vorgesetzten darauf aufmerksam machen, dass ein Ticket während eines bestimmten Zeitraums nicht bearbeitet wurde.

Wenn ein Ticket gewisse Kriterien erfüllt, wird eine von Ihnen festgelegte Gruppe per E-Mail darüber benachrichtigt, dass die Bearbeitung eines Tickets aussteht. So haben Sie die Möglichkeit, die Service Level-Vereinbarungen zu überwachen und automatisch die entsprechenden Mitarbeiter zu benachrichtigen, wenn ein Ticket nicht korrekt bearbeitet wurde.

Eskalations-E-Mails werden am Ende der Eskalationsfrist für Tickets gesendet, die folgende Kriterien erfüllen:

- Der Status lautet **Geöffnet**.
- Eine Priorität, die eine Eskalationszeit beinhaltet.

Im folgenden Beispiel sehen Sie die Standardstatusangaben und die Prioritäten für Tickets sowie die Eskalationseinstellungen. Mit diesen Einstellungen wird der Service Desk angewiesen, für Tickets mit dem Status **Geöffnet** und der Priorität **Hoch** nach 30 Minuten Inaktivität eine Eskalations-E-Mail zu senden.

Sie können Folgendes tun:

- Eskalations-E-Mails für Tickets mit anderen Prioritäten konfigurieren
- Die Eskalationsfrist ändern
- Festlegen, wer eine Eskalations-E-Mail erhält
- Die E-Mail-Vorlagen entsprechend Ihren Anforderungen ändern.

HINWEIS: Ticketeskalation und Service Level-Vereinbarungen sind zwei separate Benachrichtigungsaktivitäten. Benachrichtigungen für die Ticketeskalation basieren darauf, wie lange ein Ticket geöffnet war, während Benachrichtigungen für Service Level-Vereinbarungen auf dem Fälligkeitsdatum eines Tickets basieren. Geschäftszeiten und Feiertage werden bei der Ticketeskalation nicht berücksichtigt.

Informationen zu Ticketstatusangaben

Der Service Desk-Ticketzustand gibt den aktuellen Status des Tickets an. Die verfügbaren Zustände sind **Geöffnet**, **Angehalten** und **Abgeschlossen**.

Tickets können nur eskaliert werden, wenn sie den Status **Geöffnet** aufweisen. Diese Anforderung kann nicht konfiguriert werden.

HINWEIS: Wenn die Standardeinstellungen verwendet werden, müssen Tickets die Priorität **Hoch** und den Status **Geöffnet** aufweisen, damit sie eskaliert werden können.

Informationen zur Eskalationsfrist

Sobald einem Service Desk-Ticket der Status **Geöffnet** zugewiesen wird, startet ein Countdown-Timer für die Eskalationszeit.

Der Timer wird mit jeder Änderung am Ticket zurückgesetzt. Wenn der Timer abläuft, wird eine Eskalations-E-Mail gesendet und der Timer startet erneut. Wenn das Ticket nicht geändert wird, wird der Timer zurückgesetzt. Eine Eskalations-E-Mail wird immer dann gesendet, wenn die Eskalationsfrist erreicht ist. Standardmäßig wird die Eskalations-E-Mail alle 30 Minuten bis zur Änderung des Tickets gesendet.

Informationen zur Eskalation

Wenn Service-Desk-Tickets eskaliert werden, werden E-Mails an die in den Warteschlangeneinstellungen festgelegten Empfänger gesendet.

Sie können die Eskalations-E-Mail an folgende Personen senden:

- Ticketbesitzer
- Ticketabsender
- Benutzer mit den technischen Fähigkeiten, um das Problem zu beheben
- Benutzer mit der Befugnis, weitere Ressourcen für das Problem abzustellen

Der Abschnitt *E-Mail bei Ereignissen* der Seite *Warteschlangen-Detail* und die Liste **Kategorie CC** auf dem jeweiligen Ticket bestimmen, an wen Eskalations-E-Mails gesendet werden.

Einstellungen für die Eskalation von Tickets ändern

Die Einstellungen für die Eskalation von Service-Desk-Tickets bestimmen, welche Aktionen bei einer Änderung der Ticketpriorität oder des Ticketstatus ausgeführt werden.

Eskalations-E-Mails werden für Tickets gesendet, die die Priorität **Hoch** aufweisen und deren Status sich von **Neu** in **Geöffnet** geändert hat. Falls ein Ticketbesitzer nicht innerhalb von 30 Minuten auf ein Ticket reagiert, können Sie die Eskalationseinstellungen ändern, damit das Ticket eskaliert werden kann.

Liste der Empfänger von Eskalations-E-Mails ändern

Sie können die E-Mail-Empfänger für die Eskalation von Service-Desk-Tickets nach Bedarf ändern.

Wenn Sie die Standardeinstellungen verwenden, ändern Sie den Ticketstatus von **Neu** in **Geöffnet**. Wurden die Standardeinstellungen geändert, stellen Sie sicher, dass mindestens eine der Statusangaben **Geöffnet** lautet. Weisen Sie dann dem Ticket diesen Status zu. Siehe Konfigurieren der Ticketeinstellungen.

(Optional) Legen Sie den Status **Geöffnet** als Standard für Tickets fest oder geben Sie mithilfe einer Richtlinie vor, dass Ticketbesitzer den Ticketstatus ändern müssen, sobald sie sich des gemeldeten Problems annehmen.

1. Rufen Sie die Seite *Warteschlangen-Detail* des Service Desks auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Service Desk** und anschließend auf **Konfiguration**.
   c. Klicken Sie im Fensterbereich **Konfiguration** auf **Warteschlangen**.
   d. Klicken Sie auf den Namen einer Warteschlange.
2. Aktivieren Sie im Abschnitt *E-Mail bei Ereignissen* die entsprechenden Kontrollkästchen, um Besitzer, Absender, Genehmiger, Ticket CC-Mitglieder und Kategorie CC-Mitglieder als Empfänger von Eskalations-E-Mails hinzuzufügen.
3. Klicken Sie auf **Speichern**.

Eskalationsfrist ändern

Sie können die Zeitlimits für die Eskalation von Tickets nach Bedarf ändern.

1. Rufen Sie die Seite *Warteschlangen-Detail* des Service Desks auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Service Desk** und anschließend auf **Konfiguration**.
   c. Klicken Sie im Fensterbereich **Konfiguration** auf **Warteschlangen**.
   d. Klicken Sie auf den Namen einer Warteschlange.
2. Klicken Sie im Abschnitt *Standardwerte für Tickets* auf **Diese Werte anpassen**, um die Seite *Anpassung von Warteschlange* anzuzeigen.
3. Klicken Sie im Abschnitt *Prioritätswerte* in einer Zeile auf die Schaltfläche **Bearbeiten**, um die Eskalationsfrist zu ändern: .
4. Klicken Sie in der Zeile auf **Speichern** und anschließend unten auf der Seite auf **Speichern**.

Standardmäßige Eskalations-E-Mail-Nachricht ändern

Sie können den Text der E-Mail-Nachricht ändern, die gesendet wird, wenn Service-Desk-Tickets eskaliert werden.

1. Rufen Sie die Seite *Warteschlangen-Detail* des Service Desks auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Service Desk** und anschließend auf **Konfiguration**.

c. Klicken Sie im Fensterbereich **Konfiguration** auf **Warteschlangen**.
d. Klicken Sie auf den Namen einer Warteschlange.

2. Klicken Sie im Abschnitt *E-Mail bei Ereignissen* auf **E-Mails anpassen**, um die Seite *Service Desk E-Mail-Benachrichtigungen* anzuzeigen.
3. Bearbeiten Sie die Nachricht *Ticket eskaliert* entsprechend Ihren Anforderungen.
4. Klicken Sie auf **Speichern**.

Weitere Informationen zur Nachricht *Eskalation von Tickets* finden Sie unter E-Mail-Auslöser und E-Mail-Vorlagen konfigurieren.

Verwenden von Service Desk-Prozessen

Ein Service Desk-Prozess ist eine Sammlung von Tickets, die in einer vordefinierten Reihenfolge angezeigt werden, mit der Sie Aufgaben verfolgen können, die mehrere Schritte oder Aktivitäten erfordern.

Gehen Sie hierbei beispielsweise von den Aufgaben aus, die erforderlich sind, um Systeme und Geräte für neue Mitarbeiter vorzubereiten:

- Erkennen von Büroflächen- und Mobiliaranforderungen
- Einrichten des Telefonservices
- Erhalten von Geräten und Software
- Einrichten der Netzwerk-Anmeldeinformationen
- Ausfüllen der erforderlichen Formulare zur Einstellung

Sie können eine Prozessvorlage erstellen, die all diese erforderlichen Aufgaben als untergeordnete Aktivitäten enthält. Wenn Sie daraufhin Tickets basierend auf dieser Prozessvorlage erstellen, werden für jede Phase des Prozesses automatisch die untergeordneten Tickets für alle erforderlichen Aufgaben erstellt.

Informationen zur Einrichtung einer Service Desk-Prozessvorlage finden Sie unter Hinzufügen, Bearbeiten und Aktivieren von Prozessvorlagen.

Hinzufügen, Bearbeiten und Aktivieren von Prozessvorlagen

Sie können Prozessvorlagen zum Service Desk hinzufügen. Eine Prozessvorlage muss mindestens ein übergeordnetes Ticket enthalten, damit Sie für den Endbenutzer verfügbar gemacht werden kann und der Endbenutzer Ticket basierend auf dieser Prozessvorlage erstellen kann.

1. Gehen Sie zum Service-Desk-Assistent *Prozessvorlage erstellen*:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Service Desk** und anschließend auf **Konfiguration**.
   c. Klicken Sie im Fensterbereich **Konfiguration** auf **Prozessvorlagen**.
   d. Um eine neue Prozessvorlage zu erstellen, wählen Sie auf der Seite *Prozessvorlagen* die Option **Aktion auswählen** > **Neu**.
   e. Zum Bearbeiten oder Kopieren einer bestehenden Prozessvorlage klicken Sie auf der Seite *Prozessvorlagen* auf den Namen einer Prozessvorlage.

Der Assistent *Prozessvorlage erstellen* wird angezeigt, die Seite *Prozessvorlage definieren* ist offen.

2. Zum Kopieren einer bestehenden Prozessvorlage klicken Sie auf der Seite *Prozessvorlagen definieren* auf **Duplizieren**.

   Eine Kopie der duplizierten Prozessvorlage wird angezeigt. Obgleich die duplizierte Prozessvorlage deaktiviert ist, sind alle anderen Optionen die gleichen wie bei der Originalvorlage. Wenn Sie die Aktualisierung der duplizierten Version abgeschlossen haben, können Sie die Option **Aktiviert** auf der Seite *Optionen veröffentlichen* auswählen.

3. Auf der Seite *Prozessvorlage definieren* geben Sie die folgenden Informationen an:

Option	Beschreibung
Name	Ein Name, der den Prozess bezeichnet, beispielsweise Neueinstellung, Kündigung oder Büroumzug.
Beschreibung	Eine Prozessbeschreibung. Bei längeren Beschreibungen wird das Feld automatisch erweitert, während Sie tippen

HTML/Markdown	Eine Angabe, ob die Beschreibung Rich Text enthält. Einige Prozessbeschreibungen sind länger als andere, daher kann das Formatieren bestimmter Textelemente die Gesamtlesbarkeit verbessern und dem Endbenutzer helfen, den Prozess besser zu verstehen. Verwenden Sie die Formatierungssyntax des Projekts „Markdown“, um den Inhalt des Feldes *Beschreibung* zu formatieren. Beispiel:
	`<h1> Bevor Sie fortfahren:</h1>`
	`<h1><ol>`
	`<li>Stellen Sie sicher, dass HR den Vorgang der Mitarbe`
	`<li>Stellen Sie sicher, dass die Badge-ID für den neuen`
	`<b>Wenn Sie nicht über eine Badge-ID verfügen, wenden S`
	`</ol></h1>`
	Weitere Informationen zur Markdown-Syntax finden Sie unter http://daringfireball.net/projects/markdown/syntax.

Prozesstyp	Der Prozesstyp. In einer Standardinstallation sind nur die Prozesstypen *Serviceanfrage* und *Softwareanforderung: Genehmigung erforderlich* enthalten. Sie können falls erforderlich neue Prozesstypen erstellen. Sie können beispielsweise einen Prozesstyp für den Zugriff auf eine bestimmte Anwendung oder eine Gruppe von Anwendungen erstellen. Weitere Informationen hierzu finden Sie unter Prozesstypen definieren.
Untergeordnete Tickets übernehmen bei der Erstellung Felder aus übergeordneten Tickets	Wählen Sie diese Option aus, wenn untergeordnete Tickets Feldwerte von ihren übergeordneten Tickets übernehmen sollen, die zu derselben Warteschlange gehören. Nur die Werte, die in übergeordneten Tickets vorhanden sind, wenn untergeordnete Tickets erstellt werden, können übernommen werden. Alle nachfolgenden Änderungen an den zugehörigen übergeordneten Ticketfeldwerten werden nicht an die untergeordneten Tickets weitergegeben, für die diese Option ausgewählt

Option	Beschreibung
	ist. Übernommene Feldwerte werden pro Ticket während der Konfiguration angegeben.

Klicken Sie auf **Speichern und Fortfahren**.

4. Ordnen Sie auf der Seite *Übergeordnetes Ticket* im Assistent *Prozessvorlage erstellen* ein übergeordnetes Ticket dieser Prozessvorlage zu.
   a. **Softwareanforderung: Nur genehmigungspflichtige Prozesstypen**. Dieser Prozesstyp ist für die Erstellung von speziellen Prozessvorlagen vorgesehen, die zum Einrichten von Benutzerdownloads verwendet werden können, die eine oder mehrere Genehmigungen erfordern. Wenn diese Option ausgewählt ist, wird standardmäßig ein übergeordnetes Ticket aus diesem Prozesstyp erstellt.
   - Um den Inhalt des Tickets anzuzeigen oder zu bearbeiten, klicken Sie auf **Softwareanforderung: Genehmigung erforderlich**.
   - Tickets dieses Typs erlauben es Ihnen nicht, die Felder *Titel*, *Zusammenfassung*, *Gerät* oder *Absender* zu bearbeiten. Diese Felder werden mit den Werten aus der Anforderung ausgefüllt, die den Prozess initiiert hat.
   - Genehmigungen für diesen Prozesstyp sind obligatorisch.

   b. Wählen Sie eine Warteschlange mit dem übergeordneten Ticket, das Sie mit dieser Prozessvorlage verknüpfen möchten, und klicken Sie auf **Übergeordnetes Ticket hinzufügen**.
   c. Auf der Seite *Neues übergeordnetes Ticket* erstellen Sie ein neues übergeordnetes Ticket für diese Prozessvorlage:
   - Falls Sie mehrere Warteschlangen haben, wählen Sie eine Warteschlange aus. Über- und untergeordnete Tickets können sich jeweils in unterschiedlichen Warteschlangen befinden. Wenn Sie nicht über mehrere Warteschlangen verfügen, wird Ihnen keine Auswahl angezeigt.
   - Wenn Sie eine Warteschlange auswählen, der eine oder mehrere Ticketvorlagen zugeordnet sind, wählen Sie die Ticketvorlage aus.
   - Die meisten Felder ähneln denen auf der Seite *Details zum Ticket*. Siehe Erstellen von Tickets auf der Ticketseite der Administratorkonsole. Sie müssen für das übergeordnete Ticket nicht dieselbe Kategorie, denselben Besitzer usw. wie für die untergeordneten Tickets verwenden.
   - Das *Offset-Fälligkeitsdatum* ist der Zeitraum, der für den Abschluss der Arbeit an einem untergeordneten Ticket erforderlich ist. Dieser Zeitraum dient zur Berechnung des Ticketfälligkeitsdatums. Wenn Sie z. B. das *Offset-Fälligkeitsdatum* auf vier Tage einstellen, wird das Fälligkeitsdatum für das untergeordnete Ticket um vier Tage nach dem Ticketerstellungsdatum versetzt. Fälligkeitsdaten werden nicht erzwungen, wenn aber das Fälligkeitsdatum überschritten ist, werden die Tickets auf der Liste *Ticket* als „Überfällig“ markiert und in Berichten als „Überfällig“ aufgeführt.

   Weitere Informationen zur Erstellung von Tickets finden Sie unter Erstellen von Tickets auf der Ticketseite der Administratorkonsole.

   d. Klicken Sie auf **Speichern**, um zurück zum Assistenten *Prozessvorlage erstellen*.
5. **Optional**. Nach dem Hinzufügen eines übergeordneten Tickets zu einem Prozess, können Sie untergeordnete Tickets oder Aktivitäten für diesen Prozess konfigurieren. Untergeordnete Tickets können aus verschiedenen Warteschlangen stammen und unterschiedlichen Stufen zugewiesen sein.
   a. Wählen Sie auf der Seite *Übergeordnetes Ticket*, die im Assistenten *Prozessvorlage erstellen* angezeigt wird, unter *Untergeordnete Tickets* eine dem untergeordneten Ticket zugeordnete Warteschlange aus.
   b. Wenn der ausgewählten Warteschlange eine oder mehrere Ticketvorlagen zugeordnet sind, wählen Sie eine Ticketvorlage aus.

   Wenn die Warteschlange eine oder mehrere Vorlagen enthält und Sie nicht angeben, welche Vorlage Sie verwenden möchten, wird die Standardwarteschlangenvorlage ausgewählt.

c. Klicken Sie auf **Untergeordnetes Ticket hinzufügen**.

Wenn ein Ticket auf Grundlage dieser Prozessvorlage erstellt wurde, werden untergeordnete Tickets der Stufe 1 automatisch erstellt (sofern eventuelle Genehmigungen und Anforderungen erfüllt sind). Wenn das letzte untergeordnetes Ticket in Stufe 1 geschlossen ist, werden die im nächsten Schritt definierten untergeordneten Tickets erstellt.

d. Erstellen Sie auf der Seite *Untergeordnetes Ticket* ein neues untergeordnetes Ticket für diese Prozessvorlage:

- **Stufe**: Die Stufe des Prozesses, auf der das Ticket erstellt wird, z. B. 1, 2, 3 usw. Bei Bedarf können Sie mehrere Tickets der gleichen Stufe zuweisen. Wenn z. B. die erste Stufe die Bestellung von Ausstattungen und Verbrauchsmaterialien für eine Neueinstellung ist, könnten mehrere separate untergeordnete Tickets für die Bestellung von Geräten, Büroausstattungen und Verbrauchsmaterialien sinnvoll sein, die alle Stufe 1 zugewiesen sind.

Bei der Erstellung eines Prozesstickets werden alle der Stufe 1 zugewiesenen Prozesstickets automatisch erstellt. Tickets der Stufe 2 werden erstellt, wenn alle Tickets der Stufe 1 abgeschlossen sind. Tickets der Stufe 3 werden erstellt, wenn alle Tickets der Stufe 2 abgeschlossen sind usw.

- **Titel**: Ein Titel für das untergeordnete Ticket.
- **Zusammenfassung**: Eine Beschreibung der Aufgabe im Zusammenhang mit diesem untergeordneten Ticket.
- **Kategorie**, **Eigentümer** und **Fälligkeitsdaten**: Diese Werte müssen nicht mit denen übergeordneten Tickets übereinstimmen.

Wenn Sie auf der Seite *Prozessvorlagen definieren* die Option **Untergeordnete Tickets übernehmen bei der Erstellung Felder aus übergeordneten Tickets** ausgewählt haben, wird für jedes Feld das Kontrollkästchen **Übernommen** angezeigt. Dies ermöglicht es Ihnen, den aktuellen Wert dieses Felds aus dem übergeordneten Ticket zu übernehmen. Weitere Informationen hierzu finden Sie in Schritt 3.

Weitere Informationen zur Erstellung von Tickets finden Sie unter Erstellen von Tickets auf der Ticketseite der Administratorkonsole.

e. Klicken Sie auf **Speichern**, um zurück zum Assistenten *Prozessvorlage erstellen*.

6. Wenn Tickets, die mit dieser Prozessvorlage erstellt werden, Genehmigungen erfordern sollen, wählen Sie auf der angezeigten Seite *Genehmigungen* **Eine oder mehrere Genehmigungen erforderlich, damit Vorgang startet**, und geben die in der Tabelle unten aufgeführten Informationen an.

Wenn Sie den Prozesstyp *Softwareanforderung: Genehmigung erforderlich* ausgewählt haben, ist dieses Kontrollkästchen standardmäßig aktiviert und kann nicht deaktiviert werden. Genehmigungen für diesen Prozesstyp sind obligatorisch.

Wenn ein Prozessticket für einen Prozess, der Genehmigung erfordert, erstellt wird, werden untergeordnete Tickets erst erstellt, wenn alle Genehmigungen empfangen wurden. Gibt es mehrere Genehmigungsstufen, werden E-Mails, die die Genehmigungen anfordern, zunächst an Schritt 1 Genehmiger gesendet. Schritt 2 Genehmiger erhalten ihre E-Mails erst, wenn alle Schritt 1 Genehmigungsanforderungen erfüllt sind.

Genehmiger können ein Prozessticket per E-Mail mit e-Mail-Token genehmigen oder ablehnen. Verwenden Sie nach Bedarf die folgenden Syntaxbeispiele:

- Tickets per E-Mail genehmigen:

```
@approval = approved
@approval_note = Diese Anforderung wird per E-Mail genehmigt
```

- Tickets per E-Mail ablehnen:

```
@approval = rejected
@approval_note = Diese Anforderung wird per E-Mail abgelehnt
```

Weitere Informationen zu diesen Token finden Sie unter Ticketgenehmigungsfelder per E-Mail ändern.

Option	Beschreibung
Genehmigungsschritt	
Genehmigungsschritt 1	Ein oder mehrere Ticketgenehmiger. Sie können die Liste der Genehmiger nach Bedarf bearbeiten. • **Neue Prozessvorlagen**. Dieses Feld wird leer angezeigt. • **Bestehende Prozessvorlagen**. Wenn ein oder mehrere Genehmiger bereits in der Prozessvorlage definiert sind, werden sie in diesem Feld aufgeführt. **HINWEIS:** Der Manager des Einsenders wird standardmäßig als ausgewählt angezeigt.
Jede erforderliche Genehmigung	Mindestens eine Ticketgenehmigung ist erforderlich.
Alle Genehmigungen sind erforderlich	Alle Ticketgenehmigungen sind erforderlich.
Alle entfernen	Entfernt alle Genehmiger aus der Liste.
Einen weiteren Schritt hinzufügen	Fügt einen Genehmigungsschritt hinzu.
Genehmigungsoptionen	
Zeitlimit für Genehmigungen	Die Zeit, die jeder Ticketgenehmiger hat, um ein Ticket zu genehmigen oder abzulehnen, basiert auf dieser Prozessvorlage. Das Zeitlimit für Genehmigungen erstreckt sich nicht über mehrere Genehmigungsstufen. Gibt es beispielsweise für einen Prozess zwei Genehmigungsschritte und das Zeitlimit für Genehmigungen ist mit acht Stunden definiert: • Schritt 1 Genehmiger haben 8 Stunden für die Genehmigung. • Wenn alle der Schritt 1 Genehmigungen eingegangen sind, erhalten Schritt 2 Genehmiger acht Stunden um ihre Genehmigungsanforderungen auszuführen.
Wiederholung von Benachrichtigungen für Genehmigungen	Gibt an, wie oft das System Benachrichtigungen an jeden Genehmiger sendet, wenn die Genehmigung für ein Ticket aussteht. Ist diese Option auf Null '0' gesetzt, werden einmalige Benachrichtigungen ohne Wiederholungen gesendet.

Option	Beschreibung
Verwenden Sie Arbeits- und Feiertage für das Zeitlimit für Genehmigungen und die Benachrichtigungsfrequenz	Gibt an, ob arbeitsfreie Tage bei der Berechnung der Genehmigungsfrist berücksichtigt werden.
Erforderliche Genehmigungen außer Kraft setzen	Eine Genehmigung außer Kraft zu setzen, bringt das Prozessticket voran zum nächsten Schritt, ohne ausstehende Gernehmigungen abzuwarten. Nachdem eine Genehmigung außer Kraft gesetzt worden ist, werden alle ausstehenden Genehmigungen als gegeben betrachtet, der Ticketverlauf wird geschrieben und die Genehmiger erhalten die E-Mail „Zustimmung empfangen“, wie sie in den E-Mail-Benachrichtigungen definiert ist.
Kein(e)	Außer Kraft setzen der Genehmigung nicht zulässig.
Allen Admins außer Kraft setzen von Genehmigungen erlauben	Alle Benutzer mit Administratorrechten dürfen Genehmigungen außer Kraft setzen.
Label angeben	Benutzer, die der Gruppe mit diesem Label angehören, können Genehmigungen außer Kraft setzen.

Klicken Sie auf **Speichern und Fortfahren**.

7. Wählen Sie auf der angezeigten Seite *E-Mail-Benachrichtigungen* die Empfänger der E-Mail-Benachrichtigungen für jede Stufe des Lebenszyklus des Tickets. Klicken Sie auf den angegebenen Link, um diese Optionen auf der Seite *Service Desk Queue Email Settings (Service Desk-Warteschlange – E-Mail-Einstellungen)* zu konfigurieren. Weitere Informationen hierzu finden Sie unter Warteschlangen-spezifische E-Mail-Einstellungen konfigurieren.

   Klicken Sie auf **Speichern und Fortfahren**.

8. Geben Sie auf der daraufhin angezeigten Seite *Recurring Ticket Schedule (Zeitplan für wiederkehrende Tickets)* die Häufigkeit an, mit der ein Ticket erstellt wird. Dies ist nützlich, wenn Sie bei diesem Prozess in regelmäßigen Abständen Tickets erstellen möchten, z. B. zur Überprüfung des Systemzustands oder zum regelmäßigen Löschen von Dateiprotokollen.

Option	Beschreibung
Kein(e)	Die Ausführung erfolgt im Zusammenhang mit einem Ereignis anstatt zu einem bestimmten Datum oder zu einem bestimmten Zeitpunkt.
jede Stunde	Der Vorgang wird im angegebenen Intervall durchgeführt.
Täglich/an einem bestimmten Tag um HH:MM	Die Erfassung wird täglich zu einem bestimmten Zeitpunkt oder an einem bestimmten Wochentag um eine bestimmte Uhrzeit ausgeführt.
Ausführen am n-ten jedes Monats/eines bestimmten Monats um HH:MM	Die Erfassung wird jeden Monat oder in einem bestimmten Monat an einem festgelegten Datum zu einer festgelegten Uhrzeit ausgeführt.

Option	Beschreibung
Ausführen am n-ten Wochentag **jedes Monats/ eines bestimmten Monats um HH:MM**	Die Erfassung wird jeden Monat oder in einem bestimmten Monat an einem festgelegten Wochentag zu einer festgelegten Uhrzeit ausgeführt.

Benutzerdefiniert	Führen Sie die Erfassung nach einem benutzerdefinierten Zeitplan aus.
	Verwenden Sie das Standard-5-Feld-Cron-Format (das erweiterte Cron-Format wird nicht unterstützt):
	`* * * * *`
	`| | | | +————Wochentag (0-6) (Sonntag=0)`
	`| | | +————Monat (1-12)`
	`| | +————Monatstag (1-31)`
	`| +————Stunde (0-23)`
	`+————Minute (0-59)`
	Verwenden Sie bei der Angabe von Werten die folgenden Zeichen:
	• **Leerzeichen( )**: Die einzelnen Felder mit einem Leerzeichen trennen.
	• **Sternchen (*)**: Ein Sternchen repräsentiert den gesamten Wertebereich in einem Feld. Zum Beispiel repräsentiert ein Sternchen im Stundenfeld eine beliebige Stunde.
	• **Kommas (,)**: Mehrere Werte in einem Feld werden mit einem Komma getrennt. Zum Beispiel werden mit `0,6` im Feld „Wochentag“ Sonntag und Samstag angegeben.
	• **Bindestriche (-)**: Mit einem Bindestrich wird ein Wertebereich in einem Feld angegeben. Zum Beispiel entspricht `1-5` im Feld „Wochentag“ `1,2,3,4,5`, d. h. Montag bis Freitag.
	• **Schrägstriche (/)**: Die Angabe der Zeitabstände, mit denen eine Aktion wiederholt werden soll, erfolgt mit einem Schrägstrich. Zum Beispiel entspricht `*/3` im Feld Stunde `0,3,6,9,12,15,18,21`. Das Sternchen (`*`) gibt jede Stunde an, mit `/3` erfolgt aber eine Einschränkung auf durch drei teilbare Stunden.

Option	Beschreibung
	Beispiele: • `15 * * * * Jeden Tag 15 Minuten nach jeder vollen Stunde ausführen` • `0 22 * * * Jeden Tag um 22:00 Uhr ausführen` • `0 0 1 1,6 * Am 1. Januar und 1. Juni um 00:00 Uhr ausführen` • `30 8,12 * * 1-5 An Wochentagen um 08:30 Uhr und 12:30 Uhr ausführen` • `0 2 */2 * * Jeden zweiten Tag um 02:00 Uhr ausführen`
Aufgabenplan anzeigen	Klicken Sie, um den Aufgabenplan anzuzeigen. Im Dialogfeld *Aufgabenplan* wird eine Liste der geplanten Aufgaben angezeigt. Klicken Sie auf eine Aufgabe, um die Aufgabendetails anzuzeigen. Weitere Informationen hierzu finden Sie unter Aufgabenpläne anzeigen.

9. Auf der angezeigten Seite *Veröffentlichungsoptionen* wählen Sie nach Bedarf Veröffentlichungsoptionen:

Option	Beschreibung
Aktiviert	Prozesse müssen aktiviert sein, bevor Sie sie zum Erstellen von Prozesstickets verwenden können. Markieren Sie dieses Kontrollkästchen, wenn Sie Benutzern ermöglichen möchten, Tickets aus dieser Prozessvorlage zu erstellen.
Genehmigungsinformationen vor Nicht-Besitzern verbergen	Wählen Sie diese Option, wenn Sie nicht möchten, dass die Benutzer, die keine Eigentümer sind, Ticket-Genehmigungsinformationen sehen.
Prozessschritte vor Absendern verbergen	Wählen Sie diese Option aus, wenn Sie Prozessschritte (untergeordnete Tickets) nicht für Absender auf der Seite „Übergeordnete Ticketdetails“ anzeigen möchten.
Prozess für alle Benutzer anzeigen	Diese Option ist standardmäßig ausgewählt. Wenn Sie die den Endbenutzerzugriff auf diesen Prozess beschränken möchten, deaktivieren Sie diese Option. Wählen Sie alternativ ein Label, das mit der Gruppe verbunden ist, zu der Sie Zugang gewähren möchten.
Prozessbeschreibungsseite beim Erstellen neuer Prozessanfragen anzeigen	Wählen Sie diese Option, wenn Sie die Seite Prozessbeschreibung bei der Erstellung neuer Tickets basierend auf dieser Prozessvorlage anzeigen möchten.
Prozessstatus-Workflow anstelle des Ticketstatus verwenden	Wenn Sie die Genehmigungs- und Benachrichtigungsfunktionen in der Prozessvorlage nutzen möchten, müssen Sie diese Option

Option	Beschreibung
	auswählen. Wenn Sie bereits Genehmigungen oder Benachrichtigungen konfiguriert haben, ist diese Option standardmäßig ausgewählt und kann nicht gelöscht werden. Wird die Verwendung des Prozessstatus-Workflows gewählt, durchläuft das übergeordnete Ticket automatisch verschiedene prozessspezifische Zustände, wie „Ausstehende Genehmigung“, „Genehmigung abgelehnt“, „Zeitlimit für Genehmigung überschritten“, „In Bearbeitung“ oder „Prozess abgeschlossen“. Wenn Sie sich entscheiden, diese Option nicht zu wählen und weiterhin Ticketstatus-Workflows verwenden, müssen Sie benutzerdefinierte Ticketregeln erstellen, um die gewünschte Genehmigungs- und Benachrichtigungsfunktionalität zu erzielen. Wenn Sie Prozessstatus-Workflows verwenden, wird das Feld *Status* nicht auf der Seite *Ticketdetail* angezeigt, auch wenn das Feld für die zugehörige Warteschlange konfiguriert wurde. Das Feld *Status* wird für untergeordnete Tickets weiter angezeigt.
Status 'Geschlossen' des übergeordneten Tickets	Wählen Sie, welchen Status Sie verwenden möchten, wenn das zu diesem Prozess gehörige übergeordnete Ticket geschlossen ist. Wenn die letzte untergeordnete Aktivität geschlossen ist, wird das übergeordnete Ticket automatisch geschlossen, und der Status in diesem Feld angezeigt.

Klicken Sie auf **Fertig stellen**.

Der Assistent *Prozessvorlage erstellen* wird geschlossen und die neu erstellte oder aktualisierte Prozessvorlage wird auf der Seite *Prozessvorlagen* angezeigt.

Prozesstypen definieren

In einer Standardinstallation sind nur die Prozesstypen *Serviceanfrage* und *Softwareanforderung: Genehmigung erforderlich* enthalten. Sie können falls erforderlich neue Prozesstypen erstellen. Sie können beispielsweise einen Prozesstyp für den Zugriff auf eine bestimmte Anwendung oder eine Gruppe von Anwendungen erstellen.

Die *Softwareanforderung:* Der Prozesstyp *Genehmigungspflichtig* ist für die Erstellung von speziellen Prozessvorlagen vorgesehen, die zum Einrichten von Benutzerdownloads verwendet werden können, die eine oder mehrere Genehmigungen erfordern.

Erstellen Sie ein übergeordnetes Ticket.

1. Rufen Sie die Seite *Prozessdetail* des Service Desks auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Service Desk** und anschließend auf **Konfiguration**.

c. Klicken Sie im Fensterbereich **Konfiguration** unter **Prozessvorlagen** auf **Prozesstypen definieren**.

2. Um einen neuen Prozesstyp hinzufügen, klicken Sie in der Ecke oben rechts auf +. Geben Sie in dem angezeigten Textfeld den Prozesstypname ein und klicken Sie auf **Speichern**.
3. Um den Namen eines vorhandenen Prozesses zu ändern, klicken Sie in der Zeile, die den Prozesstyp enthält, den Sie bearbeiten möchten, auf . Geben Sie in dem angezeigten Textfeld den neuen Prozesstypname ein und klicken Sie auf **Speichern**.

Prozesstickets zur Verwaltung zugehöriger Aufgaben erstellen

Wenn Sie Prozessvorlagen zu einer Warteschlange hinzugefügt und aktiviert haben, können Sie Prozesstickets erstellen, um zugehörige Aufgaben als Gruppe zu verwalten (wie z. B. Aufgaben im Zusammenhang mit der Einrichtung von Systemen für neue Mitarbeiter).

Sie haben Prozessvorlagen hinzugefügt und aktiviert. Siehe Hinzufügen, Bearbeiten und Aktivieren von Prozessvorlagen.

1. Rufen Sie die Seite *Neues Ticket* des Service Desks auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Service Desk** und anschließend auf **Tickets**.
   c. Klicken Sie auf **Aktion auswählen** > **Neues Ticket aus Prozess** > **Prozessname**.

   Die Seite *Neues Ticket* wird angezeigt. Die Aktivitäten jeder Prozessphase sind im Abschnitt *Prozessinformation* aufgelistet.
2. Geben Sie die erforderlichen Ticketinformationen an. Siehe Erstellen von Tickets auf der Ticketseite der Administratorkonsole.
3. Führen Sie einen der folgenden Schritte aus:
   - Klicken Sie auf **Speichern**, um das Ticket zu speichern und zur Liste *Ticket* zurückzukehren.
   - Klicken Sie auf **Änderungen übernehmen**, um das Ticket zu speichern und mit der Bearbeitung fortzufahren.
   - Klicken Sie auf **Abbrechen**, um die Änderungen am Ticket zu verwerfen.

   Wenn andere Benutzer das Ticket gleichzeitig geändert haben, wird das Dialogfeld *Aktualisierungsbenachrichtigung* angezeigt, wenn das Dialogfeld für die Warteschlange aktiviert ist und Sie der Ticketbesitzer oder ein Administrator sind. Dieses Dialogfeld wird nur Administratoren und Ticketbesitzern angezeigt. Anderen Benutzern wird es nicht angezeigt. Administratoren können die Konfliktwarnungsmeldung für jede Warteschlange separat aktivieren/deaktivieren. Siehe Aktivieren oder Deaktivieren der Konfliktwarnung.

Siehe Erstellen von Tickets auf der Ticketseite der Administratorkonsole. Das Prozessticket wird erstellt. Für Stufe 1 zugewiesene Aktivitäten werden die untergeordneten Tickets automatisch erstellt. Untergeordnete Tickets der Stufe 2 werden erstellt, wenn alle Tickets der Stufe 1 abgeschlossen sind usw. Wenn Genehmigungen für den Prozess festgelegt wurden, werden untergeordnete Tickets erstellt, nachdem die Genehmigungen für das Prozessticket eingegangen sind.

Prozesstickets per E-Mail erstellen

Sie können ein Prozessticket für vorhandene Prozessvorlagen schnell per E-Mail erstellen.

Bevor Sie ein Prozessticket per E-Mail erstellen, benötigen Sie die folgenden Informationen:

- Prozessname
- E-Mail-Adresse der Ticket-Warteschlange, die mit dem übergeordneten Ticket der Prozessvorlage verknüpft ist

1. Melden Sie sich bei Ihrem E-Mail-Konto an und erstellen Sie eine neue E-Mail-Nachricht.
2. Geben Sie in der Zeile für den E-Mail-Empfänger die E-Mail-Adresse der Ticket-Warteschlange ein, die mit dem übergeordneten Ticket der Prozessvorlage verknüpft ist.
3. Geben Sie in der Betreffzeile der E-Mail den Namen der Prozessvorlage in geschweiften Klammern an. Jeder Text, den Sie nach diesem Segment hinzufügen, wird dem Tickettitel hinzugefügt. Beispiel: `{New Hire} Jane Smith`.
4. Der E-Mail-Text ist optional. Alle Inhalte, die Sie dem E-Mail-Text hinzufügen, werden der Ticketbeschreibung hinzugefügt.
5. Senden Sie die E-Mail.
6. Rufen Sie die Listenseite *Tickets* des Service Desks auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Service Desk** und anschließend auf **Tickets**.
7. Suchen Sie nach dem neu erstellten Ticket und klicken Sie auf den Tickettitel.
8. Nehmen Sie alle zutreffenden Änderungen vor.

   Weitere Informationen zum Bearbeiten der Ticketseite finden Sie unter Erstellen von Tickets auf der Ticketseite der Administratorkonsole.

Prozessinformationen anzeigen

Wenn Sie Prozesstickets erstellt haben, um zugehörige Aufgabensätze zu verwalten, können Sie die zugehörigen Prozessinformationen in diesen Tickets anzeigen.

Sie haben ein Ticket basierend auf einer Prozessvorlage erstellt. Siehe Prozesstickets zur Verwaltung zugehöriger Aufgaben erstellen.

1. Rufen Sie die Seite *Ticket* des Service Desks auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Service Desk** und anschließend auf **Tickets**.
   c. Klicken Sie auf den Titel eines Tickets.

   Die Seite *Ticket* wird angezeigt. Die Aktivitäten jeder Prozessphase sind im Abschnitt *Prozessinformation* aufgelistet. Die in diesem Abschnitt angezeigte Informationsebene hängt von den Einstellungen ab, die auf der Seite *Veröffentlichen* des *Vorgangsvorlage Erstellen* Assistenten konfiguriert wurden. Wenn Sie zum Beispiel die zugehörige Prozessvorlage konfiguriert haben, dass sie Genehmigungs- und

Prozessinformationen anzeigt, werden sie in diesem Abschnitt angezeigt. Weitere Informationen zu diesem Assistenten finden Sie unter Hinzufügen, Bearbeiten und Aktivieren von Prozessvorlagen.

2. Führen Sie einen der folgenden Schritte aus:
   - Klicken Sie auf **Speichern**, um das Ticket zu speichern und zur Liste *Ticket* zurückzukehren.
   - Klicken Sie auf **Änderungen übernehmen**, um das Ticket zu speichern und mit der Bearbeitung fortzufahren.
   - Klicken Sie auf **Abbrechen**, um die Änderungen am Ticket zu verwerfen.

   Wenn andere Benutzer das Ticket gleichzeitig geändert haben, wird das Dialogfeld *Aktualisierungsbenachrichtigung* angezeigt, wenn das Dialogfeld für die Warteschlange aktiviert ist und Sie der Ticketbesitzer oder ein Administrator sind. Dieses Dialogfeld wird nur Administratoren und Ticketbesitzern angezeigt. Anderen Benutzern wird es nicht angezeigt. Administratoren können die Konfliktwarnungsmeldung für jede Warteschlange separat aktivieren/deaktivieren. Siehe Aktivieren oder Deaktivieren der Konfliktwarnung.

Das Prozessticket wird erstellt. Für Stufe 1 zugewiesene Aktivitäten werden die untergeordneten Tickets automatisch erstellt. Untergeordnete Tickets der Stufe 2 werden erstellt, wenn alle Tickets der Stufe 1 abgeschlossen sind usw.

Prozesstickets abbrechen oder abschließen

Wenn Sie Prozesstickets erstellt haben, um zugehörige Aufgabensätze zu verwalten, können Sie die zugehörigen Prozessinformationen in diesen Tickets anzeigen. Ein Prozess kann entweder vom Eigentümer oder Absender als abgebrochen gekennzeichnet werden. Er kann von seinem Besitzer als abgeschlossen gekennzeichnet werden.

Sie haben ein übergeordnetes Ticket basierend auf einer Prozessvorlage erstellt. Siehe Prozesstickets zur Verwaltung zugehöriger Aufgaben erstellen.

1. Rufen Sie die Seite *Ticket* des Service Desks auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Service Desk** und anschließend auf **Tickets**.
   c. Klicken Sie auf den Titel eines übergeordneten Prozesstickets.

   Die Seite *Ticket* wird angezeigt.
2. Führen Sie einen der folgenden Schritte aus:
   - Wählen Sie zum Abbruch von Prozesstickets **Aktion wählen** > **Prozess abbrechen**.
   - Wählen Sie zum Abschluss von Prozesstickets **Aktion wählen** > **Prozess abschließen**.
3. Bestätigen Sie im daraufhin angezeigten Dialogfeld, dass Sie das Prozessticket abbrechen oder abschließen wollen.
4. Führen Sie einen der folgenden Schritte aus:
   - Klicken Sie auf **Speichern**, um das Ticket zu speichern und zur Liste *Ticket* zurückzukehren.
   - Klicken Sie auf **Änderungen übernehmen**, um das Ticket zu speichern und mit der Bearbeitung fortzufahren.
   - Klicken Sie auf **Abbrechen**, um die Änderungen am Ticket zu verwerfen.

   Wenn andere Benutzer das Ticket gleichzeitig geändert haben, wird das Dialogfeld *Aktualisierungsbenachrichtigung* angezeigt, wenn das Dialogfeld für die Warteschlange aktiviert ist und Sie der Ticketbesitzer oder ein Administrator sind. Dieses Dialogfeld wird nur Administratoren und Ticketbesitzern angezeigt. Anderen Benutzern wird es nicht angezeigt. Administratoren können die Konfliktwarnungsmeldung für jede Warteschlange separat aktivieren/deaktivieren. Siehe Aktivieren oder Deaktivieren der Konfliktwarnung.

Prozessvorlagen löschen

Sie können Prozesse mithilfe der Liste Service Desk *Prozesse* löschen. Wenn Tickets für einen bestimmten Prozess vorhanden sind, kann nur der Vorgang als deaktiviert gekennzeichnet werden. Zum Löschen des Prozesses müssen zunächst die unter Verwendung dieses Prozesses erstellten Tickets gelöscht werden.

1. Rufen Sie die Liste *Prozesse* des Service Desks auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Service Desk** und anschließend auf **Konfiguration**.
   c. Klicken Sie im Fensterbereich **Konfiguration** auf **Prozessvorlagen**.
2. Wählen Sie einen oder mehrere Prozessvorlagen, und wählen Sie dann **Aktion auswählen** > **Löschen**.
3. Klicken Sie auf der Bestätigungsseite auf **Ja**, um die ausgewählten Prozessvorlagen zu löschen.

Prozesstickets in reguläre Tickets umwandeln

Sie können Service Desk-Prozesstickets nach Bedarf in reguläre Tickets umwandeln. Diese Umwandlung ist für Tickets nützlich, die versehentlich als Prozesstickets erstellt worden sind, obwohl sie nicht alle Schritte eines Prozesses erfordern.

Weitere Informationen zu Prozesstickets finden Sie unter Verwenden von Service Desk-Prozessen.

1. Rufen Sie die Seite *Details zum Ticket* des Service Desks auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Service Desk** und anschließend auf **Tickets**.
   c. Klicken Sie auf den Titel eines Tickets.
2. Klicken Sie auf **Aktion auswählen** > **Von Prozess Prozessname in reguläres Ticket umwandeln**.

   HINWEIS: Diese Menüoption ist nur verfügbar, wenn das ausgewählte Ticket anhand eines Prozesses erstellt wurde.

   Ein Bestätigungsfenster wird angezeigt.
3. Klicken Sie auf **Ja**, um mit der Umwandlung des Prozesstickets in ein reguläres Ticket fortzufahren.
4. Führen Sie einen der folgenden Schritte aus:
   - Klicken Sie auf **Speichern**, um das Ticket zu speichern und zur Liste *Ticket* zurückzukehren.
   - Klicken Sie auf **Änderungen übernehmen**, um das Ticket zu speichern und mit der Bearbeitung fortzufahren.
   - Klicken Sie auf **Abbrechen**, um die Änderungen am Ticket zu verwerfen.

   Wenn andere Benutzer das Ticket gleichzeitig geändert haben, wird das Dialogfeld *Aktualisierungsbenachrichtigung* angezeigt, wenn das Dialogfeld für die Warteschlange aktiviert ist und Sie der Ticketbesitzer oder ein Administrator sind. Dieses Dialogfeld wird nur Administratoren und Ticketbesitzern angezeigt. Anderen Benutzern wird es nicht angezeigt. Administratoren können die Konfliktwarnungsmeldung für jede Warteschlange separat aktivieren/deaktivieren. Siehe Aktivieren oder Deaktivieren der Konfliktwarnung.

Reguläre Tickets in Prozesstickets umwandeln

Reguläre Service-Desk-Tickets können in Prozesstickets umgewandelt werden. Diese Umwandlung ist für Tickets mit Prozessbezug nützlich, die über E-Mails erstellt werden, da diese immer als einzelne Tickets erstellt werden.

Darüber hinaus kann es sein, dass Benutzer einzelne Tickets erstellen, weil sie Prozesse nicht kennen oder keinen Zugriff auf Prozesse haben. Durch die Umwandlung regulärer Tickets in Prozesstickets können Administratoren und Ticketbesitzer auch dann Prozesse nutzen, wenn Tickets nicht ursprünglich als Prozesstickets gesendet worden sind. Weitere Informationen zu Prozesstickets finden Sie unter Verwenden von Service Desk-Prozessen.

1. Rufen Sie die Seite *Details zum Ticket* des Service Desks auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Service Desk** und anschließend auf **Tickets**.
   c. Klicken Sie auf den Titel eines Tickets.
2. Klicken Sie auf **Aktion auswählen** > **Umwandeln in Prozess** > **Prozessname**.

   Ein Bestätigungsfenster wird angezeigt.
3. Klicken Sie auf **Ja**, um mit der Umwandlung des Tickets in ein Prozessticket fortzufahren.
4. Führen Sie einen der folgenden Schritte aus:
   - Klicken Sie auf **Speichern**, um das Ticket zu speichern und zur Liste *Ticket* zurückzukehren.
   - Klicken Sie auf **Änderungen übernehmen**, um das Ticket zu speichern und mit der Bearbeitung fortzufahren.
   - Klicken Sie auf **Abbrechen**, um die Änderungen am Ticket zu verwerfen.

   Wenn andere Benutzer das Ticket gleichzeitig geändert haben, wird das Dialogfeld *Aktualisierungsbenachrichtigung* angezeigt, wenn das Dialogfeld für die Warteschlange aktiviert ist und Sie der Ticketbesitzer oder ein Administrator sind. Dieses Dialogfeld wird nur Administratoren und Ticketbesitzern angezeigt. Anderen Benutzern wird es nicht angezeigt. Administratoren können die Konfliktwarnungsmeldung für jede Warteschlange separat aktivieren/deaktivieren. Siehe Aktivieren oder Deaktivieren der Konfliktwarnung.

Verwenden von Ticketregeln

Mithilfe von Ticketregeln können Sie Abfragen für Service-Desk-Tickets und Aktionen für die Liste zurückgegebener Tickets durchführen.

Sie können beispielsweise eine Ticketregel verwenden, um den Status eines Tickets automatisch von *Abgeschlossen* in *Erneut geöffnet* zu ändern, wenn eine andere Person als der Besitzer auf das Ticket reagiert. Es gibt vier Standard-Ticketregeln und Sie können je nach Bedarf beliebig viele benutzerdefinierte Ticketregeln hinzufügen.

Systemticketregeln verwenden und konfigurieren

Sie können Systemticketregeln verwenden und konfigurieren, um die speziellen Anforderungen Ihrer Service Desk-Umgebung zu erfüllen.

Zur Auswahl stehen folgende Optionen:

- Standardticketregel aktivieren und Standardeinstellungen verwenden
- Benutzerdefinierte Ticketregeln erstellen
- Benutzerdefinierte Ticketregeln duplizieren
- Benutzerdefinierte Ticketregeln löschen
- Ticketregeln von einer Warteschlange in eine andere verschieben

Informationen zu den Systemticketregeln und Anpassen der Regeln

Systemticketregeln ändern automatisch den Status von Service-Desk-Tickets oder senden unter bestimmten Bedingungen E-Mail-Benachrichtigungen.

Die folgende Tabelle zeigt die Namen, das Verhalten und die Nutzung von Systemticketregeln:

Ticketregel	Standardverhalten	Kann kopiert und für Folgendes verwendet werden
WartenÜberfällig	Weist Tickets, die sieben Tage lang nicht bearbeitet wurden, den Status Überfällig zu.	Ändern eines Ticketstatus nach einer konfigurierbaren Zeitspanne. Sie können auch eine E-Mail-Nachricht über die Statusänderung senden.
ÜberfälligAbschluss	Schließt überfällige Tickets ab, die seit sieben Tagen nicht mehr bearbeitet wurden.	Ändern eines Ticketstatus nach einer konfigurierbaren Zeitspanne. Sie können auch eine E-Mail-Nachricht über die Statusänderung senden.
E-MailBeiAbschluss	Sendet beim Ticketabschluss eine E-Mail-Nachricht an die Ticketabsender. Auf abgeschlossene Tickets muss nur geantwortet werden, wenn das Ticket erneut geöffnet wird.	Senden einer E-Mail-Nachricht, wenn ein Ticket abgeschlossen wird.
KundenantwortVorhanden	Verschieben eines Tickets auf den Status Beantwortet, sobald der Kunde auf ein Ticket antwortet, für das eine Kundenaktion ausgestanden hat.	Ändern des Status eines geöffneten Tickets und Senden einer E-Mail-Nachricht, wenn es aktualisiert wird.
TicketErneutÖffnen	Öffnet ein abgeschlossenes Ticket erneut, wenn jemand anders als der Besitzer darauf antwortet.	Wenn ein abgeschlossenes Ticket erneut geöffnet wird, kann diese Ticketregel den Status des Tickets ändern und eine E-Mail-Nachricht senden.

Benutzerdefinierte Ticketregeln erstellen

Sie können nach Bedarf benutzerdefinierte Ticketregeln für Service-Desk-Tickets erstellen.

1. Rufen Sie die Seite *Warteschlangen-Detail* des Service Desks auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Service Desk** und anschließend auf **Konfiguration**.
   c. Klicken Sie im Fensterbereich **Konfiguration** auf **Warteschlangen**.
   d. Klicken Sie auf den Namen einer Warteschlange.
2. Klicken Sie unten auf der Seite im Abschnitt *Ticketregeln* auf **Anpassen**, um die Seite *Ticketregeln* anzuzeigen.
3. Klicken Sie auf **Aktion auswählen** > **Neu (Assistent)**, um den Fensterbereich *Ticketregel definieren* anzuzeigen.
4. Geben Sie die erforderlichen Kriterien für die Auswahl der Tickets für die benutzerdefinierten Ticketregeln ein. Beispiel:

   ```
   Priorität | = | Mittel
   ```

5. Klicken Sie auf **Testen**, um Tickets anzuzeigen, die den angegebenen Kriterien entsprechen.
6. Klicken Sie auf **Weiter**.
7. Wählen Sie die Werte aus, zu denen Sie wechseln möchten. Beispiel:

   ```
   Priorität | Wert ändern in | Hoch
   ```

8. Klicken Sie auf **Abgeschlossen**, um die Seite *Detail zur Ticketregel* anzuzeigen.
9. Geben Sie die folgenden Informationen an:

   WICHTIG: Bearbeiten Sie SQL-Abfragen nur dann, wenn Sie die Auswirkungen genau kennen. Falsche SQL-Anweisungen könnten die Leistung der Appliance beeinträchtigen.

Option	Beschreibung
Name	Der Name der Ticketregel.
Reihenfolge	Eine Zahl, mit der die Ebene in der Auswertungsreihenfolge angegeben wird. Die Ticketregel wird entsprechend der angegebenen Auswertungsreihenfolge ausgeführt. Kleinere Zahlen werden vor größeren Zahlen ausgeführt.
Warteschlange	(Schreibgeschützt) Der Name der Warteschlange, zu der das Ticket gehört.
Beschreibung	Geben Sie nach Bedarf beliebige weitere Informationen ein.
Aktiviert	Die Ticketregel ist verfügbar. Die Ticketregel wird nur ausgeführt, wenn sie aktiviert ist.
SQL auswählen	Ändert die SQL-Abfrage bei Bedarf. Die Abfrage wird durch den Assistenten für Ticketregeln auf Grundlage der Kriterien generiert, die auf der Seite

Option	Beschreibung
	Ticketregel angegeben werden. Die Abfrage gibt eine Gruppe von Ticket-IDs zurück, mit denen **Update-Abfrage** arbeitet. Die **Select-Abfrage** wird entsprechend der angegebenen Häufigkeit ausgeführt. Klicken Sie zum Anzeigen der Abfrageergebnisse auf **Ticketsuchergebnisse anzeigen**. **WICHTIG: Bearbeiten Sie SQL-Abfragen nur dann, wenn Sie die Auswirkungen genau kennen. Falsche SQL-Anweisungen könnten die Leistung der Appliance beeinträchtigen.**
Ergebnisse per E-Mail senden	Sendet die Ergebnisse der Select-Abfrage an die angegebenen E-Mail-Adressen. Alle von der Select-Abfrage zurückgegebenen Spalten sind in der E-Mail-Nachricht enthalten. Geben Sie die E-Mail-Adressen als durch Kommas getrennte Liste in das Feld *E-Mail* ein.
Kommentar an Ticket anhängen	Aktivieren Sie dieses Kontrollkästchen, um zu jedem von der Select-Abfrage zurückgegebenen Ticket einen Kommentar hinzuzufügen. Dies ist hilfreich, wenn die später genannte Update-Abfrage Tickets aktualisiert, ohne diese Informationen zu protokollieren. Sie können beispielsweise eine Mitteilung Ticketregel: Ändern der Priorität in "Hoch" veranlasst hinzufügen. Dank dieser Mitteilung können Sie erkennen, welche Tickets geändert wurden. Geben Sie beliebige Kommentare in das Feld *Kommentar* ein.
E-Mail an jeden Empfänger in den Abfrageergebnissen senden	Aktivieren Sie dieses Kontrollkästchen, um an die von der Select-Abfrage zurückgegebenen E-Mail-Adressen eine Nachricht zu senden. Alle E-Mail-Adressen, die von der Select-Abfrage in der Spalte *E-Mail* zurückgegeben werden, erhalten eine Nachricht. Variablen werden im Betreff oder Text der E-Mail ausgewertet. Zeichenfolgen wie "$title" und "$due_date" werden durch die Werte in den Spalten *TITLE* bzw. *DUE_DATE* ersetzt. Jede von der Select-Abfrage zurückgegebene Spalte kann so ersetzt werden. Der vom Assistenten für Ticketregeln erzeugte SQL-Code liefert **OWNER_**, **SUBMITTER_** und **CC_LIST** als mögliche Werte. Geben Sie den Betreff in das Feld *Betreff* ein. Geben Sie den E-Mail-Spaltennamen in das Feld *E-Mail* ein, beispielsweise OWNER_. Alle E-Mail-Adressen, die von der Select-Abfrage in der Spalte

Option	Beschreibung
	E-Mail zurückgegeben werden, erhalten eine Nachricht. Geben Sie die E-Mail-Nachricht in das Feld *E-Mail-Text* ein.
Update-Abfrage ausführen	Eine zweite Datenbankabfrage mit den Ergebnissen aus dem Feld *Update-Abfrage* als Eingabe ausführen. Nutzen Sie dieses Feld, um eine weitere SQL-UPDATE-Anweisung mit der durch Kommas getrennten Liste der Tickets auszuführen, die von der Select-Abfrage zurückgegeben wurde. Dadurch wird beispielsweise "update HD_TICKET set TITLE = 'changed' where HD_TICKET.ID in (<TICKET_IDS>)" zu "update HD_TICKET set TITLE = 'changed' where HD_TICKET.ID in (1,2,3)". Ändert die SQL-Abfrage bei Bedarf. Die Abfrage wird durch den Assistenten für Ticketregeln auf Grundlage der Kriterien generiert, die auf der Seite *Ticketregel* angegeben werden. Diese Abfrage arbeitet mit den Tickets, die von der **Select-Abfrage** ausgewählt werden. Die *Update-Abfrage* wird entsprechend der angegebenen Häufigkeit ausgeführt. **WICHTIG: Bearbeiten Sie SQL-Abfragen nur dann, wenn Sie die Auswirkungen genau kennen. Falsche SQL-Anweisungen könnten die Leistung der Appliance beeinträchtigen.**
Fälligkeitsdaten neu berechnen	Wählen Sie diese Option nur aus, wenn Ihre Update-Abfrage die Aktualisierung der Priorität vorhandener Tickets beinhaltet. Durch die Auswahl der Option werden die Fälligkeitsdaten basierend auf der neuen, durch die Ticketregel festgelegten Priorität neu berechnet. **HINWEIS:** Manuell überschriebene Fälligkeitsdaten von Tickets werden nicht durch Ticketregeln überschrieben.
Letztes Ausführungsprotokoll	Zeigt die letzten Abfrageergebnisse an, einschließlich aller Fehler. Diese Ergebnisse werden bei jeder Ausführung der Ticketregel aktualisiert.
Häufigkeit	Das Intervall, in dem die Ticketregel ausgeführt wird. **HINWEIS:** Ticketregeln, die *beim Speichern des Tickets* ausgeführt werden, sollten so konzipiert werden, dass sie für ein einzelnes Ticket funktionieren und ein einzelnes Ereignis auslösen. Ticketregeln, die nach einem Zeitplan ausgeführt werden, können für mehrere Tickets ausgeführt werden und mehrere Ereignisse auslösen.

Option	Beschreibung
Nächste Ausführung	Datum und Uhrzeit der nächsten Ausführung der Ticketregel.

10. Klicken Sie auf **Jetzt ausführen**, um die Ticketregel sofort auszuführen.
11. Klicken Sie auf **Speichern**.

Benutzerdefinierte Ticketregeln duplizieren

Wenn Sie eine benutzerdefinierte Ticketregel duplizieren, werden deren Eigenschaften in die neue Regel kopiert. Wenn Sie eine Regel erstellen möchten, die einer bereits vorhandenen Regel ähnelt, können Sie durch das Duplizieren der Ticketregel Zeit sparen.

1. Rufen Sie die Seite *Warteschlangen-Detail* des Service Desks auf:
    a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
    b. Klicken Sie in der linken Navigationsleiste auf **Service Desk** und anschließend auf **Konfiguration**.
    c. Klicken Sie im Fensterbereich **Konfiguration** auf **Warteschlangen**.
    d. Klicken Sie auf den Namen einer Warteschlange.
2. Klicken Sie unten auf der Seite im Abschnitt *Ticketregeln* auf **[Anpassen]**, um die Seite *Ticketregeln* anzuzeigen.
3. Klicken Sie auf eine Ticketregel, um sie zu öffnen.
4. Klicken Sie unten auf der Seite auf die Schaltfläche **Duplizieren**.

    Die Seite *Ticketregeln* wird mit der neuen Regel angezeigt. Der Standardname lautet **Kopie von Originalregel**.
5. Ändern Sie die duplizierte Ticketregel entsprechend Ihren Anforderungen oder benennen Sie sie um.

    Informationen zu Ticketregelfeldern finden Sie unter Benutzerdefinierte Ticketregeln erstellen.

Benutzerdefinierte Ticketregeln löschen

Sie können benutzerdefinierte Ticketregeln bei Bedarf aus dem Service Desk löschen.

1. Rufen Sie die Seite *Warteschlangen-Detail* des Service Desks auf:
    a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
    b. Klicken Sie in der linken Navigationsleiste auf **Service Desk** und anschließend auf **Konfiguration**.
    c. Klicken Sie im Fensterbereich **Konfiguration** auf **Warteschlangen**.

   d. Klicken Sie auf den Namen einer Warteschlange.
2. Klicken Sie unten auf der Seite im Abschnitt *Ticketregeln* auf **[Anpassen]**, um die Seite *Ticketregeln* anzuzeigen.
3. Führen Sie einen der folgenden Schritte aus:
   - **Aktivieren Sie das Kontrollkästchen neben der Ticketregel und klicken Sie anschließend auf Aktion auswählen > Löschen.**
   - **Klicken Sie auf den Namen der Ticketregel und dann auf der Seite** *Detail zur Ticketregel* **auf Löschen.**
4. Klicken Sie zur Bestätigung auf **Ja**.

Ticketregeln von einer Warteschlange in eine andere verschieben

Wenn Sie mehrere Service Desk-Ticketwarteschlangen haben, können Sie Ticketregeln nach Bedarf zwischen Warteschlangen verschieben. Falls Sie eine Ticketregel in mehreren Warteschlangen verwenden möchten, können Sie sie kopieren und dann die erforderlichen Änderungen vornehmen.

1. Rufen Sie die Liste *Warteschlangen* des Service Desks auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Service Desk** und anschließend auf **Konfiguration**.
   c. Klicken Sie im Fensterbereich **Konfiguration** auf **Warteschlangen**.
2. Klicken Sie auf die Warteschlange mit der zu verschiebenden Ticketregel.

   Die Seite *Warteschlangen-Detail* wird angezeigt.
3. Klicken Sie unten auf der Seite im Abschnitt *Ticketregeln* auf **Anpassen**, um die Seite *Ticketregeln* anzuzeigen.

   TIPP: Verwenden Sie die Dropdown-Liste *Anzeigen nach*, die über der Tabelle auf der rechten Seite angezeigt wird, um auf der Seite *Ticketregeln* zwischen Warteschlangen wechseln.
4. Aktivieren Sie das Kontrollkästchen neben der Ticketregel.
5. Wählen Sie **Aktion auswählen** > **Verschieben** > **Warteschlangenname** aus.

Die Ticketregel wird in die ausgewählte Warteschlange verschoben. Die Regel wird nicht mehr in der Regelliste der aktuellen Warteschlange angezeigt.

Ausführen von Service Desk-Berichten

Sie können Berichte zu Service Desk-Elementen nach Bedarf ausführen.

Die Appliance enthält eine Reihe vorkonfigurierter Berichte für Service Desk-Daten.

1. Rufen Sie die Liste *Berichte* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Berichterstellung** und anschließend auf **Berichte**.
2. Wählen Sie rechts oberhalb der Liste in der Dropdown-Liste *Anzeigen nach* die Option **Service Desk** aus.

Die Seite *Berichte* zeigt Service Desk-Berichte an.

3. Klicken Sie in der Spalte *Bericht generieren* auf einen Formattyp, um den Bericht auszuführen.

HINWEIS: Weitere Informationen zu Berichten finden Sie unter Informationen zu Berichten.

Archivieren, Wiederherstellen und Löschen von Tickets

Bei der Archivierung von Tickets werden die Ticketdaten physisch aus den Transaktionstabellen verschoben, wobei der Zugriff auf die Ticketdaten erhalten bleibt. Durch die Archivierung werden die Ticketdaten nicht dauerhaft von der Appliance gelöscht. Diese Funktion ist für alte Tickets hilfreich, die Sie möglicherweise noch zur Referenz benötigen.

Wenn Tickets archiviert werden, bleiben sie so lange erhalten, bis sie manuell oder basierend auf in der Warteschlange konfigurierten Datenbeschränkungen gelöscht werden. Diese Einschränkung verringert das Risiko, dass Tickets versehentlich gelöscht werden.

Der typische Lebenszyklus für Tickets umfasst die Erstellung, Lösung, Archivierung und endgültige Löschung. Tickets können auch wie in Archivierte Tickets wiederherstellen beschrieben "wiederhergestellt" werden. Bei der Wiederherstellung eines Tickets werden dessen Daten aus der Archivtabelle zurück in die Transaktionstabelle verschoben, sodass die Ticketdaten wieder über die Registerkarte *Tickets* verfügbar sind.

Durch das Löschen von Tickets werden die Ticketdaten unwiderruflich aus der Appliance gelöscht.

Ticketarchivierung aktivieren

Sie können die Ticketarchivierung für den Service Desk oder bei aktivierter Organisationskomponente für den Service Desk der jeweils ausgewählten Organisation aktivieren.

1. Rufen Sie die Seite *Service Desk-Einstellungen* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Service Desk** und anschließend auf **Konfiguration**.
   c. Klicken Sie im Fensterbereich **Konfiguration** auf **Einstellungen**.
2. Aktivieren Sie im Abschnitt *Ticketarchivierung* das Kontrollkästchen **Aktiviert**, um die Zeitplanoptionen anzuzeigen.
3. Legen Sie die folgenden Einstellungen fest:

HINWEIS: Wenn Sie keine zeitplangesteuerte Ticketarchivierung durchführen möchten, klicken Sie auf **Jetzt ausführen**, um Tickets jederzeit zu archivieren und zu löschen. Diese Option erfasst alle Warteschlangen, für die die Archivierung konfiguriert wurde. Die Option **Jetzt ausführen** ist außerdem für jede Warteschlange verfügbar. Bei der Verwendung dieser Option wird die Archivierung und Löschung von Tickets mit den Einstellungen der jeweiligen Warteschlange ausgeführt.

Option	Beschreibung
Alle __ Stunden	Der Vorgang wird im angegebenen Intervall durchgeführt.

Option	Beschreibung
Täglich/an einem bestimmten Tag um HH:MM	Die Erfassung wird täglich zu einem bestimmten Zeitpunkt oder an einem bestimmten Wochentag um eine bestimmte Uhrzeit ausgeführt.
Ausführen am n-ten jedes Monats/eines bestimmten Monats um HH:MM	Die Erfassung wird jeden Monat oder in einem bestimmten Monat an einem festgelegten Datum zu einer festgelegten Uhrzeit ausgeführt.
Ausführen am n-ten Wochentag **jedes Monats/ eines bestimmten Monats um HH:MM**	Die Erfassung wird jeden Monat oder in einem bestimmten Monat an einem festgelegten Wochentag zu einer festgelegten Uhrzeit ausgeführt.

Benutzerdefiniert	Ausführung nach einem benutzerdefinierten Zeitplan.
	Verwenden Sie das Standard-5-Feld-Cron-Format (das erweiterte Cron-Format wird nicht unterstützt):
	`* * * * *`
	`| | | | +————Wochentag (0-6) (Sonntag=0)`
	`| | | +————Monat (1-12)`
	`| | +————Monatstag (1-31)`
	`| +————Stunde (0-23)`
	`+————Minute (0-59)`
	Verwenden Sie bei der Angabe von Werten die folgenden Zeichen:
	• **Leerzeichen( )**: Die einzelnen Felder mit einem Leerzeichen trennen.
	• **Sternchen (*)**: Ein Sternchen repräsentiert den gesamten Wertebereich in einem Feld. Zum Beispiel repräsentiert ein Sternchen im Stundenfeld eine beliebige Stunde.
	• **Kommas (,)**: Mehrere Werte in einem Feld werden mit einem Komma getrennt. Zum Beispiel werden mit `0,6` im Feld „Wochentag“ Sonntag und Samstag angegeben.
	• **Bindestriche (-)**: Mit einem Bindestrich wird ein Wertebereich in einem Feld angegeben. Zum Beispiel entspricht `1-5` im Feld „Wochentag“ `1,2,3,4,5`, d. h. Montag bis Freitag.
	• **Schrägstriche (/)**: Die Angabe der Zeitabstände, mit denen eine Aktion wiederholt werden soll, erfolgt mit einem Schrägstrich. Zum Beispiel entspricht `*/3` im Feld Stunde `0,3,6,9,12,15,18,21`. Das Sternchen (`*`) gibt jede Stunde an, mit `/3` erfolgt aber eine Einschränkung auf durch drei teilbare Stunden.

Option	Beschreibung
	Beispiele: • `15 * * * *` Jeden Tag 15 Minuten nach jeder vollen Stunde ausführen • `0 22 * * *` Jeden Tag um 22:00 Uhr ausführen • `0 0 1 1,6 *` Am 1. Januar und 1. Juni um 00:00 Uhr ausführen • `30 8,12 * * 1-5` An Wochentagen um 08:30 Uhr und 12:30 Uhr ausführen • `0 2 */2 * *` Jeden zweiten Tag um 02:00 Uhr ausführen
Aufgabenplan anzeigen	Klicken Sie, um den Aufgabenplan anzuzeigen. Im Dialogfeld *Taskplan* wird eine Liste der geplanten Ziele angezeigt. Klicken Sie auf eine Aufgabe, um die Aufgabendetails anzuzeigen. Weitere Informationen hierzu finden Sie unter Aufgabenpläne anzeigen.

4. Führen Sie einen der folgenden Schritte aus:
   - **Klicken Sie auf Jetzt ausführen, um sie sofort für alle Warteschlangen auszuführen, für die die Archivierung konfiguriert wurde. Siehe Ausgewählte Tickets archivieren.**
   - **Klicken Sie auf Speichern.**

     Die Ticketarchivierung ist für den Service Desk oder bei aktivierter Organisationskomponente für die jeweils ausgewählte Organisation aktiviert. Sie müssen jedoch bestimmte Warteschlangen konfigurieren, um die Tickets auszuwählen, die Sie archivieren möchten. Siehe Einstellungen für die Warteschlangenarchivierung konfigurieren.
     Der Link *Service Desk > Archiv* wird in der linken Navigationsleiste angezeigt.

Einstellungen für die Warteschlangenarchivierung konfigurieren

Wenn die Ticketarchivierung aktiviert ist, können Sie die Archivierungseinstellungen für jede Warteschlange individuell konfigurieren.

Sie haben die Ticketarchivierung für den Service Desk aktiviert. Informationen zum Aktivieren der Ticketarchivierung finden Sie unter Ticketarchivierung aktivieren.

1. Rufen Sie die Seite *Warteschlangen-Detail* des Service Desks auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Service Desk** und anschließend auf **Konfiguration**.
   c. Klicken Sie im Fensterbereich **Konfiguration** auf **Warteschlangen**.
   d. Klicken Sie auf den Namen einer Warteschlange.
2. Wählen Sie im Abschnitt *Archiveinstellungen* die Einstellungen für die Ticketarchivierung aus. Klicken Sie auf den Link **Einstellungen**, um die Ticketarchivierung zu aktivieren.

HINWEIS: Wenn die Ticketarchivierung abgeschaltet ist, siehe Ticketarchivierung aktivieren.

Option	Beschreibung
Archiv geschlossen für Tickets älter als	Das Alter der zu archivierenden Tickets. Wenn Sie z. B. **3 Monate** auswählen, werden die Tickets nach dem Ablauf von drei Monaten nach ihrer Schließung archiviert. Um zu verhindern, dass in der Warteschlange enthaltene Tickets archiviert werden, wählen Sie **Nie** aus. Archivierte Tickets können gegebenenfalls in der Warteschlange wiederhergestellt werden. Siehe Archivierte Tickets wiederherstellen.
Löschen von archivierten Tickets älter als	Das Alter von Tickets, die dauerhaft aus dem Archiv entfernt werden sollen. Wenn Sie z. B. **6 Monate** auswählen, werden archivierte Tickets nach dem Ablauf von sechs Monaten nach ihrer Archivierung aus dem Archiv gelöscht. Um zu verhindern, dass in der Warteschlange enthaltene Tickets aus dem Archiv gelöscht werden, wählen Sie **Nie** aus. Gelöschte Tickets können nicht in der Warteschlange wiederhergestellt werden.

3. Klicken Sie unten auf der Seite auf **Speichern**.
4. Klicken Sie auf **Jetzt ausführen**, um die Tickets zu archivieren und zu löschen, die den unter *Archiveinstellungen* angegebenen Kriterien entsprechen.

Ausgewählte Tickets archivieren

Wenn die Archivierung von Service-Desk-Tickets aktiviert ist, können Sie ausgewählte Tickets nach Bedarf archivieren.

Sie haben die Ticketarchivierung für den Service Desk aktiviert. Informationen zum Aktivieren der Ticketarchivierung finden Sie unter Ticketarchivierung aktivieren.

TIPP: Die Auswahl der zu archivierenden Tickets ist hilfreich, wenn Sie bestimmte Tickets archivieren möchten oder wie unter Ticketarchivierung aktivieren beschrieben keinen Zeitplan für die Archivierung festgelegt haben.

1. Rufen Sie die Liste *Tickets* des Service Desks auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Service Desk** und anschließend auf **Tickets**.
2. Aktivieren Sie das Kontrollkästchen neben mindestens einem Ticket.
3. Klicken Sie auf **Aktion auswählen** > **Archiv**.
4. Klicken Sie im Bestätigungsdialogfeld auf **Ja**.
5. Wenn Sie auf archivierte Tickets zugreifen möchten, klicken Sie auf **Service Desk** > **Archiv** und anschließend auf den Link für das Ticket, das Sie anzeigen möchten.

Archivierte Tickets wiederherstellen

Archivierte Tickets können bei Bedarf in der Ticket-Warteschlange wiederhergestellt werden.

1. Rufen Sie die Liste *Archivierte Tickets* des Service Desks auf:
    a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
    b. Klicken Sie in der linken Navigationsleiste auf **Service Desk** und anschließend auf **Archiv**.
2. Aktivieren Sie das Kontrollkästchen neben mindestens einem archivierten Ticket.
3. Klicken Sie auf **Aktion auswählen** > **Wiederherstellen** und anschließend zum Bestätigen auf **Ja**.

Das Ticket wird sofort auf der Registerkarte *Tickets* wiederhergestellt.

Archivierte Tickets löschen

Sie können archivierte Tickets löschen, um sie dauerhaft aus dem Service Desk zu entfernen. Gelöschte Tickets können nicht wiederhergestellt werden.

1. Rufen Sie die Liste *Archivierte Tickets* des Service Desks auf:
    a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
    b. Klicken Sie in der linken Navigationsleiste auf **Service Desk** und anschließend auf **Archiv**.
2. Aktivieren Sie das Kontrollkästchen neben mindestens einem archivierten Ticket.
3. Wählen Sie **Aktion auswählen** > **Löschen** und klicken Sie dann zum Bestätigen auf **Ja**.

Das Ticket wird sofort aus der Appliance entfernt.

Verwalten der Ticketlöschung

Standardmäßig kann jeder Service Desk-Administrator oder Ticketbesitzer Tickets aus einer Warteschlange löschen. Sie können diese Einstellung bei Bedarf ändern. Wenn Sie mehrere Warteschlangen haben, können die einzelnen Warteschlangen unterschiedliche Einstellungen aufweisen.

Einstellungen für die Ticketlöschung konfigurieren

Sie können Einstellungen für die Löschung von Service-Desk-Tickets für Warteschlangen konfigurieren. Wenn Sie mehrere Warteschlangen haben, können Sie für die einzelnen Warteschlangen unterschiedliche Einstellungen konfigurieren.

1. Rufen Sie die Seite *Warteschlangen-Detail* des Service Desks auf:
    a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
    b. Klicken Sie in der linken Navigationsleiste auf **Service Desk** und anschließend auf **Konfiguration**.
    c. Klicken Sie im Fensterbereich **Konfiguration** auf **Warteschlangen**.

   d. Klicken Sie auf den Namen einer Warteschlange.
2. Führen Sie im Abschnitt *Benutzereinstellungen* einen der folgenden Schritte aus:
   - **Um zu verhindern, dass Administratoren und Ticketbesitzer Tickets löschen können, deaktivieren Sie das Kontrollkästchen** *Löschen von Tickets zulassen***.**
   - **Um Administratoren und Ticketbesitzern das Löschen von Tickets zu ermöglichen, aktivieren Sie das Kontrollkästchen** *Löschen von Tickets zulassen***.**
3. Klicken Sie auf **Speichern**.

Tickets löschen

Wenn die Ticketlöschung in den Service Desk-Warteschlangeneinstellungen aktiviert ist, können Sie Tickets bei Bedarf löschen.

Sie haben die Ticketlöschung für die Warteschlange aktiviert. Siehe Einstellungen für die Ticketlöschung konfigurieren.

1. Rufen Sie die Liste *Tickets* des Service Desks auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Service Desk** und anschließend auf **Tickets**.
2. Aktivieren Sie das Kontrollkästchen neben mindestens einem Ticket.
3. Wählen Sie **Aktion auswählen > Löschen** und klicken Sie dann zum Bestätigen auf **Ja**.

Verwalten von Warteschlangen für Service-Desk-Tickets

Standardmäßig enthält der Service Desk nur eine Ticketwarteschlange und in vielen Fällen genügt diese Warteschlange für eine Organisation, um effektiv zu funktionieren. Sie können aber Warteschlangen nach Bedarf hinzufügen, duplizieren und löschen. Sie können auch eine oder mehrere Ticketvorlagen in einer Warteschlange erstellen. Wenn mehrere Vorlagen in einer Warteschlange vorhanden sind, müssen Sie eine Ticketvorlage als Standardvorlage auswählen.

Informationen zu Service Desk-Ticketwarteschlangen

Service Desk-Tickets werden in einer oder mehreren Warteschlangen auf der Appliance gespeichert. Die meisten Organisationen benötigen nur eine einzige Warteschlange. Sie können jedoch bei Bedarf weitere Warteschlangen erstellen und verwalten.

Über mehrere Ticketwarteschlangen zu verfügen ist in folgenden Fällen hilfreich:

- **Sie haben verschiedene Ticketgruppen mit unterschiedlichen Anforderungen**. Dies könnte beispielsweise der Fall sein, wenn Sie Tickets für häufige Service Desk-Aufgaben wie das Beheben von Geräteproblemen und darüber hinaus auch für die Verfolgung von Problemen mit der Fahrzeugflotte Ihrer

Organisation verwenden. In diesem Fall können Sie für jeden Problemtyp eine separate Warteschlange einrichten.

- **Service Desk-Mitarbeiter sind einer bestimmten Ticketgruppe zugewiesen**. Wenn Ihre Organisation beispielsweise über Niederlassungen in verschiedenen Städten verfügt und jeder Standort Service Desk-Mitarbeiter beschäftigt, die nur für diesen Standort zuständig sind, können Sie getrennte Warteschlangen verwalten. Wenn Ihre Service Desk-Mitarbeiter jedoch mehrere Niederlassungen von einem einzigen Standort aus betreuen, kommen Sie mit einer Warteschlange aus.

Weitere Informationen zum Konfigurieren von Ticketwarteschlangen finden Sie unter Konigurieren von Service Desk-Ticketwarteschlangen.

Hinzufügen und Löschen von Warteschlangen

Sie können Warteschlangen nach Bedarf hinzufügen, duplizieren und löschen. Dies kann hilfreich sein, wenn Sie unterschiedliche Tickettypen für verschiedene Gruppen in Ihrer Organisation einrichten möchten.

Warteschlangen hinzufügen

Sie können Service Desk-Warteschlangen nach Bedarf hinzufügen.

Wenn Sie vorhaben, Service-Desk-Tickets von einer Warteschlange in eine andere zu verschieben, achten Sie darauf, dass beide Warteschlangen dieselben Werte (einschließlich benutzerdefinierter Felder) verwenden. Anderenfalls werden die Daten aus der alten Warteschlange an die neue angepasst. Siehe Verschieben von Tickets zwischen Warteschlangen.

1. Rufen Sie die Seite *Warteschlangen-Detail* des Service Desks auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Service Desk** und anschließend auf **Konfiguration**.
   c. Klicken Sie im Fensterbereich **Konfiguration** auf **Warteschlangen**.
   d. Wählen Sie **Aktion auswählen** > **Neu**.
2. Geben Sie für die neue Warteschlange Werte für *Name*, *E-Mail-Adresse* und *Alternative E-Mail-Adresse* ein.

   VORSICHT: Bei der Zustellung von E-Mails direkt an die Appliance (Weiterleitung von E-Mails an die Appliance) müssen der lokale Teil der Adresse der Appliance und derjenige der alternativen Adresse übereinstimmen. Beispiel: servicedesk@kbox und servicedesk@company.com.

   VORSICHT: Jede Warteschlange muss über eigene E-Mail-Adressen verfügen. Bevor Sie die neue Warteschlange speichern können, wird dies von der Appliance geprüft. Wenn Sie eine E-Mail-Adresse angeben, die bereits mit einer anderen Warteschlange verknüpft ist, wird eine Warnung angezeigt.
3. Wenn Sie einen POP3-Server verwenden, geben Sie in den Feldern *Benutzer/Kennwort* Benutzer-ID und Kennwort für die POP3-E-Mail ein.

   Siehe Informationen zu POP3-E-Mail-Konten.

   TIPP: Wenn Sie POP verwenden, um E-Mails auf die Appliance herunterzuladen, können Sie jede gültige Mailbox verwenden.
4. Zur Einrichtung der POP3-Authentifizierung können Sie für die Warteschlange Secure Sockets Layer (SSL) übernehmen. Aktivieren Sie dazu das Kontrollkästchen *SSL*.

Die Einstellung dieser Option hängt davon ab, wie Sie Ihr POP3-Konto konfiguriert haben.

5. Klicken Sie auf **Speichern**.
6. Wählen Sie nach Bedarf weitere Einstellungen für die Warteschlange aus. Siehe Konigurieren von Service Desk-Ticketwarteschlangen.

Warteschlangen durch Duplizieren einer vorhandenen Warteschlange hinzufügen

Wenn Sie eine Warteschlange duplizieren oder klonen, werden alle Daten in der vorhandenen Warteschlange in die neue Warteschlange kopiert. Dies kann weniger Zeit in Anspruch nehmen als die vollständige Neuerstellung einer Warteschlange. Die Ticketregeln werden in die duplizierte Warteschlange kopiert, jedoch standardmäßig deaktiviert.

1. Rufen Sie die Liste *Warteschlangen* des Service Desks auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Service Desk** und anschließend auf **Konfiguration**.
   c. Klicken Sie im Fensterbereich **Konfiguration** auf **Warteschlangen**.
2. Klicken Sie auf den Namen einer Warteschlange, um die Seite *Warteschlangen-Detail* anzuzeigen.
3. Klicken Sie unten auf der Seite auf **Duplizieren**.

   Die neue Warteschlange hat den gleichen Namen wie diejenige, von der sie dupliziert wurde, ergänzt durch eine angehängte eindeutige Bezeichnernummer. Die Ticketregeln sind in der neuen Warteschlange standardmäßig deaktiviert.
4. Ändern Sie den Namen und die Einstellungen der Warteschlange wie gewünscht.
5. Klicken Sie auf **Speichern**.

Warteschlangen löschen

Sie können Warteschlangen nach Bedarf löschen.

> **VORSICHT: Stellen Sie vor dem Löschen einer Warteschlange sicher, dass Sie auch wirklich sämtliche Daten in der Warteschlange löschen möchten. Hierzu zählen auch zugehörige Tickets und Prozesse. Diese Aktion kann nicht rückgängig gemacht werden.**

1. Rufen Sie die Seite *Warteschlangen-Detail* des Service Desks auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Service Desk** und anschließend auf **Konfiguration**.
   c. Klicken Sie im Fensterbereich **Konfiguration** auf **Warteschlangen**.
   d. Klicken Sie auf den Namen einer Warteschlange.
2. Klicken Sie unten auf der Seite auf **Löschen** und dann zur Bestätigung auf **Ja**.

Anzeigen von Tickets in Warteschlangen

Sie können die Seite *Tickets* sortieren, um sämtliche Tickets in all Ihren Warteschlangen in einer Liste anzuzeigen. Wenn Sie mehrere Warteschlangen haben, können Sie festlegen, welche Warteschlange standardmäßig auf der Seite *Tickets* angezeigt werden soll.

Wenn Sie mehrere Warteschlangen haben, können Sie auswählen, welche Warteschlange standardmäßig auf der Seite *Tickets* angezeigt werden soll. Die Standardwarteschlange kann auf folgenden Ebenen angegeben werden:

- **Auf Systemebene**. Diese Einstellung wird verwendet, wenn keine Benutzereinstellungen angegeben werden. Siehe Standardwarteschlangen auf Systemebene festlegen.
- **Auf Benutzerebene**. Diese Einstellung überschreibt die Einstellungen auf Systemebene. Einzelne Benutzer und Administratoren, die zum Ändern von Benutzereinstellungen berechtigt sind, können die Standardwarteschlange auf der Benutzerebene angeben. Siehe Standardwarteschlangen auf Benutzerebene festlegen.

Ticket warteschlangenübergreifend anzeigen

Wenn Sie mehrere Warteschlangen haben, können Sie Tickets aus allen Warteschlangen in derselben Liste anzeigen.

1. Rufen Sie die Liste *Tickets* des Service Desks auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Service Desk** und anschließend auf **Tickets**.
2. Wählen Sie über der Tabelle in der Dropdown-Liste *Warteschlange* die Option **Alle Warteschlangen** aus.
3. Wählen Sie rechts neben der Dropdown-Liste *Warteschlange* in der Dropdown-Liste *Anzeigen nach* die Ticketgruppe aus, die Sie anzeigen möchten.

Einrichten der Standardwarteschlange

Wenn Sie mehrere Warteschlangen haben, können Sie auswählen, welche Warteschlange standardmäßig auf der Seite *Tickets* angezeigt werden soll.

Die Standardwarteschlange kann auf folgenden Ebenen angegeben werden:

- **Auf Systemebene**. Diese Einstellung wird verwendet, wenn keine Benutzereinstellungen angegeben werden. Siehe Standardwarteschlangen auf Systemebene festlegen.
- **Auf Benutzerebene**. Diese Einstellung überschreibt die Einstellungen auf Systemebene. Einzelne Benutzer und Administratoren, die zum Ändern von Benutzereinstellungen berechtigt sind, können die Standardwarteschlange auf der Benutzerebene angeben. Siehe Standardwarteschlangen auf Benutzerebene festlegen.

Standardwarteschlangen auf Systemebene festlegen

Die Einstellungen der Standardwarteschlange auf Systemebene bestimmen, welche Ticketwarteschlange standardmäßig angezeigt wird, sofern keine Einstellungen auf Benutzerebene vorgenommen wurden.

1. Rufen Sie die Seite *Einstellungen* des Service Desks auf:

a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://appliance_hostname/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.

b. Klicken Sie in der linken Navigationsleiste auf **Service Desk** und anschließend auf **Konfiguration**.

c. Klicken Sie im Fensterbereich *Konfiguration* auf **Einstellungen**.

2. Wählen Sie im Abschnitt *Einstellungen für Warteschlange* in der Dropdown-Liste *Standardwarteschlange für Ticket-Liste* eine Option aus:

Option	Beschreibung
Kein Standard	Bei der Anzeige von Warteschlangen keine Standardeinstellung verwenden. Bei Auswahl dieser Option wird standardmäßig die erste zum System hinzugefügte Warteschlange angezeigt, wenn Benutzer auf **Service Desk** > **Tickets** klicken. Diese Einstellung wird ignoriert, wenn eine Einstellung auf Benutzerebene angegeben wird.
Alle Warteschlangen	Standardmäßig die Ansicht *Alle Warteschlangen* anzeigen. Bei Auswahl dieser Option wird die Ansicht *Alle Warteschlangen* angezeigt, wenn Benutzer auf **Service Desk** > **Tickets** klicken. Diese Einstellung wird ignoriert, wenn eine Einstellung auf Benutzerebene angegeben wird.
<Warteschlangenname>	Standardmäßig die ausgewählte Warteschlange anzeigen. Bei Auswahl dieser Option wird die angegebene Warteschlange angezeigt, wenn Benutzer auf **Service Desk** > **Tickets** klicken. Diese Einstellung wird ignoriert, wenn eine Einstellung auf Benutzerebene angegeben wird. Wenn eine Warteschlange in dieser Liste nicht angezeigt wird, überprüfen Sie, ob Sie zur Anzeige der Warteschlange berechtigt sind.

TIPP: Diese Einstellungen können auf Benutzerebene überschrieben werden. Siehe Standardwarteschlangen auf Benutzerebene festlegen.

3. Klicken Sie auf **Speichern**.

Standardwarteschlangen auf Benutzerebene festlegen

Die Warteschlangeneinstellungen auf Benutzerebene bestimmen, welche Ticketwarteschlange standardmäßig angezeigt wird. Einstellungen auf Benutzerebene haben Vorrang vor Einstellungen auf Systemebene. Einzelne Benutzer und Administratoren, die zum Ändern von Benutzereinstellungen berechtigt sind, können die Standardwarteschlange auf der Benutzerebene angeben.

Falls keine Standardwarteschlange auf Benutzerebene festgelegt wurde, wir die Standardwarteschlange auf Systemebene verwendet.

1. Rufen Sie die Seite *Benutzerdetails* auf.

a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://appliance_hostname/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen*

aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.

b. Klicken Sie auf der linken Navigationsleiste auf **Einstellungen** und anschließend auf **Benutzer**.

c. Klicken Sie auf den Namen eines Benutzers.

2. Wählen Sie aus der Dropdown-Liste *Standardwarteschlange* eine Option aus:

Option	Beschreibung
Kein Standard	Bei der Anzeige von Warteschlangen keine Standardeinstellung verwenden. Bei Auswahl dieser Option wird standardmäßig die erste zum System hinzugefügte Warteschlange angezeigt, wenn der ausgewählte Benutzer auf **Service Desk** > **Tickets** klickt.
Alle Warteschlangen	Standardmäßig die Ansicht *Alle Warteschlangen* anzeigen. Bei Auswahl dieser Option wird die Ansicht *Alle Warteschlangen* angezeigt, wenn der ausgewählte Benutzer auf **Service Desk** > **Tickets** klickt.
<Warteschlangenname>	Standardmäßig die ausgewählte Warteschlange anzeigen. Bei Auswahl dieser Option wird die angegebene Warteschlange angezeigt, wenn der ausgewählte Benutzer auf **Service Desk** > **Tickets** klickt. Wenn eine Warteschlange in dieser Liste nicht angezeigt wird, überprüfen Sie, ob Sie zur Anzeige der Warteschlange berechtigt sind.

3. Klicken Sie auf **Speichern**.

Standardwerte für die Ticketliste "Alle Warteschlangen" festlegen

Sie können die Ticketfelder festlegen, die in der Ansicht *Alle Warteschlangen* angezeigt werden sollen.

Wenn Sie mehrere Warteschlangen haben, können Sie in der Ansicht *Alle Warteschlangen* alle Tickets im System in einer einzigen Liste anzeigen.

Beispielsweise können für jede Warteschlange unterschiedliche Namen für Ticketfelder verwendet werden. In einer Warteschlange wird möglicherweise das Ticketfeld *Priorität* verwendet, in einer anderen Warteschlange das Ticketfeld *Geschäftliche Auswirkungen*. Sie können auswählen, welches Feld in der Ansicht *Alle Warteschlangen* angezeigt werden soll.

Felder werden entsprechend den folgenden Einstellungen angezeigt:

- Die Feldnamen in der Warteschlange, die als die *Standard-Warteschlange für Feld-Labels der Anzeige 'Alle Warteschlangen'* ausgewählt wurde
- Die Felder, die in der Einstellung *Listenlayout für 'Alle Warteschlangen' anpassen* angegeben sind

1. Rufen Sie die Seite *Einstellungen* des Service Desks auf:

   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.

b. Klicken Sie in der linken Navigationsleiste auf **Service Desk** und anschließend auf **Konfiguration**.

c. Klicken Sie im Fensterbereich *Konfiguration* auf **Einstellungen**.

2. Wählen Sie im Abschnitt *Warteschlangeneinstellungen* in der Dropdown-Liste *Ticket-Listenlayout für alle Warteschlangen* eine Warteschlange aus.

   Die Feldnamen aus dieser Warteschlange werden auf der Seite *Tickets* angezeigt.

3. Klicken Sie auf **Speichern**.
4. Klicken Sie auf **Listenlayout für 'Alle Warteschlangen' anpassen**, um die Seite *Layout* anzuzeigen.
5. Ändern Sie die Felder über die folgenden Symbole:

   - : Ein Feld hinzufügen.
   - : Feldnamen oder Breite der Feldspalte ändern

     HINWEIS: Die Breite gibt an, welcher Teil der verfügbaren Seitenbreite der Feldspalte zugewiesen wird. Wenn Sie beispielsweise 10 Spalten haben und jeder Spalte die Breite 10 zugewiesen ist, wäre die Summe aller Zahlen in der Spalte *Breite* 100. Daher hätte jede Feldspalte eine Breite von 10 Prozent der verfügbaren Seitenbreite. Wenn die Summe aller Zahlen in der Spalte *Breite* mehr oder weniger als 100 beträgt, werden die Zahlen zur Bestimmung der Breite auf Prozentsätze normalisiert. Wenn Sie beispielsweise 3 Spalten haben und jeder Spalte wird eine Breite von 10 zugewiesen, beträgt die Gesamtzahl in der Spalte "Breite" 30. Durch die Normierung zu Prozentangaben beliefe sich die Breite pro Spalte auf etwa 33,3 Prozent.

     TIPP: Mit den in der *Ansicht Alle Warteschlangen* angegebenen Feldspaltenbreiten werden die Eigenschaften einzelner Warteschlangen überschrieben.

   - : Reihenfolge, in der Felder angezeigt werden, durch Ziehen ändern
   - : Feld löschen

6. Klicken Sie bei jedem bearbeiteten Feld am Ende der Zeile auf **Speichern**.

   Die Einstellungen für die Standardwarteschlange werden gespeichert.

7. Zeigen Sie die neuen Einstellungen an:

   a. Klicken Sie auf **Service Desk > Tickets**, um die Seite anzuzeigen.

   b. Wählen Sie in der Dropdown-Liste *Warteschlange* die Option **Alle Warteschlangen** aus. Wählen Sie in der Dropdown-Liste *Anzeigen nach* die Option **Alle Tickets** aus.

      Felder aus der ausgewählten Warteschlange werden in der Liste in der Reihenfolge angezeigt, die in den Einstellungen für die Warteschlange angegeben ist.

      VORSICHT: Wenn das System in der Ansicht *Alle Warteschlangen* **aktive Tickets oder alle Tickets anzeigt, werden im Menü** *Aktion auswählen* **und in der Dropdown-Liste** *Anzeigen nach* **die Standardeinstellungen verwendet. Anpassungen, die in einzelnen Warteschlangen angezeigt werden, gelten nicht für die Ansicht** *Alle Warteschlangen***.**

Verschieben von Tickets zwischen Warteschlangen

Wenn Sie mehrere Warteschlangen haben, können Sie Tickets nach Bedarf zwischen diesen verschieben.

Wenn Sie ein Ticket in eine andere Warteschlange verschieben, werden die ursprünglichen Einstellungen dieses Tickets wie Status, Auswirkung, Priorität oder Kategorie durch die Einstellungen in der Warteschlange

überschrieben, in die das Ticket verschoben wird. Die ursprünglichen Werte sind im Änderungsverlauf des Tickets gespeichert.

Das folgende Beispiel zeigt, wie ein benutzerdefiniertes Feld behandelt wird, wenn Tickets zwischen Warteschlangen verschoben werden:

1. Das Feld *CUSTOM_1* im Ticket, das verschoben wird, enthält als Problemursache den Wert **Pilotfehler**.
2. Das Feld *CUSTOM_1* der Zielwarteschlange enthält Orte wie **Tampa**, **Los Angeles** und **Denver**.

   Der Wert von CUSTOM_1, **Pilotfehler**, wird im Ticket, das verschoben wird, beibehalten.
3. Wenn Sie den Wert von *CUSTOM_1* des Tickets, das verschoben wird, in **Tampa** ändern, steht der Wert **Pilotfehler** nicht mehr für das verschobene Ticket zur Verfügung.
1. Rufen Sie die Seite *Details zum Ticket* des Service Desks auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Service Desk** und anschließend auf **Tickets**.
   c. Klicken Sie auf den Titel eines Tickets.
2. Klicken Sie auf **Aktion auswählen** > **In Warteschlange verschieben** > **Warteschlangenname**.
3. Klicken Sie auf **Ja**, um das Verschieben des Tickets zu bestätigen.
4. Klicken Sie auf **Speichern**, um das Ticket in der neuen Warteschlange zu speichern.

Informationen zu Benutzerdownloads und Knowledge Base-Artikeln

Sie können Software, Skripte und andere herunterladbare Dateien über die **Benutzerkonsole** an Benutzer verteilen. Darüber hinaus können Sie Benutzern Knowledge Base-Artikel zur Anzeige in der **Benutzerkonsole** zur Verfügung stellen.

Damit Benutzer auf die **Benutzerkonsole** zugreifen können, müssen Sie Benutzerkonten auf der Appliance erstellen oder die LDAP-Authentifizierung aktivieren. Siehe Informationen zu Benutzerkonten und Benutzerauthentifizierung.

Verwalten von Benutzerdownloads

Sie können *Benutzerdownloads* über die **Administratorkonsole** erstellen, etikettieren und löschen.

Um die Elemente in der **Benutzerkonsole** verfügbar zu machen, müssen Sie sie im Bereich *Benutzerdownloads* der **Administratorkonsole** hochladen. Siehe Benutzerdownloads hinzufügen.

Damit Benutzer Installationsprogramme und Skripte ausführen können, muss die KACE Agent-Software auf ihren Geräten installiert sein. Siehe Informationen zur Geräteverwaltung.

Um den Benutzerzugriff auf herunterladbare Elemente zu beschränken, wählen Sie die Geräte-Label aus, für die die Elemente gelten, oder weisen Sie die Label den Elementen selbst zu. Siehe Benutzerdownloads Labels zuweisen.

Benutzerdownloads hinzufügen

Mit der **Benutzerkonsole** können Sie Software, Skripte und andere herunterladbare Dateien zur **Administratorkonsole** hinzufügen.

Alle Elemente, die Sie zur **Benutzerkonsole** hinzufügen möchten, müssen bereits in den Abschnitten *Inventar* bzw. *Skripterstellung* der Appliance existieren. Mit der **Administratorkonsole** ist keine Erstellung von Software oder Skripten möglich.

TIPP: Die Softwareverteilung ist nur für Elemente auf der Seite *Software* und für vom Agenten verwaltete Geräte verfügbar. Sie steht nicht für Elemente auf der Seite *Softwarekatalog* oder für Geräte ohne Agent zur Verfügung.

1. Rufen Sie die Seite *Detail Benutzer-Downloads* auf.
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Service Desk** und anschließend auf **Benutzerdownloads**.
   c. Wählen Sie **Aktion auswählen** > **Neu**.
2. Aktivieren Sie das Kontrollkästchen **Aktiviert**, damit das Element in der Benutzerkonsole angezeigt wird. Wenn Sie das Kontrollkästchen deaktivieren, wird das Element ausgeblendet.
3. Wählen Sie unter *Konfigurieren* einen *Typ* aus:

Option	Beschreibung
Herunterladen	Wählen Sie eine der folgenden Optionen aus: • **Katalogisierte Software**: Wählen Sie diese Option, um ein Element aus dem Softwarekatalog auszuwählen, der ein oder mehrere verknüpfte Dateien umfasst. Wählen Sie zunächst die Anwendung und dann die Datei, die zum Download verfügbar sein soll. Eine Anwendung im Softwarekatalog kann mehrere Dateien umfassen, wie Installationsprogramme für unterschiedliche Anwendungsversionen und Plattformen. **TIPP:** Wenn Sie ein katalogisiertes Softwareelement zu den Benutzer-Downloads hinzufügen, zeigen die Seiten *Benutzer-Downloads* (**Administratorkonsole**) und *Downloads* (**Benutzerkonsole**) einige zusätzliche Informationen über die Anwendung in den Spalten *Kategorie*, *Lizenztyp*, *Plattform*, *End of Life*, *Allgemeine Verfügbarkeit* und *MSRP ($)*. Mehr Informationen über katalogisierte Software finden Sie unter Informationen zum Softwarekatalog und Einzelheiten zu den Anwendungen im Softwarekatalog anzeigen. • **Software**: Damit erstellen Sie ein Element, mit dem Dokumentationen, Dateien oder andere Softwareprogramme heruntergeladen werden, für die keine automatische Installation erfolgt.
Installieren	Erstellen Sie ein Element, das ein Softwareprogramm auf dem Benutzergerät ausführt.

Option	Beschreibung
	Damit ein Gerät Installationen ausführen kann, muss auf ihm der Agent installiert werden. Wählen Sie eine der folgenden Optionen aus: • **Bestehende verwaltete Installation verwenden**: Wählen Sie diese Option, um eine bestehende verwaltete Installation (MI) auszuwählen. Jede MI umfasst eine zu installierende oder zu entfernende Kombination aus Anwendungstitel und Version – einschließlich Installationsbefehlen, Installationsdateien und Zielgeräten (nach Label). Weitere Informationen hierzu finden Sie unter Verwenden verwalteter Installationen. • **Standardinstallation**: Wählen Sie unter **Inventar** > **Software** die gewünschten Programme aus. Weitere Informationen hierzu finden Sie unter Informationen zur Seite "Software".
Skripte	Erstellen Sie ein Element, das ein Skript auf dem Benutzergerät ausführt. Wählen Sie unter **Skripterstellung** > **Skripte** die gewünschten Skripte aus. Damit ein Gerät Skripte ausführen kann, muss auf ihm die Agenten-Software installiert werden.

4. Wenn Sie im vorangehenden Schritt den Pakettyp **Installieren** ausgewählt haben, geben Sie die Parameter zum Ausführen der Installation einschließlich der erforderlichen Installationsoptionen oder -parameter ein.
5. Geben Sie die folgenden Informationen an:

Feld	Beschreibung
Produktschlüssel	Senden Sie den Produktschlüssel an Benutzer, wenn diese die Anwendung herunterladen. Klicken Sie auf **Assets**, um Lizenzinformationen zu den *Asset-Details* anzuzeigen.
Kosten pro Einheit	(Optional) Die Kosten pro Einheit.
Installationsanweisungen	Anweisungen, rechtliche Hinweise und jegliche anderen Informationen, die Sie zusammen mit der Anwendung in die **Benutzerkonsole** hochladen möchten.
Beschreibung	Geben Sie nach Bedarf beliebige weitere Informationen ein.
Lizenz des Herstellers	(Optional) Beliebiger herstellerspezifischer Text.
Richtlinie zur Unternehmenslizenzierung	(Optional) Beliebiger organisationsspezifischer Text.
Produktschlüssel per E-Mail an Benutzer senden	Senden Sie den Produktschlüssel an Benutzer, wenn diese die Anwendung herunterladen. Klicken

Feld	Beschreibung
	Sie auf **Assets**, um Lizenzinformationen zu den *Asset-Details* anzuzeigen.
Manager benachrichtigen	Benutzer müssen die E-Mail-Adresse ihres Managers eingeben, bevor sie Anwendungen herunterladen und installieren können.
Anhang	(Optional) Die Datei, die Sie als Dokumentation beifügen möchten. Die Dateigröße wird angezeigt, nachdem das Element gespeichert wurde.

6. Geben Sie im Abschnitt *Zugriffssteuerung* die Verteilungsbeschränkungen an:

Feld	Beschreibung
Labels	(Optional) Klicken Sie auf **Bearbeiten**, um ein Label auszuwählen und die Anwendungsbereitstellung auf die Benutzer zu beschränken, denen dieses Label zugewiesen wurde.
Restrict User Labels to Assigned Devices (Benutzerlabels auf zugewiesene Geräte beschränken)	(Optional) Beschränken Sie den Zugriff für Benutzer, sodass Benutzer-Downloads nur auf den ihnen zugewiesenen Geräten auslösen können.
Genehmigung erforderlich	(Optional) Aktivieren Sie dieses Kontrollkästchen, wenn der Endbenutzer eine oder mehrere Genehmigungen zum Herunterladen der Software erhalten sollen, und konfigurieren Sie die folgenden Felder: • **Genehmigungsprozessvorlage**: Wählen Sie die Prozessvorlage aus, die den gewünschten Genehmigungsprozess enthält. Die Prozessvorlage muss auf der *Softwareanforderung* basieren: Der Prozesstyp *Genehmigungspflicht*, der für Software-Download-Anfragen gilt. • **Genehmigungshäufigkeit**: Geben Sie an, wie oft der Benutzer eine Berechtigung zum Herunterladen der ausgewählten Software anfordern soll: *Einmalige Genehmigung* oder *Jede Download-Genehmigung*. **HINWEIS:** Wenn ein Endbenutzer versucht, ein Element herunterzuladen, das eine Genehmigung erfordert, erstellt das System automatisch ein Ticket unter Verwendung der konfigurierten Prozessvorlage. Genehmigende Personen werden automatisch benachrichtigt. Nach der Genehmigung erhält der Benutzer eine Benachrichtigung und kann das ausgewählte Element herunterladen.

7. Klicken Sie auf **Speichern**.

Benutzerdownloads Labels zuweisen

Sie können Labels zur Gruppierung von Benutzerdownloads verwenden. Das ist hilfreich, wenn Sie mehrere Elemente gleichzeitig verwalten und verteilen und den Zugriff auf Elemente beschränken möchten.

1. Rufen Sie die Liste *Benutzerdownloads* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Service Desk** und anschließend auf **Benutzerdownloads**.
2. Aktivieren Sie das Kontrollkästchen neben mindestens einem Element.
3. Wählen Sie **Aktion auswählen** > **Labels zuweisen**.
4. Ziehen Sie ein Label mit der Maus in das Feld *Diese Labels zuweisen* und klicken Sie dann auf **Labels zuweisen**.

Das Label ist neben dem Element in Klammern angegeben.

Labels bei Benutzerdownloads entfernen

Sie können Labels nach Bedarf von Benutzerdownloads entfernen.

1. Rufen Sie die Liste *Benutzerdownloads* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Service Desk** und anschließend auf **Benutzerdownloads**.
2. Aktivieren Sie das Kontrollkästchen neben einem Element.
3. Klicken Sie auf **Aktion auswählen** > **Labels entfernen**.
4. Klicken Sie neben dem Label, das entfernt werden soll, auf die Schaltfläche **Löschen**: .
5. Klicken Sie auf **Labels entfernen**.

Das Label wird vom Element entfernt.

Benutzerdownloads löschen

Sie können Benutzerdownloads nach Bedarf löschen.

1. Rufen Sie die Liste *Benutzerdownloads* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Service Desk** und anschließend auf **Benutzerdownloads**.
2. Aktivieren Sie das Kontrollkästchen neben mindestens einem Element.
3. Wählen Sie **Aktion auswählen** > **Löschen** und klicken Sie dann zum Bestätigen auf **Ja**.

Verwalten von Knowledge Base-Artikeln

Sie können Knowledge Base-Artikel mithilfe der **Administratorkonsole** hinzufügen, bearbeiten, duplizieren und löschen.

Benutzer können mithilfe von Schlüsselwörtern in der **Benutzerkonsole** nach Artikeln suchen und die Artikel nach Artikel-ID, Titel, Kategorie, Plattform oder Wichtigkeit sortieren. Außerdem haben Benutzer die Möglichkeit, die Nützlichkeit von Knowledge Base-Artikeln zu bewerten.

Klicken Sie auf den Link **Verwandte Artikel suchen** auf der Ticketseite, um den Knowledge Base-Artikeltext in Service-Desk-Tickets einzufügen.

Knowledge Base-Artikel hinzufügen, bearbeiten oder duplizieren

Sie können Knowledge Base-Artikel hinzufügen, bearbeiten und duplizieren. Diese Artikel stehen den Benutzern in der**Benutzerkonsole** zur Verfügung.

1. Rufen Sie die Seite *Artikeldetail* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Service Desk** und anschließend auf **Knowledge Base**.
   c. Führen Sie zum Anzeigen der Seite *Artikeldetail* einen der folgenden Schritte aus:
   - Klicken Sie auf den Namen eines Artikels.
   - Wählen Sie **Aktion auswählen** > **Neu**.
2. Geben Sie die folgenden Informationen an:

Feld	Beschreibung
Titel	Eine genaue Beschreibung des Knowledge Base-Artikelthemas. Verfassen Sie den Titel anschaulich und verwenden Sie gängige Begriffe, damit Benutzer gesuchte Informationen leicht finden.
Kategorie	Eine allgemeine Beschreibung des Themas, beispielsweise „Drucken“ oder „Netzwerkzugriff“.
Plattform	Das Betriebssystem, für das dieser Knowledge Base-Artikel gilt.
Wichtigkeit	Die relative Bedeutung des Knowledge Base-Artikels, beispielsweise „Referenz“, „niedrig“, „kritisch“ oder „hoch“.
Zu Labels zuweisen	Wenn Sie den Zugriff auf einen Artikel auf bestimmte Benutzer beschränken möchten, wählen Sie die entsprechenden Benutzerlabels aus der Liste aus. Wenn dieses Feld leer ist, können alle Benutzer mit

Feld	Beschreibung
	Zugang zur**Benutzerkonsole** den Knowledge Base-Artikel aufrufen.
Text	Der Inhalt des Knowledge Base-Artikels. Dieses Feld umfasst eine umfassende Reihe von Bearbeitungsoptionen zum Formatieren Ihrer Inhalte, wie Schaltflächen für fettgedruckten Text, Hyperlinks, Listen, Textfarbe, Einbetten von Bildern und Videos. Beispiel: • Um Fettdruck auf eine Textfolge anzuwenden, wählen Sie diese im Editor aus und klicken auf B. • Sie können Bilder zu Knowledge Base-Artikeln mit drei verschiedenen Methoden hinzufügen. Klicken Sie hierfür auf das Bild und führen Sie einen der folgenden Schritte aus: ◦ Um von Ihrem Computer zu einer Datei zu navigieren und sie in den Artikel hochzuladen, klicken Sie auf . Alle auf diese Weise hinzugefügten Bilder werden automatisch als Anhänge des KB-Artikels gespeichert. ◦ Klicken Sie auf , um eine Verknüpfung zu einer Datei herzustellen, die an anderer Stelle gehostet oder Teil eines anderen KB-Artikels ist. ◦ Um eine Verknüpfung zu einer Datei herzustellen, die bereits dem KB-Artikel zugeordnet ist, klicken Sie auf . • Um externe Links oder Links zu anderen KB-Artikeln hinzuzufügen, klicken Sie auf . • Um eine Datei anzuhängen, klicken Sie auf . Jede Datei, die mit dieser Option hochgeladen wird, wird als Anhang des KB-Artikels gespeichert. • Um ein extern gehostetes Video einzubetten, klicken Sie auf . • Wenn Sie eine Bilddatei aus dem Artikelinhalt entfernen, jedoch nicht die Dateianhänge löschen, können Sie sie später wieder zum Artikelinhalt hinzufügen. Klicken Sie dazu auf

Feld	Beschreibung
	und klicken Sie im daraufhin angezeigten Bildbereich auf . • Zum Löschen eines Dateianhangs klicken Sie auf

3. **Optional**: Klicken Sie im Abschnitt *Anhang* auf **Hinzufügen** und anschließend auf **Durchsuchen** oder **Datei auswählen**, um einen Anhang hinzuzufügen.
4. Klicken Sie auf **Speichern**.

   TIPP: Um aus Kommentaren in einem Ticket einen Knowledge Base-Artikel zu erstellen, klicken Sie auf **KB-Artikel erstellen** auf der Seite *Details zum Ticket*.

   Die Appliance weist dem Knowledge Base-Artikel eine Artikel-ID zu und zeigt ihn auf der Seite *Knowledge Base* an. Wenn Sie sehen möchten, wie der Knowledge Base-Artikel den Benutzern in der **Benutzerkonsole** angezeigt wird, klicken Sie auf der Seite *Knowledge Base* auf den Titel des Knowledge Base-Artikels und dann auf der Seite *Artikeldetail* auf die Benutzer-URL.
5. **Optional**: Klicken Sie auf **Duplizieren**.

Knowledge Base-Artikel löschen

Sie können Knowledge Base-Artikel löschen, um sie dauerhaft aus der Appliance zu entfernen.

1. Rufen Sie die Liste *Knowledge Base-Artikel* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Service Desk** und anschließend auf **Knowledge Base**.
2. Aktivieren Sie das Kontrollkästchen neben mindestens einem Artikel.
3. Wählen Sie **Aktion auswählen** > **Löschen** und klicken Sie dann zum Bestätigen auf **Ja**.

Benutzerbewertungen und Häufigkeit der Anzeige von Knowledge Base-Artikeln anzeigen

Sie können Benutzerbewertungen sowie die Häufigkeit der Anzeige von Knowledge Base-Artikeln anzeigen.

1. Rufen Sie die Seite Knowledge Base-Seite *Artikeldetail* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Service Desk** und anschließend auf **Knowledge Base**.
   c. Klicken Sie auf den Namen eines Artikels.

   Unten auf der Seite wird die aktuelle Benutzerbewertung für den Artikel und die Häufigkeit der Anzeige des Artikels angezeigt.
2. Zeigen Sie mit der Maus auf die Sterne, um die Definitionen des 5-Sterne-Bewertungssystems anzuzeigen.

   1 Stern steht für eine geringe Bewertung, 5 Sterne für eine hohe.

HINWEIS: Benutzer können ihre Bewertungen ändern. In der Datenbank wird jedoch nur die aktuellste Bewertung des Benutzers für die einzelnen Artikel gespeichert.

Anpassen von Einstellungen für Service-Desk-Tickets

Sie können die Einstellungen für Service-Desk-Tickets entsprechend den Anforderungen Ihrer Benutzer und Ihrer Umgebung anpassen. Wenn Sie mehrere Warteschlangen haben, können Sie die Ticketeinstellungen für jede Warteschlange individuell anpassen.

Informationen zum Anpassen von Einstellungen für Service-Desk-Tickets

Sie können entsprechend Ihren Service Desk-Anforderungen Ticketwerte anpassen, benutzerdefinierte Felder hinzufügen sowie Ticketkategorien und -unterkategorien erstellen.

Zu den standardmäßigen Ticketwerten zählen Kategorie, Status, Priorität und Auswirkungen.

- Folgende Ticketeigenschaften sind verfügbar:
  - Feldname
  - im Ticket angezeigte Feldreihenfolge
  - eine Angabe dazu, ob das Feld erforderlich ist
  - wer berechtigt ist, das Feld zu ändern
- Folgende benutzerdefinierte Felddefinitionen sind verfügbar:
  - Feldtyp (Kontrollkästchen, Datum, Zeitstempel, Link, Mehrfachauswahl, Hinweise, Nummer, Einfachauswahl, Text oder Benutzer)
  - zulässige Werte für das Feld
  - Standardwert für das Feld

Erstellen von Ticketkategorien und -unterkategorien

Sie können Ticketkategorien und Unterkategorien nach Bedarf erstellen. Kategorien und Unterkategorien sind warteschlangenspezifisch und stehen nach der Erstellung in der ausgewählten Warteschlange für alle neuen und vorhandenen Tickets zur Verfügung.

Sie können so viele Kategorien hinzufügen wie Sie benötigen, jede mit einer oder mehreren Unterkategorien. Zum Beispiel können Sie in der Ticketkategorie *Hardware* eine Unterkategorie wie *Monitor* anlegen. Diese Kategorien werden auf der Seite *Details zum Ticket* wie folgt angezeigt:

Wenn die Benutzer die Unterkategorie *Monitor* auswählen, können Sie zusätzliche Unterkategorien anzeigen lassen, z. B. Modellinformationen:

Die meisten Kunden verwenden für die Kategorien und Unterkategorien einen zweistufigen Ansatz. Es werden allgemeine Kategorien und Unterkategorien für die Benutzer, erstellt, wie zum Beispiel:

- Hardware – Monitor

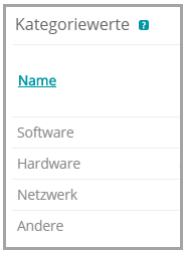
Dann werden zusätzliche Unterkategorien mit Modellinformationen für die Service Desk-Mitarbeiter erstellt, wie zum Beispiel:

- Hardware – Monitor – AceElectronics – V4500
- Hardware – Monitor – AceElectronics – V4600

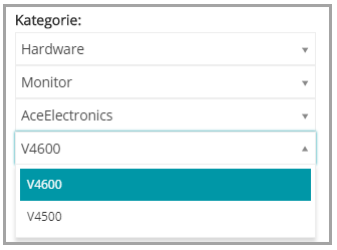
1. Rufen Sie die Seite *Warteschlangen-Detail* des Service Desks auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Service Desk** und anschließend auf **Konfiguration**.
   c. Klicken Sie im Fensterbereich **Konfiguration** auf **Warteschlangen**.
   d. Führen Sie zum Anzeigen der Seite *Warteschlangen-Detail* einen der folgenden Schritte aus:
   - Klicken Sie auf den Namen einer Warteschlange.
   - Wählen Sie **Aktion auswählen** > **Neu**.
2. Klicken Sie im Abschnitt *Standardwerte für Tickets* auf **Diese Werte anpassen**, um die Seite *Anpassung von Warteschlange* anzuzeigen.

   Auf der Seite *Anpassung von Warteschlange* wird im Bereich *Kategoriewerte* standardmäßig die Registerkarte *Strukturansicht* geöffnet, auf der Sie Ticketkategorien und Unterkategorien erstellen und verwalten können. Sie können vorhandene Kategorien und Unterkategorien bei Bedarf im Listenformular auf der Registerkarte *Listenansicht* überprüfen.
3. Erstellen und bearbeiten Sie Knoten für Ticketkategorien und Unterkategorien mit dem Struktur-Widget nach Bedarf.
   - **Um eine neue Stammkategorie hinzuzufügen, klicken Sie auf , und geben Sie den Kategorienamen an.**
   - **Um eine neue Unterkategorie hinzuzufügen, klicken Sie mit der rechten Maustaste auf den Knoten der übergeordneten Kategorie, und wählen Sie im angezeigten Menü die Option Erstellen.**

     Auf der Seite *Anpassung von Warteschlange* werden Kategorien und Unterkategorien wie folgt angezeigt:



Auf der Seite *Details zum Ticket* werden Kategorien und Unterkategorien wie folgt angezeigt:



- **Um eine Kategorie umzubenennen, klicken Sie mit der rechten Maustaste auf den Kategoriehinweis, wählen Sie im Menü die Option Umbenennen, und geben Sie den neuen Namen ein.**
- **Um eine Kategorie zu löschen, klicken Sie mit der rechten Maustaste auf die Kategoriehinweis, wählen Sie im Menü die Option Löschen, und klicken Sie im daraufhin angezeigten Dialogfeld** *Bestätigen* **auf Ja.**
- **Um alle Unterkategorien in einer Kategorie zu sortieren, klicken Sie mit der rechten Maustaste auf den Kategoriehinweis, und wählen Sie im Menü Sortieren > Aufsteigend oder Sortieren > Absteigend aus.**
- **Um alle Kategorien und ihre Unterkategorien in aufsteigender Reihenfolge zu sortieren, klicken Sie auf ⇅. Klicken Sie dann im angezeigten Dialogfeld** *Bestätigen* **auf Ja.**

  HINWEIS: Durch das Löschen einer Kategorie werden die zugehörigen Unterkategorien nicht aus der Struktur entfernt.

- **Um nach einer bestimmten Kategorie zu suchen, geben Sie den Namen der Kategorie in das Suchfeld ein. Die übereinstimmenden Ergebnisse werden während der Eingabe im Struktur-Widget hervorgehoben angezeigt.**
- **Um eine Kategorie zu verschieben, ziehen Sie den Kategorieknoten an die gewünschte Position in der Struktur.**

4. Um eine Kategorie zu bearbeiten, wählen Sie sie in der Baumstruktur aus, und geben Sie im Bereich auf der rechten Seite die folgenden Informationen ein. Wenn Sie alle Änderungen an der Kategorie vorgenommen haben, klicken Sie auf **Hinzufügen**.

Feld	Beschreibung
Standardbesitzer	Der Benutzer, der automatisch als Besitzer der Ticketkategorie oder Unterkategorie zugewiesen wird, wenn Tickets erstellt werden. Wenn Sie ein vorhandenes Ticket in eine andere Kategorie mit einem anderen Standardbesitzer verschieben, ändert sich der Besitzer des Tickets nicht automatisch. Der Besitzer des Tickets muss manuell geändert werden.
CC-Liste	Wenn Sie dieses Kontrollkästchen deaktivieren, wird die CC-Liste nicht auf Tickets angezeigt. Da **DefaultTicketOwners** der Standardbesitzer

Feld	Beschreibung
	ist, erhalten alle potenziellen Ticketbesitzer beim Erstellen eines Tickets eine E-Mail.
Vom Benutzer einstellbar	Erlaubt Benutzern das Ändern der entsprechenden Kategorie. Deaktivieren Sie das Kontrollkästchen, wenn diese Aktion Service Desk-Mitarbeitern vorbehalten bleiben soll. Ihren Benutzern werden diese Kategorien trotzdem angezeigt, auch wenn sie sie nicht ändern können.

5. Klicken Sie unten auf der Seite auf **Speichern** oder fahren Sie mit dem Bearbeiten von Ticketwerten fort.

Die neuen Kategorien und Unterkategorien werden auf der Seite *Details zum Ticket* angezeigt und stehen für neue und vorhandene Tickets zur Verfügung.

Anpassen von Ticketwerten

Sie können die verfügbaren Werte für Ticketstatus, -priorität und -auswirkungen anpassen.

Ticketstatuswerte anpassen

Sie können die Werte für den Ticketstatus (zum Beispiel Geöffnet oder Abgeschlossen) anpassen.

WICHTIG: Statuswerte werden oft in Ticketregeln verwendet. Bevor Sie die Statuswerte ändern, sollten Sie Ihre Ticketregeln überprüfen und über ein gutes Verständnis der Verwendung der Statuswerte in diesen Regeln verfügen. Siehe Informationen zu Ticketregeln.

1. Rufen Sie die Seite *Warteschlangen-Detail* des Service Desks auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Service Desk** und anschließend auf **Konfiguration**.
   c. Klicken Sie im Fensterbereich **Konfiguration** auf **Warteschlangen**.
   d. Führen Sie zum Anzeigen der Seite *Warteschlangen-Detail* einen der folgenden Schritte aus:
   - Klicken Sie auf den Namen einer Warteschlange.
   - Wählen Sie **Aktion auswählen** > **Neu**.
2. Klicken Sie im Abschnitt *Standardwerte für Tickets* auf **Diese Werte anpassen**, um die Seite *Anpassung von Warteschlange* anzuzeigen.
3. Klicken Sie im Abschnitt *Statuswerte* neben dem Wert, den Sie ändern möchten, auf die Schaltfläche **Bearbeiten**: . Oder klicken Sie zum Hinzufügen eines neuen Werts oben in der Liste auf die Schaltfläche **Hinzufügen** .
4. Bearbeiten Sie die Felder *Statuswerte*:

Feld	Beschreibung
Name	Der Name für den Statuswert.

Feld	Beschreibung
Zustand	Der dem Statuswert zugewiesene Zustand. • Geöffnet: Das Ticket ist aktiv. Nur dieser Status kann eskaliert werden. Siehe Verwenden des Prozesses zur Eskalation von Tickets. • Abgeschlossen: Das Ticket wurde aufgelöst. • Angehalten: Das Ticket ist über das Fälligkeitsdatum hinaus geöffnet, wurde jedoch nicht eskaliert.

5. Klicken Sie in der Zeile auf **Speichern**.

   Mit den Symbolen rechts neben jeder Zeile können Kategorien aktualisiert werden:

   - : Die Sortierreihenfolge der Spalten ändern.
   - : Ein Feld hinzufügen.
   - : Die Werte ändern.
   - : Die Reihenfolge der Werte ändern.
   - : Die Werte entfernen.

   HINWEIS: Sie können keine Werte löschen, die gerade verwendet werden oder als Standardticketwert festgelegt sind. Wenn Sie einen derzeit verwendeten Wert entfernen möchten, fügen Sie einen Wert hinzu und ändern anschließend in dem Ticket, in dem der Wert verwendet wird, den alten Wert in den neuen Wert. Wenn der alte Wert nicht mehr verwendet wird, wird neben dem Wert die Schaltfläche **Löschen** angezeigt: .

6. Klicken Sie unten auf der Seite auf **Speichern** oder fahren Sie mit dem Bearbeiten von Ticketwerten fort.

Ticketprioritätswerte anpassen

Sie können die Werte für die Ticketpriorität nach Bedarf anpassen.

1. Rufen Sie die Seite *Warteschlangen-Detail* des Service Desks auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Service Desk** und anschließend auf **Konfiguration**.
   c. Klicken Sie im Fensterbereich **Konfiguration** auf **Warteschlangen**.

d. Führen Sie zum Anzeigen der Seite *Warteschlangen-Detail* einen der folgenden Schritte aus:

- Klicken Sie auf den Namen einer Warteschlange.
- Wählen Sie **Aktion auswählen** > **Neu**.

2. Klicken Sie im Abschnitt *Standardwerte für Tickets* auf **Diese Werte anpassen**, um die Seite *Anpassung von Warteschlange* anzuzeigen.
3. Klicken Sie im Abschnitt *Prioritätswerte* neben dem Wert, den Sie ändern möchten, auf die Schaltfläche **Bearbeiten**: . Oder klicken Sie zum Hinzufügen eines neuen Werts oben in der Liste auf die Schaltfläche **Hinzufügen** +.
4. Bearbeiten Sie die Felder *Prioritätswerte* :

Feld	Beschreibung
Name	Geben Sie einen Namen für das benutzerdefinierte Feld ein.
Farbe	(Optional) Wählen Sie eine Farbe aus, die auf den Ticketlistenseiten für diesen Status verwendet werden soll.
Eskalationszeit	(Optional) Geben Sie ein Zeitlimit ein, nach dessen Ablauf ein offenes Ticket dieser Priorität eskaliert werden soll. Geben Sie einen ganzzahligen Zeitwert ein und wählen Sie eine Zeiteinheit aus der Dropdown-Liste aus. Siehe Verwenden des Prozesses zur Eskalation von Tickets.
Geschäftszeiten/Feiertage verwenden	(Optional) Gibt an, ob die Einstellungen für Geschäftszeiten und Feiertage bei der Berechnung der Priorität von Tickets in der Warteschlange verwendet werden sollen. Wenn Geschäftszeiten und Feiertage für den Service Desk konfiguriert sind, aktivieren Sie dieses Kontrollkästchen, um diese Geschäftszeiten und Feiertage bei der Entscheidung zu berücksichtigen, ob Tickets auf der Grundlage ihrer Priorität eskaliert werden sollen. Deaktivieren Sie das Kontrollkästchen, wenn die Einstellungen für Geschäftszeiten und Feiertage in dieser Warteschlange ignoriert werden sollen.

5. Klicken Sie in der Zeile auf **Speichern**.
6. Mit den Symbolen rechts neben jeder Zeile können zusätzliche Werte geändert werden:
   - : Die Sortierreihenfolge der Spalten ändern.
   - +: Ein Feld hinzufügen.
   - : Die Werte ändern.
   - : Die Reihenfolge der Werte ändern.
   - : Die Werte entfernen.

HINWEIS: Sie können keine Werte löschen, die gerade verwendet werden oder als Standardticketwert festgelegt sind. Wenn Sie einen derzeit verwendeten Wert entfernen möchten, fügen Sie einen Wert hinzu und ändern anschließend in dem Ticket, in dem der Wert verwendet wird, den alten Wert in den neuen Wert. Wenn der alte Wert nicht mehr verwendet wird, wird neben dem Wert die Schaltfläche **Löschen** angezeigt: .

7. Klicken Sie unten auf der Seite auf **Speichern**, um die Änderungen zu speichern und zur Seite *Warteschlangen-Detail* zurückzukehren.

Ticketauswirkungswerte anpassen

Sie können die Werte für die Ticketauswirkung nach Bedarf anpassen.

HINWEIS: Nur Ticketbesitzer können Tickets mit den Feldern *Kategoriewerte* und *Prioritätswerte* in Kategorien einstufen. Ticketabsender können diese Art von Bewertung im Feld *Auswirkungen* des Tickets vornehmen.

1. Rufen Sie die Seite *Warteschlangen-Detail* des Service Desks auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Service Desk** und anschließend auf **Konfiguration**.
   c. Klicken Sie im Fensterbereich **Konfiguration** auf **Warteschlangen**.
   d. Führen Sie zum Anzeigen der Seite *Warteschlangen-Detail* einen der folgenden Schritte aus:
   - Klicken Sie auf den Namen einer Warteschlange.
   - Wählen Sie **Aktion auswählen** > **Neu**.
2. Klicken Sie im Abschnitt *Standardwerte für Tickets* auf **Diese Werte anpassen**, um die Seite *Anpassung von Warteschlange* anzuzeigen.
3. Klicken Sie im Abschnitt *Auswirkungswerte* neben dem Wert, den Sie ändern möchten, auf die Schaltfläche **Bearbeiten**: . Oder klicken Sie zum Hinzufügen eines neuen Werts oben in der Liste auf die Schaltfläche **Hinzufügen** .
4. Ändern Sie bei Bedarf das Feld *Name*.
5. Klicken Sie in der Zeile auf **Speichern**.

   Mit den Symbolen rechts neben jeder Zeile kann die Kategorie aktualisiert werden.

   - : Die Sortierreihenfolge der Spalten ändern.
   - : Ein Feld hinzufügen.
   - : Die Werte ändern.
   - : Die Reihenfolge der Werte ändern.
   - : Die Werte entfernen.

HINWEIS: Sie können keine Werte löschen, die gerade verwendet werden oder als Standardticketwert festgelegt sind. Wenn Sie einen derzeit verwendeten Wert entfernen möchten, fügen Sie einen Wert hinzu und ändern anschließend in dem Ticket, in dem der Wert verwendet wird, den alten Wert in den neuen Wert. Wenn der alte Wert nicht mehr verwendet wird, wird neben dem Wert die Schaltfläche **Löschen** angezeigt: .

6. Klicken Sie unten auf der Seite auf **Speichern** oder fahren Sie mit dem Bearbeiten von Ticketwerten fort.

Anpassen des Ticketlayouts

Sie können anpassen, wie Tickets auf der Seite *Tickets* für jede Warteschlange angezeigt werden.

Folgende Möglichkeiten stehen Ihnen zum Anpassen des Layouts zur Auswahl:

- Reihenfolge der meisten Standardfelder ändern oder Standardfelder ausblenden.
- Benutzerdefinierte Felder hinzufügen. Die Anzahl benutzerdefinierter Felder ist nur durch die maximale Spaltenanzahl der Tabelle beschränkt. Sie können statische Werte für die Felder festlegen oder die Werte mittels Datenbankabfrage dynamisch aus einer Datenbank beziehen.
- Ticketansichten anpassen und Lese-/Schreibzugriff für Benutzer, Ticketbesitzer und Administratoren gewähren. Mit jeder dieser Rollen ist die Fähigkeit verknüpft, einzelne Ticketfelder ausblenden, anzeigen, anzeigen, aber nicht ändern oder ändern zu können.
- Schauen Sie die angepasste Ticketseite an, um sicherzustellen, dass das resultierende Layout Ihren Anforderungen entspricht.
- Beziehungen zwischen über-/untergeordneten Tickets einrichten und entweder das Abschließen des übergeordneten Elements bis zum Abschluss aller untergeordneter Tickets untersagen oder das Abschließen aller untergeordneten Tickets durch das übergeordnete Ticket zulassen. Siehe Verwendung von über- und untergeordneten Ticketbeziehungen.
- Verhindern, dass ein Ticket ohne die erforderliche Genehmigung geöffnet oder abgeschlossen wird. Sie können auch festlegen, dass nur beim Abschließen eines Tickets eine Genehmigung erforderlich ist. Siehe Verwenden von Ticketgenehmigern.

TIPP: Beachten Sie, dass die hier vorgenommenen Änderungen automatisch auf alle vorhandenen Tickets in der Warteschlange angewendet werden.

Ticket-Layoutfelder und zugehörige Ticketfelder anpassen

Sie können die Art der Anzeige der *Ticket-Layoutfelder* und *Zugehörigen Ticketfelder* auf der Seite *Details zum Ticket* anpassen.

1. Rufen Sie die Seite *Warteschlangen-Detail* des Service Desks auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Service Desk** und anschließend auf **Konfiguration**.
   c. Klicken Sie im Fensterbereich **Konfiguration** auf **Warteschlangen**.

d. Führen Sie zum Anzeigen der Seite *Warteschlangen-Detail* einen der folgenden Schritte aus:

- Klicken Sie auf den Namen einer Warteschlange.
- Wählen Sie **Aktion auswählen** > **Neu**.

2. Klicken Sie oben auf der Seite auf **Felder und Layout anpassen**, um die Seite *Anpassung von Warteschlange* mit den *Layout*- und *zugehörigen Ticketfeldern* anzuzeigen:

Abschnitt	Beschreibung
Ticket-Layoutfelder	Dieser Abschnitt umfasst die Felder *Übersicht*, *Titel* und *Zusammenfassung* die Abschnitte *Absender*, *Asset* und *Gerät* und andere Felder, die nicht im Abschnitt *Zugehörige Ticketfelder* angezeigt werden. Zudem enthält der Abschnitt alle benutzerdefinierten Felder. Die hier angezeigten Felder können beliebig innerhalb des Abschnitts verschoben werden und werden auf der Seite *Ticket* in der angegebenen Reihenfolge angezeigt. Mit Ausnahme des Felds *Auflösung*, das eine vollständige Zeile belegt, werden alle Felder in diesem Abschnitt im Format „zwei Felder pro Zeile“ angezeigt. **HINWEIS:** Wenn das Feld *Zusammenfassung* ausgeblendet ist, wird das Feld *Kommentar* auf der Seite *Neues Ticket*. Text der im Feld *Zusammenfassung* eingegeben wird, wird als erster Kommentar gespeichert und der erste Kommentar wird als Übersicht gespeichert, um Abwärtskompatibilität zu gewährleisten.
Zugehörige Ticketfelder	Dieser Abschnitt enthält Felder, in denen Informationen über zugehörige Tickets erfasst werden. Sie können diese Felder ausblenden, aber ihre Position nicht ändern. • *PARENT_INFO*: Tickets mit einer Beziehung mit einem übergeordneten Element bezüglich des ausgewählten Tickets. • *SEE_ALSO*: Tickets, die Ähnlichkeit mit dem ausgewählten Ticket haben oder zusätzliche Informationen darüber enthalten. • *REFERERS*: Benutzer, die auf das Ticket verwiesen haben.

3. Klicken Sie neben dem Feld, das angepasst werden soll, auf die Schaltfläche **Bearbeiten** .
4. Wählen Sie in den Feldern *Label* und *Erforderlich* entsprechende Optionen aus:

Abschnitt	Beschreibung
Label	Der Name, der neben dem Feld auf der Seite *Details zum Ticket* angezeigt werden soll.

Abschnitt	Beschreibung
Erforderlich	Gibt an, ob das Feld erforderlich oder optional ist. • **Nicht erforderlich**: Das Feld ist nie erforderlich. Es kann leer gelassen werden. • **Stets erforderlich**: Das Feld kann nicht leer gelassen werden. Es muss ausgefüllt werden, bevor Tickets gespeichert werden können. • **Bei Abschluss erforderlich**: Tickets können erst abgeschlossen werden, wenn das Feld ausgefüllt ist.

5. Wählen Sie im Feld *Berechtigungen* die gewünschte Berechtigungseinstellung aus:

Berechtigungseinstellung	Können angezeigt werden von	Können geändert werden von	Können erstellt werden von
Ausgeblendet	Niemandem	Niemandem	Niemandem
Schreibgeschützt	Benutzern, Ticketbesitzern, Administratoren*	Niemandem	Niemandem
Nur Besitzer - Ausgeblendet für Benutzer	Ticketbesitzern, Administratoren*	Ticketbesitzern, Administratoren*	Ticketbesitzern, Administratoren*
Nur Besitzer - für Benutzer sichtbar	Benutzern, Ticketbesitzern, Administratoren*	Ticketbesitzern, Administratoren*	Ticketbesitzern, Administratoren*
Vom Benutzer erstellbar	Benutzern, Ticketbesitzern, Administratoren*	Ticketbesitzern, Administratoren*	Benutzern, Ticketbesitzern, Administratoren*
Vom Benutzer änderbar	Benutzern, Ticketbesitzern, Administratoren*	Benutzern, Ticketbesitzern, Administratoren*	Benutzern, Ticketbesitzern, Administratoren*

* steht für die Standardeinstellung. Diese Standardeinstellung kann durch Deaktivieren des folgenden Kontrollkästchens auf der Seite *Warteschlangen-Detail* entfernt werden: *Benutzern mit Administratorrolle gestatten, Tickets in dieser Warteschlange zu lesen und zu bearbeiten (nur Administratorkonsole)*.

6. **Optional**: Verwenden Sie die folgenden Steuerelemente für die Änderung der Feldanzeige:
   - **: Die Sortierreihenfolge der Spalten ändern.**
   - **: Die Reihenfolge der Werte ändern.**
7. Klicken Sie in der Zeile auf **Speichern**.
8. Klicken Sie unten auf der Seite auf **Speichern**, um die Änderungen zu übernehmen.

Kommentar-Feldoptionen konfigurieren

Die Kommentar-Feldoptionen ermöglichen es Ihnen, das Erscheinungsbild des Kommentarfelds und den Abschnitt Anlagen auf der Seite *Neues Ticket* zu konfigurieren.

1. Rufen Sie die Seite *Warteschlangen-Detail* des Service Desks auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Service Desk** und anschließend auf **Konfiguration**.
   c. Klicken Sie im Fensterbereich **Konfiguration** auf **Warteschlangen**.
   d. Führen Sie zum Anzeigen der Seite *Warteschlangen-Detail* einen der folgenden Schritte aus:
   - Klicken Sie auf den Namen einer Warteschlange.
   - Wählen Sie **Aktion auswählen** > **Neu**.
2. Klicken Sie oben auf der Seite auf **Felder und Layout anpassen**, um die Seite *Anpassung von Warteschlange* anzuzeigen.
3. Im Abschnitt *Kommentarfeldoptionen* aktivieren oder deaktivieren Sie diese Kontrollkästchen nach Bedarf.
   - **Kommentarfeld auf Ticket-Eingabeformular anzeigen. Markieren Sie dieses Kontrollkästchen, wenn Sie möchten, dass das Feld Kommentar auf dem Ticketeingabeformular angezeigt wird.**
   - **Bereich 'Anlagen anzeigen' auf dem Ticket-Eingabeformular. Markieren Sie dieses Kontrollkästchen, wenn Sie möchten, dass der Abschnitt Anhänge auf dem Ticketeingabeformular angezeigt wird.**

   Sind diese Optionen aktiviert, werden das Feld **Kommentar** und der Bereich **Anlagen** auf der Seite *Neues Ticket* angezeigt werden, wenn neue Tickets erstellt werden. Sie werden nicht auf der Seite *Ticketdetail* angezeigt, wenn ein vorhandenes Ticket geändert wird.
4. Klicken Sie unten auf der Seite auf **Speichern**, um die Änderungen zu übernehmen.

Benutzerdefinierte Ticketfelder definieren

Sie können zu den Service-Desk-Tickets benutzerdefinierte Felder hinzufügen. Die Anzahl dieser Felder wird nur durch die Anzahl der maximal in der Tabelle möglichen Spalten beschränkt.

Das Erstellen eines benutzerdefinierten Feldes betrifft zwei Bereiche der Seite *Anpassung von Warteschlange*:

- Im Feld *Benutzerdefiniert* legen Sie die Eigenschaften für das benutzerdefinierte Feld fest.
- Im Abschnitt *Ticketlayout* legen Sie das Verhalten des benutzerdefinierten Feldes fest.

1. Rufen Sie die Seite *Warteschlangen-Detail* des Service Desks auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Service Desk** und anschließend auf **Konfiguration**.
   c. Klicken Sie im Fensterbereich **Konfiguration** auf **Warteschlangen**.

d. Führen Sie zum Anzeigen der Seite *Warteschlangen-Detail* einen der folgenden Schritte aus:

- Klicken Sie auf den Namen einer Warteschlange.
- Wählen Sie **Aktion auswählen** > **Neu**.

2. Klicken Sie oben auf der Seite auf **Felder und Layout anpassen**, um die Seite *Anpassung von Warteschlange* anzuzeigen.
3. Führen Sie im Abschnitt *Benutzerdefinierte Felder* einen der folgenden Schritte aus:

   - **Klicken Sie auf die Schaltfläche Bearbeiten, um ein Feld zu ändern: .**
   - **Klicken Sie auf die Schaltfläche Hinzufügen, um ein Feld zu erstellen: .**

   Die editierbaren Felder werden angezeigt.
4. Wählen Sie den Feldtyp aus der Dropdown-Liste *Feldtyp* aus.

   Zur Auswahl stehen folgende Optionen:

   - **Kontrollkästchen**: Fügen Sie ein Feld vom Typ "Kontrollkästchen" zum Ticket hinzu.
   - **Datum**: Fügen Sie ein Feld vom Typ "Datum" zum Ticket hinzu.
   - **Zeitstempel**: Fügen Sie ein Feld vom Typ "Zeitstempel" zum Ticket hinzu.
   - **Link**: Fügen Sie einen Link zu einer internen/externen URL zum Ticket hinzu und definieren Sie ihn.
   - **Mehrfachauswahl**: Fügen Sie ein Feld vom Typ "Mehrfachauswahl" zum Ticket hinzu. Trennen Sie die einzelnen Einträge durch Kommata.
   - **Hinweise**: Fügen Sie ein Feld vom Typ "Hinweise" zum Ticket hinzu.
   - **Nummer**: Fügen Sie ein Feld vom Typ "Ganzzahlauswahl" zum Ticket hinzu.
   - **Einfachauswahl**: Fügen Sie ein Feld vom Typ "Einfachauswahl" zum Ticket hinzu.
   - **Text**: Fügen Sie ein Feld vom Typ "Text" zum Ticket hinzu.
   - **Benutzer**: Fügen Sie eine filter- und durchsuchbare Dropdown-Liste hinzu, die Benutzer aus der Benutzertabelle enthält.

     HINWEIS: Das benutzerdefinierte Feld *Benutzer* speichert die Benutzer-ID aus der Tabelle "USER" in der Tabelle "HD_TICKET", die den Ticketdatensatz enthält. Beim Erstellen eines Berichts oder einer Abfrage der Tabelle HD_TICKET müssen Sie die Tabelle USER anfügen, wenn im Bericht anstelle der Benutzer-ID der Benutzername angezeigt werden soll.
5. Geben Sie die zulässigen Werte für das Feld *Auswahlwerte* an.

   Verwenden Sie das Feld *Auswahlwerte* für die Typen Einfachauswahl oder Mehrfachauswahl für benutzerdefinierte Felder. Trennen Sie die Zeichenfolgen mehrerer Werte durch Kommata voneinander.

   Sie können eine Datenbankabfrage verwenden, um Werte für dieses Feld anzugeben. Die Syntax hierfür lautet: `query`**:query_instructions**. Wählen Sie neben **Benutzerdefinierte Felder** die Schaltfläche *Hilfe*, um ein Beispiel anzuzeigen: .
6. Geben Sie einen Wert in das Feld *Standard* ein.

   Dieser Wert wird beim Erstellen eines Tickets standardmäßig vorgegeben.

   HINWEIS: Wenn Sie den Namen eines benutzerdefiniertes Feldes entfernen, werden die Werte für dieses Feld von allen Tickets entfernt. Wenn Sie ein benutzerdefiniertes Feld umbenennen, werden die Werte für dieses Feld beibehalten.

Sie können eine Datenbankabfrage verwenden, um Werte für dieses Feld anzugeben. Die Syntax hierfür lautet: `query:query_instructions`. Wählen Sie neben **Benutzerdefinierte Felder** die Schaltfläche *Hilfe*, um ein Beispiel anzuzeigen: ?.

7. Klicken Sie auf **Speichern**.
8. Scrollen Sie zum Abschnitt *Ticket-Layoutfelder* und klicken Sie neben dem gerade konfigurierten benutzerdefinierten Feld auf die Schaltfläche **Bearbeiten**: .

   Nun können die Optionen für das Verhalten des benutzerdefinierten Feldes editiert werden:
9. Geben Sie einen Namen in das Feld *Label* ein.
10. Wählen Sie im Feld *Erforderlich* die gewünschte Option aus:
    - **Nicht erforderlich. Das Feld ist nicht erforderlich.**
    - **Stets erforderlich. Felder mit dieser Option müssen grundsätzlich ausgefüllt werden, bevor das Ticket gespeichert und gesendet werden kann.**
    - **Bei Abschluss erforderlich. Felder mit dieser Option müssen grundsätzlich ausgefüllt werden, bevor das Ticket abgeschlossen werden kann.**
11. Wählen Sie im Feld *Berechtigungen* die gewünschte Berechtigungseinstellung aus:

Berechtigungseinstellung	Können angezeigt werden von	Können geändert werden von	Können erstellt werden von
Ausgeblendet	Niemandem	Niemandem	Niemandem
Schreibgeschützt	Benutzern, Ticketbesitzern, Administratoren*	Niemandem	Niemandem
Nur Besitzer - Ausgeblendet für Benutzer	Ticketbesitzern, Administratoren*	Ticketbesitzern, Administratoren*	Ticketbesitzern, Administratoren*
Nur Besitzer - für Benutzer sichtbar	Benutzern, Ticketbesitzern, Administratoren*	Ticketbesitzern, Administratoren*	Ticketbesitzern, Administratoren*
Vom Benutzer erstellbar	Benutzern, Ticketbesitzern, Administratoren*	Ticketbesitzern, Administratoren*	Benutzern, Ticketbesitzern, Administratoren*
Vom Benutzer änderbar	Benutzern, Ticketbesitzern, Administratoren*	Benutzern, Ticketbesitzern, Administratoren*	Benutzern, Ticketbesitzern, Administratoren*

    * steht für die Standardeinstellung. Sie können diese Standardeinstellung entfernen, indem Sie auf der Seite *Warteschlangen-Detail* das Kontrollkästchen *Benutzern mit einer Administratorrolle gestatten, Tickets in dieser Warteschlange zu lesen und zu bearbeiten (nur Administratorkonsole)* deaktivieren.
12. **Optional**: Verwenden Sie die Schaltfläche **Sortieren** oben in einer Spalte oder ziehen Sie das Verschieben-Symbol, um die Anzeigereihenfolge der Felder zu ändern.
13. Klicken Sie in der Zeile auf **Speichern**.
14. Klicken Sie unten auf der Seite auf **Speichern**, um die Änderungen zu übernehmen.

Ticketlayout anpassen

Sie können das Layout der Service Desk-Ticketliste nach Bedarf anpassen, indem Sie beispielsweise die Feldnamen, Feldreihenfolge und Spaltenbreite ändern. Dadurch legen Sie fest, wie die Ticketliste in der Warteschlange angezeigt wird.

1. Rufen Sie die Seite *Warteschlangen-Detail* des Service Desks auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Service Desk** und anschließend auf **Konfiguration**.
   c. Klicken Sie im Fensterbereich **Konfiguration** auf **Warteschlangen**.
   d. Führen Sie zum Anzeigen der Seite *Warteschlangen-Detail* einen der folgenden Schritte aus:
   - Klicken Sie auf den Namen einer Warteschlange.
   - Wählen Sie **Aktion auswählen** > **Neu**.
2. Klicken Sie oben auf der Seite auf **Felder und Layout anpassen**, um die Seite *Anpassung von Warteschlange* anzuzeigen.
3. Scrollen Sie nach unten zum Abschnitt **Ticketlayout**. Verwenden Sie folgende Schaltflächen zum Anpassen des Layouts:
   - : Die Reihenfolge ändern, in der die Felder angezeigt werden.
   - : Das anzuzeigende Feld und die zulässige Breite der Spalte bearbeiten.

     HINWEIS: Die Breite gibt an, welcher Teil der verfügbaren Seitenbreite der Feldspalte zugewiesen wird. Wenn Sie beispielsweise 10 Spalten haben und jeder Spalte die Breite 10 zugewiesen ist, wäre die Summe aller Zahlen in der Spalte *Breite* 100. Daher hätte jede Feldspalte eine Breite von 10 Prozent der verfügbaren Seitenbreite. Wenn die Summe aller Zahlen in der Spalte *Breite* mehr oder weniger als 100 beträgt, werden die Zahlen zur Bestimmung der Breite auf Prozentsätze normalisiert. Wenn Sie beispielsweise 3 Spalten haben und jeder Spalte wird eine Breite von 10 zugewiesen, beträgt die Gesamtzahl in der Spalte "Breite" 30. Durch die Normierung zu Prozentangaben beliefe sich die Breite pro Spalte auf etwa 33,3 Prozent.
   - : Ein Ticketfeld zum Ticketlayout hinzufügen.
   - : Das Feld aus der Ticketliste löschen.
4. Klicken Sie unten auf der Seite auf **Speichern**.

Ticketvorlagen verwalten

Mit Ticketvorlagen können Sie verschiedene Tickettypen innerhalb derselben Warteschlange erstellen. Mit diesem Mechanismus können Sie die Informationen, die Ihre Endbenutzer für verschiedene Anforderungsszenarien bereitstellen, besser kontrollieren, ohne verschiedene Warteschlangen erstellen zu müssen.

Jede Warteschlange kann eine oder mehrere Ticketvorlagen haben. Wenn mehrere Vorlagen in einer Warteschlange vorhanden sind, müssen Sie eine Ticketvorlage als Standardvorlage auswählen.

1. Rufen Sie die Seite *Warteschlangen-Detail* des Service Desks auf:

a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.

b. Klicken Sie in der linken Navigationsleiste auf **Service Desk** und anschließend auf **Konfiguration**.

c. Klicken Sie im Fensterbereich **Konfiguration** auf **Warteschlangen**.

d. Führen Sie zum Anzeigen der Seite *Warteschlangen-Detail* einen der folgenden Schritte aus:

- Klicken Sie auf den Namen einer Warteschlange.
- Wählen Sie **Aktion auswählen** > **Neu**.

2. Klicken Sie oben auf der Seite auf **Felder und Layout anpassen**, um die Seite *Anpassung von Warteschlange* anzuzeigen.
3. Scrollen Sie nach unten zum Abschnitt *Ticketvorlagen*.
4. Um der Warteschlange eine neue Ticketvorlage hinzuzufügen, klicken Sie im Abschnitt *Ticketvorlagen* auf +. Weitere Informationen zum Erstellen einer neuen Ticketvorlage finden Sie unter Ticketvorlage konfigurieren.
5. Um eine Ticketvorlage zur Standardvorlage für die ausgewählte Warteschlange zu machen, klicken Sie in der Zeile mit der gewünschten Vorlage in der Spalte *Ist Standard* auf **Als Standard festlegen**. Jede Warteschlange mit einer oder mehreren Ticketvorlagen benötigt eine Standardvorlage.

   Wenn eine Ticketvorlage als Standardvorlage für eine Warteschlange konfiguriert ist, wird jedes Mal, wenn Sie ein Ticket in dieser Warteschlange erstellen, ohne eine Ticketvorlage anzugeben, die Standardvorlage angewendet. Sie können bei Bedarf zwischen Vorlagen wechseln. Weitere Informationen hierzu finden Sie unter Erstellen von Tickets auf der Ticketseite der Administratorkonsole.

Ticketvorlage konfigurieren

Eine Ticketvorlage legt einen Satz von Feldern fest, die auf der Seite *Ticketdetails* angezeigt werden. Jede Warteschlange kann eine oder mehrere Ticketvorlagen haben.

Verwenden Sie die Seite *Ticketvorlagen-Details*, um eine neue oder eine vorhandene Vorlage zu konfigurieren.

1. Rufen Sie die Seite *Warteschlangen-Detail* des Service Desks auf:

   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.

   b. Klicken Sie in der linken Navigationsleiste auf **Service Desk** und anschließend auf **Konfiguration**.

   c. Klicken Sie im Fensterbereich **Konfiguration** auf **Warteschlangen**.

d. Führen Sie zum Anzeigen der Seite *Warteschlangen-Detail* einen der folgenden Schritte aus:

- Klicken Sie auf den Namen einer Warteschlange.
- Wählen Sie **Aktion auswählen** > **Neu**.

2. Klicken Sie oben auf der Seite auf **Felder und Layout anpassen**, um die Seite *Anpassung von Warteschlange* anzuzeigen.
3. Scrollen Sie nach unten zum Abschnitt *Ticketvorlagen*.
   - Um der Warteschlange eine neue Ticketvorlage hinzuzufügen, klicken Sie im Abschnitt *Ticketvorlagen* auf +.
   - Um eine vorhandene Ticketvorlage zu ändern, klicken Sie im Abschnitt *Ticketvorlagen* auf den Namen der Ticketvorlage.

   Die Seite *Ticketvorlagen-Details* wird angezeigt.
4. Geben Sie auf der Seite *Ticketvorlagen-Details* die folgenden Informationen an:

Option	Beschreibung
Name	(Erforderlich) Der Name der Vorlage.
Aktiviert	Aktivieren Sie dieses Kontrollkästchen, wenn die Vorlage einsatzbereit ist. Diese Option ist nützlich, wenn Sie verhindern möchten, dass diese Vorlage Endbenutzern zugänglich gemacht wird, bevor sie fertiggestellt ist.
Beschreibung	Eine kurze Beschreibung der Vorlage. Dieser Text wird als Tooltip im **Benutzerportal** angezeigt, wenn Sie auf den Link für diese Ticketvorlage verweisen.
Nur für Prozess	Aktivieren Sie dieses Kontrollkästchen, wenn diese Ticketvorlage für Prozessvorlagen verfügbar sein soll. Dies führt dazu, dass einige Optionen in der Ticketvorlage deaktiviert werden, da sie in diesem Kontext nicht anwendbar sind. Beispielsweise kann die Option **Vorlage auf ausgewählte Benutzer beschränken** nicht auf prozessbasierte Ticketvorlagen angewendet werden, weil jede Prozessvorlage über eine Option im Assistenten verfügt, um Labels mit Prozessvorlagen-Tickets zu verknüpfen.
Vorlage auf ausgewählte Benutzer beschränken	Aktivieren Sie dieses Kontrollkästchen, wenn diese Vorlage nur für bestimmte Benutzer mit Labels verfügbar sein soll. Klicken Sie dann auf **Verknüpfte Labels verwalten** und wählen Sie im daraufhin angezeigten Dialogfeld *Labels auswählen* eines oder mehrere Labels aus, die mit den Benutzern verknüpft sind, denen Sie Zugriff auf diese Ticketvorlage gewähren möchten. Schließen Sie anschließend das Dialogfeld.
Als Standard festlegen	Aktivieren Sie dieses Kontrollkästchen, wenn Sie diese Ticketvorlage zur Standardvorlage in der Warteschlange machen möchten. Wenn eine Ticketvorlage als Standardvorlage für eine Warteschlange konfiguriert ist, wird jedes Mal,

Option	Beschreibung
	wenn Sie ein Ticket in dieser Warteschlange erstellen, ohne eine Ticketvorlage anzugeben, die Standardvorlage angewendet. Sie können bei Bedarf zwischen Vorlagen wechseln. Weitere Informationen hierzu finden Sie unter Erstellen von Tickets auf der Ticketseite der Administratorkonsole.
Im Benutzerportal anzeigen	Aktivieren Sie dieses Kontrollkästchen, wenn Sie möchten, dass Endbenutzer einen Link zu dieser Ticketvorlage auf der Seite *Hilfe* in der **Benutzerkonsole** erhalten sollen.
Layout	Wählen Sie ein Layout aus, das sich am besten für Ihre Anforderungen eignet: • **3 Column Layout (3-Spalten-Layout)**: Verwenden Sie dieses Layout, wenn die Vorlage Felder mit durchschnittlicher Höhe in jeder Zeile enthält. • **2 Column + Right Panel Layout (2-Spalten-Layout mit Fensterbereich rechts)**: Verwenden Sie dieses Layout, wenn die Vorlage ein oder mehrere Felder enthält, die größer sind als die übrigen Felder in derselben Zeile, wie *Zusammenfassung* oder *Auflösung*. Ein großes Feld in einer Reihe, in der andere Felder von durchschnittlicher Höhe sind, führt dazu, dass die anderen Felder in derselben Reihe nach unten gerückt werden, was unerwünschte Lücken im Layout verursacht. Wenn Sie diese Option auswählen, können Sie alle hohen Felder im rechten Bereich platzieren, um den vertikalen Raum optimal zu nutzen. Doppelklicken Sie auf das Feld, um ein Feld zwischen den Bereichen zu verschieben. Sie können bei Bedarf zwischen den beiden Layouts wechseln.

5. Fügen Sie der Ticketvorlage ein oder mehrere Ticketfelder hinzu. Verwenden Sie das Trennfeld, um Ihren Inhalt in separate Abschnitte aufzuteilen. Dieses Feld enthält dieselben Optionen wie die Datenfelder.

   HINWEIS: Sie können nur Ticketfelder hinzufügen, die in der Warteschlange vorhanden sind, zu der diese Ticketvorlage gehört.

   a. Ziehen Sie im Abschnitt *Ticket-Formularvorlage* ein oder mehrere Felder aus dem Bereich auf der rechten Seite.
   b. Wenn Sie die Felder hinzufügen, können Sie sie so anordnen, wie es für die Verwendung dieser Vorlage am sinnvollsten ist. Sie können verwandte Felder zusammen anordnen oder ein Feld nahe an einem Rand des Vorlagenbereichs platzieren und so je nach Bedarf Platz dazwischen schaffen.
   c. Ein Feld kann ein-, zwei- oder dreispaltig sein. Um die Breite des Felds zu ändern, klicken Sie auf , bis die gewünschte Breite erreicht ist.
   d. Um ein Feld zu löschen, klicken Sie auf .

e. Klicken Sie auf 🔍, um die Überschreibungen der Feldeigenschaft oder bestimmte Bedingungen zu konfigurieren, die bestimmen, ob ein Feld angezeigt wird. Konfigurieren Sie dann im angezeigten Dialogfeld die folgenden Optionen nach Bedarf.

Registerkarte	Option	Beschreibung
Überschreibungen		Verwenden Sie die Optionen auf dieser Registerkarte, um Überschreibungen für Feldparameter zu konfigurieren, die bereits in der Warteschlange angegeben sind, zu der diese Ticketvorlage gehört.
	Label	Der Feldname.
	Erforderlich	Gibt an, ob der Feldwert angegeben werden muss oder nicht. Wählen Sie einen der folgenden Werte aus: • **Nicht erforderlich** • **Immer erforderlich** • **Bei Abschluss erforderlich** Weitere Informationen zu diesen Werten finden Sie unter Benutzerdefinierte Ticketfelder definieren.
	Berechtigung	Geben Sie an, welche Benutzer Zugriff auf dieses Feld haben. Wählen Sie einen der folgenden Werte aus: • **Schreibgeschützt** • **Nur Besitzer - Ausgeblendet für Benutzer** • **Nur Besitzer - für Benutzer sichtbar** • **Vom Benutzer erstellbar** • **Vom Benutzer änderbar** Weitere Informationen zu diesen Werten finden Sie unter Benutzerdefinierte Ticketfelder definieren.
	Standardwert	Konfigurieren Sie den Standardwert für das Feld. • Wenn dieses Feld vordefinierten Werten zugeordnet ist, werden diese Werte in der Liste

Registerkarte	Option	Beschreibung
		angezeigt und können ausgewählt werden. Wenn Sie beispielsweise der Ticketvorlage ein Feld *Besitzer* hinzufügen, werden in der Liste alle Benutzer angezeigt, die mit der Warteschlange verknüpft sind. • Wenn Sie ein Textfeld ausgewählt haben, können Sie je nach Bedarf einen gewünschten Wert eingeben.
Bedingte Logik		Verwenden Sie die Optionen auf dieser Registerkarte, um bestimmte Felder basierend auf den zuvor ausgewählten Werten auf der Ticketseite ein- oder auszublenden. Wenn Sie beispielsweise eine Ticketvorlage für Druckerprobleme haben, können Sie verschiedene Felder anzeigen, die für verschiedene Arten von Druckerproblemen relevant sind. Wenn der Benutzer auf dem Ticket angibt, dass dem Drucker Papier fehlt, wird auf der Seite ein Satz von Feldern angezeigt, in denen der Benutzer das Papierformat angeben kann.
	Sichtbarkeit	Geben Sie an, ob das Feld angezeigt werden soll oder nicht, wenn die angegebenen Bedingungen erfüllt sind.
	Wann	Geben Sie die Aktion für das Feld basierend auf dem Ergebnis bedingter Ausdrücke an. Wählen Sie einen der folgenden Werte aus: • **Alle Bedingungen erfüllt** • **Eine der Bedingungen erfüllt**
	Bedingung	Fügen Sie bis zu fünf Bedingungen hinzu, um das Erscheinungsbild des ausgewählten Felds festzulegen. Jede Bedingung kann bewerten, ob der Wert eines Felds, das

Registerkarte	Option	Beschreibung
		auf der Seite angezeigt wird, mit einem bestimmten Wert übereinstimmt oder nicht. Sie können nur die Felder, denen vordefinierte Werte zugeordnet sind (und die in der Regel als Listen mit Mehrfachwerten auf der Ticketseite angezeigt werden), oder Kontrollkästchen auswählen. Einfache Textfelder, z. B. *Titel*, stehen nicht zur Auswahl zur Verfügung. Sie können beispielsweise eine Bedingung erstellen, die bewertet, ob ein Druckerproblem die Bedingung *Tinte*, *Papier* oder *Andere* erfüllt und das ausgewählte Feld nach Bedarf ein- oder ausblenden.

Klicken Sie anschließend auf **Aktualisieren**.

Das Dialogfeld wird geschlossen.

6. Klicken Sie auf **Änderungen übernehmen**.

TIPP: Sie können auch eine Kopie dieser Vorlage erstellen, indem Sie auf **Duplizieren** klicken.

Als Nächstes können Sie eine Vorschau der Ticketvorlage anzeigen. Weitere Informationen hierzu finden Sie unter Ticketlayoutvorschau.

Ticketlayoutvorschau

Wenn Sie mit den Änderungen der Art und Weise fertig sind, wie Tickets auf den Seiten *Neues Ticket* und *Ticketdetail* für eine ausgewählte Ticketvorlage angezeigt werden, können Sie eine Vorschau für das Ticketseitenlayout anzeigen.

Es gibt verschiedene Vorschauoptionen, unter denen Sie wählen können. Die Art der Informationen auf der Ticketseite hängt von den dem Benutzer der auf die Seite zugreift zugeordneten Berechtigungen ab (Benutzer oder Eigentümer) sowie vom Aktionstyp (*Neues Ticket* oder *Ticketdetail*). Ein Ticketeigentümer hat meist Zugriff auf mehr Informationen als ein Benutzer, dem das Ticket zugeordnet wird. Außerdem kann die Seite *Neues Ticket* einige zusätzliche Steuerelemente für die Bereitstellung von Kommentaren oder die Verknüpfen von Dateianhängen haben, im Gegensatz zu der Seite *Ticketdetail*.

HINWEIS: Durch die Vorschau einer Ticketvorlage wird ein Ticket erstellt und gespeichert. Alle Werte, die Sie während der Vorschau eines Tickets vornehmen, werden standardmäßig gespeichert.

1. Rufen Sie die Seite *Warteschlangen-Detail* des Service Desks auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie im Fensterbereich **Konfiguration** auf **Warteschlangen**.

c. Führen Sie zum Anzeigen der Seite *Warteschlangen-Detail* einen der folgenden Schritte aus:

- Klicken Sie auf den Namen einer Warteschlange.
- Wählen Sie **Aktion auswählen** > **Neu**.

2. Klicken Sie oben auf der Seite auf **Felder und Layout anpassen**, um die Seite *Anpassung von Warteschlange* anzuzeigen.
3. Blättern Sie auf der Seite **Anpassung von Warteschlange** nach unten zum Abschnitt *Ticketvorlagen* und klicken Sie auf den Namen der Ticketvorlage, die Sie in der Vorschau anzeigen möchten.

   Die Seite *Ticketvorlagen-Details* wird angezeigt.
4. Nehmen Sie auf der Seite *Ticketvorlagen-Details* die gewünschten Anpassungen vor.

   Entsprechende Details finden Sie unter .
5. Klicken Sie unten auf der Seite auf **Speichern und Vorschau anzeigen**.

   Die Seite *Ticketdetails* wird angezeigt.
6. Klicken Sie oben auf der Seite *Ticketdetails* auf **Formularvorschau als** und wählen Sie eine der folgenden Optionen aus:

Option	Beschreibung
Eingabeformular - Benutzer	Seite *Neues Ticket* als Benutzer
Eingabeformular - Besitzer	Seite *Neues Ticket* als Ticketeigentümer
Formular bearbeiten - Benutzer	Seite *Ticketdetail* als Benutzer
Eingabeformular - Besitzer	Seite *Ticketdetail* als Ticketeigentümer

Die Seite *Neues Ticket* wird aktualisiert und zeigt die Ticketseite basierend auf der ausgewählten Ticketvorlage und den Details des Eigentümers an.

Verwendung von über- und untergeordneten Ticketbeziehungen

Sie können jedes Service Desk-Ticket als **übergeordnetes** Ticket einrichten und ihm untergeordnete Tickets zuweisen.

Es gibt zwei Möglichkeiten, Beziehungen zwischen über-/untergeordneten Tickets zu nutzen:

- **Sie können verhindern, dass übergeordnete Tickets abgeschlossen werden, bevor alle untergeordneten Tickets abgeschlossen sind**. Bei dieser Strategie wird das übergeordnete Ticket als globale Aufgabenliste genutzt und jedes untergeordnete Ticket als separate Aufgabe in der Liste betrachtet. Wenn alle Aufgaben ausgeführt und die untergeordneten Tickets abgeschlossen sind, kann auch das übergeordnete Ticket abgeschlossen werden.
- **Sie können alle untergeordneten Tickets durch Abschließen des übergeordneten Tickets abschließen.** Diese Strategie ist für Tickets hilfreich, die Duplikate desselben Problems sind (beispielsweise, wenn ein Server ausgefallen ist und viele Benutzer Tickets zu diesem Problem eingereicht haben). Wenn der Server wiederhergestellt ist, muss der Ticketbesitzer nur das übergeordnete Ticket abschließen, um damit auch alle untergeordneten Tickets abzuschließen.

Unabhängig von der gewählten Strategie können untergeordnete Tickets nicht allein stehen bleiben. Sie können das übergeordnete Ticket also erst dann abschließen, wenn auch alle untergeordneten Tickets abgeschlossen wurden.

HINWEIS: Sie können viele Ebenen von Beziehungen zwischen über-/untergeordneten Tickets erstellen, das Abschließen von untergeordneten Tickets durch Abschließen des übergeordneten Tickets funktioniert jedoch nur für eine über-/untergeordnete Ebene.

Beziehungen zwischen über-/untergeordneten Tickets für eine Warteschlange aktivieren

Über-/untergeordnete Beziehungen sind standardmäßig deaktiviert. Zum Aktivieren dieser Beziehungen konfigurieren Sie die Warteschlange zur Anzeige des Ticketfelds *PARENT_INFO*. Wenn Sie mehrere Warteschlangen haben, können Sie die Beziehungen zwischen über-/untergeordneten Tickets für jede Warteschlange individuell anpassen.

1. Rufen Sie die Seite *Warteschlangen-Detail* des Service Desks auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Service Desk** und anschließend auf **Konfiguration**.
   c. Klicken Sie im Fensterbereich **Konfiguration** auf **Warteschlangen**.
   d. Führen Sie zum Anzeigen der Seite *Warteschlangen-Detail* einen der folgenden Schritte aus:
   - Klicken Sie auf den Namen einer Warteschlange.
   - Wählen Sie **Aktion auswählen** > **Neu**.
2. Klicken Sie oben auf der Seite auf **Felder und Layout anpassen**.
3. Scrollen Sie nach unten zum Abschnitt *Zugehörige Ticket-Felder* und klicken Sie auf die Schaltfläche **Bearbeiten** für das Feld *PARENT_INFO*, um Änderungen an den Einstellungen dieses Felds vorzunehmen: .
4. Aktivieren Sie unter *Nur Benutzer – für Benutzer sichtbar* eine der Berechtigungseinstellungen.
5. Klicken Sie in der Zeile auf **Speichern**.
6. Klicken Sie unten auf der Seite auf **Speichern**.

Wenn Sie diese Änderungen speichern, können Ticketbesitzer und Administratoren (standardmäßig) ein Ticket in der Warteschlange zu einem unter- oder übergeordneten Ticket erklären.

Option zum Abschließen untergeordneter Tickets durch übergeordnete Tickets aktivieren

Sie können Warteschlangen so konfigurieren, dass übergeordnete Tickets untergeordnete Tickets abschließen können. Wenn diese Einstellung konfiguriert ist, werden untergeordnete Tickets beim Abschließen von übergeordneten Tickets automatisch abgeschlossen.

Aktivieren Sie die Beziehungen zwischen über- und untergeordneten Tickets für Warteschlangen. Siehe Beziehungen zwischen über-/untergeordneten Tickets für eine Warteschlange aktivieren.

1. Rufen Sie die Seite *Warteschlangen-Detail* des Service Desks auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Service Desk** und anschließend auf **Konfiguration**.

c. Klicken Sie im Fensterbereich **Konfiguration** auf **Warteschlangen**.

d. Führen Sie zum Anzeigen der Seite *Warteschlangen-Detail* einen der folgenden Schritte aus:

- Klicken Sie auf den Namen einer Warteschlange.
- Wählen Sie **Aktion auswählen** > **Neu**.

2. Aktivieren Sie im Abschnitt *Benutzereinstellungen* das Kontrollkästchen *Übergeordnetes Ticket darf untergeordnete Tickets schließen*.
3. Klicken Sie unten auf der Seite auf **Speichern**.

Die Änderung wird für die Warteschlange übernommen. Beim Abschließen von übergeordneten Tickets werden alle untergeordneten Tickets automatisch abgeschlossen.

Untergeordnete Tickets für ein beliebiges Ticket erstellen

Untergeordnete Tickets sind Service-Desk-Tickets, für die übergeordnete Tickets existieren. Das Erstellen von untergeordneten Tickets ist für die Organisation von Tickets und die Verwaltung zugehöriger Aufgaben nützlich. Sie können untergeordnete Tickets für beliebige Tickets in einer beliebigen Warteschlange erstellen, für die über- und untergeordnete Ticketbeziehungen aktiviert sind.

Für die Warteschlange sind über- und untergeordnete Ticketbeziehungen aktiviert. Siehe Beziehungen zwischen über-/untergeordneten Tickets für eine Warteschlange aktivieren.

1. Rufen Sie die Liste *Tickets* des Service Desks auf:

   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.

   b. Klicken Sie in der linken Navigationsleiste auf **Service Desk** und anschließend auf **Tickets**.

2. So erstellen Sie ein untergeordnetes Ticket für ein vorhandenes Ticket:

   a. Klicken Sie in der Liste *Tickets* auf einen Tickettitel.

   b. Wählen Sie auf der Seite *Ticketdetail* **Aktion auswählen** > **Speichern und untergeordnetes Element erstellen**.

   HINWEIS: Diese Option steht nur zur Verfügung, wenn Beziehungen zwischen über- und untergeordneten Tickets für die Warteschlange aktiviert sind.

   c. Geben Sie die erforderlichen Informationen für das untergeordnete Ticket an und klicken Sie dann auf **Speichern**.

3. So erstellen Sie ein untergeordnetes Ticket für ein neues Ticket:

   a. Wählen Sie in der Liste *Tickets* die Option **Aktion auswählen** > **Neu** aus.

   b. Geben Sie auf der Seite *Ticketdetail* die erforderlichen Informationen für das übergeordnete Ticket an.

   c. Wählen Sie **Aktion auswählen** > **Speichern und untergeordnetes Element erstellen** aus.

   HINWEIS: Diese Option steht nur zur Verfügung, wenn Beziehungen zwischen über- und untergeordneten Tickets für die Warteschlange aktiviert sind.

   d. Geben Sie die erforderlichen Informationen für das untergeordnete Ticket an und klicken Sie dann auf **Speichern**.

Sie können übergeordnete Tickets für die Organisation von doppelten Tickets verwenden und übergeordneten Tickets das Abschließen von untergeordneten Tickets ermöglichen. Siehe:

- Übergeordnete Tickets zum Organisieren doppelter Tickets verwenden
- Option zum Abschließen untergeordneter Tickets durch übergeordnete Tickets aktivieren

Tickets als übergeordnete Tickets festlegen und vorhandene Tickets als untergeordnete Tickets hinzufügen

Sie können Tickets als übergeordnete Tickets erklären und dann unter- und übergeordnete Beziehungen zwischen Tickets erstellen. Sie müssen zunächst übergeordnete Tickets bestimmen, bevor Sie diesen vorhandene Tickets als untergeordnete Tickets zuweisen können.

Aktivieren Sie die Beziehungen zwischen über- und untergeordneten Tickets für eine Warteschlange. Siehe Beziehungen zwischen über-/untergeordneten Tickets für eine Warteschlange aktivieren.

1. Rufen Sie die Seite *Details zum Ticket* des Service Desks auf.
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Service Desk** und anschließend auf **Tickets**.
   c. Führen Sie zum Anzeigen der Seite *Details zum Ticket* einen der folgenden Schritte aus:
   - Klicken Sie auf den Namen eines Tickets.
   - Klicken Sie auf **Aktion auswählen** > **Neues Ticket aus Warteschlange** > **Warteschlangenname**.
2. Vergewissern Sie sich im Abschnitt *Zugehörige Ticketinformationen*, dass der Abschnitt *Übergeordnetes Ticket* sichtbar ist. Falls er nicht angezeigt wird, überprüfen Sie, ob Beziehungen zwischen über-/untergeordneten Tickets für die Warteschlange aktiviert sind. Siehe Beziehungen zwischen über-/untergeordneten Tickets für eine Warteschlange aktivieren.
3. Aktivieren Sie das Kontrollkästchen *Ticket als übergeordnetes Element zulassen*, um dieses Ticket in ein übergeordnetes Ticket zu ändern.
4. Klicken Sie auf **Speichern**.
5. So fügen Sie einem vorhandenen Ticket ein untergeordnetes Ticket hinzu:
   a. Klicken Sie unter dem Abschnitt **Untergeordnete Tickets** auf **Tickets hinzufügen**.
   b. Geben Sie die Nummern der untergeordneten Tickets durch Kommas getrennt ein oder verwenden Sie die Dropdown-Liste **Ticket zum Hinzufügen auswählen**, um nach den gewünschten Tickets zu suchen.
6. Klicken Sie auf **Speichern**, um die Änderungen am Ticket zu speichern.

Übergeordnetes Ticket als Aufgabenliste verwenden

Mit der über-/untergeordneten Ticketbeziehung vom Service Desk können Sie Aufgaben gruppieren, die von verschiedenen Benutzern durchgeführt werden müssen. Ein Beispiel dafür sind die Aufgaben, die für die Einstellung eines neuen Mitarbeiters erforderlich sind. Dadurch können Sie die Tickets als eine Gruppe nachverfolgen.

- Aktivieren Sie über-/untergeordnete Beziehungen. Siehe Beziehungen zwischen über-/untergeordneten Tickets für eine Warteschlange aktivieren.
- Überprüfen Sie, ob es in der betroffenen Ticketwarteschlange gestattet ist, dass übergeordnete Tickets untergeordnete Tickets abschließen. Siehe Option zum Abschließen untergeordneter Tickets durch übergeordnete Tickets aktivieren.

TIPP: Wenn Sie annehmen, dass sich eine aus mehreren Phasen bestehende Aufgabe regelmäßig wiederholen wird, können Sie ein Prozessticket erstellen. Siehe Verwenden von Service Desk-Prozessen.

1. Erstellen Sie ein Ticket, das als übergeordnetes Ticket dienen soll. Siehe Tickets als übergeordnete Tickets festlegen und vorhandene Tickets als untergeordnete Tickets hinzufügen.
2. Fügen Sie vom übergeordneten Ticket für jede Aufgabe auf der Aufgabenliste, die dies erfordert, untergeordnete Tickets hinzu.
3. Schließen Sie jedes untergeordnete Ticket, wenn die Aufgaben abgeschlossen sind.
4. Schließen Sie das übergeordnete Ticket ab, wenn Sie dazu aufgefordert werden. Sie erhalten diese Aufforderung, sobald die letzte untergeordnete Aufgabe abgeschlossen ist.

   HINWEIS: Wenn die Lösung für das übergeordnete Ticket leer ist, wird die Lösung aus dem untergeordneten Ticket der Lösung für das übergeordnete Ticket hinzugefügt.

Übergeordnete Tickets zum Organisieren doppelter Tickets verwenden

Wurden mehrere Tickets für die gleiche Ausgabe abgelegt, können Sie mit übergeordneten Tickets doppelte Tickets als Gruppen organisieren und verwalten.

Sie aktivieren Beziehungen von über- und untergeordneten Tickets für Warteschlangen und verwenden übergeordnete Tickets, um untergeordnete Tickets abzuschließen. Siehe:

- Beziehungen zwischen über-/untergeordneten Tickets für eine Warteschlange aktivieren
- Option zum Abschließen untergeordneter Tickets durch übergeordnete Tickets aktivieren

1. Bestimmen Sie eines der doppelten Tickets als übergeordnetes Ticket. Siehe Tickets als übergeordnete Tickets festlegen und vorhandene Tickets als untergeordnete Tickets hinzufügen.
2. Ändern Sie die restlichen doppelten Tickets in untergeordnete Tickets:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie auf **Service Desk**, um die Seite *Tickets* anzuzeigen.
   c. Wählen Sie alle Tickets aus, die Sie in untergeordnete Tickets ändern möchten.
   d. Wählen Sie im Menü *Aktion auswählen* den Eintrag **Hinzufügen zu übergeordnetem Element** aus.

   HINWEIS: **Hinzufügen zu übergeordnetem Element** wird nur dann angezeigt, wenn Sie Tickets in einer einzigen Warteschlange anzeigen und für die Warteschlange über- und untergeordneten Ticketbeziehungen aktiviert sind. Dies ist nicht verfügbar, wenn Sie die Ansicht *Alle Warteschlangen* anzeigen. Siehe Beziehungen zwischen über-/untergeordneten Tickets für eine Warteschlange aktivieren.

   Die ausgewählten Tickets werden untergeordnete Tickets der übergeordneten Tickets.
3. Wenn das Problem behoben ist, schließen Sie das übergeordnete Ticket ab.

   Die untergeordneten Tickets werden automatisch abgeschlossen.

Verwenden von Ticketgenehmigern

Sie können festlegen, dass ein bestimmter Benutzer oder eine Gruppe Tickets genehmigen muss, bevor sie geöffnet oder abgeschlossen werden können. Außerdem können Sie festlegen, dass nur Benutzer, die als Genehmiger konfiguriert sind, Tickets abschließen können. Wenn Sie über mehrere Warteschlangen verfügen, können Sie die E-Mail-Einstellungen für jede Warteschlange individuell anpassen.

Das Einrichten von Ticketgenehmigern umfasst die folgenden Schritte:

- Erstellen Sie ein Label zur Angabe von Genehmigern.
- Fügen Sie dem Label Benutzer (Genehmiger) hinzu. Sie wählen Genehmiger aus der Liste aller Benutzer unabhängig von der Warteschlange aus, sodass sie nicht auf eine einzige Warteschlange beschränkt sind.
- Konfigurieren Sie das Ticketfeld *APPROVAL_INFO* in der Warteschlange so, dass diese Funktion erforderlich ist.

HINWEIS: Genehmiger haben nur Zugriff auf die Felder *Genehmigung* und *Genehmigungsvermerk* eines Tickets. Das Feld *Genehmigung* bietet die folgenden Optionen:

- Genehmigt
- Abgelehnt
- Weitere Informationen erforderlich

HINWEIS: Das Feld *Genehmigung* muss festgelegt sein, bevor das Ticket geöffnet oder abgeschlossen werden kann. Dies ist abhängig von der Konfiguration der Option *Erforderlich*. Das Feld *Genehmigungsvermerk* ist optional. Genehmiger können alle von ihnen zu genehmigenden Tickets anzeigen, indem sie auf **Service Desk** > **Tickets** klicken und dann auf den Link **Anzeigen nach** > **Eigene Genehmigungen**.

Ticketgenehmiger konfigurieren

Sie können festlegen, dass ein bestimmter Benutzer oder eine bestimmte Gruppe ein Ticket genehmigen muss, bevor es in einer Warteschlange geöffnet und abgeschlossen werden kann.

1. Rufen Sie die Liste *Benutzer* auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie auf der linken Navigationsleiste auf **Einstellungen** und anschließend auf **Benutzer**.
2. Aktivieren Sie das Kontrollkästchen neben einem Benutzer.
3. Klicken Sie im Menü *Aktion auswählen* auf **Label hinzufügen**.
4. Geben Sie im Fenster *Label hinzufügen* einen Namen für das Label ein, beispielsweise Ticketgenehmiger, und klicken Sie dann auf **Label hinzufügen**.

   TIPP: Vermeiden Sie in Labelnamen die Verwendung des umgekehrten Schrägstrichs (\). Wenn Sie einen umgekehrten Schrägstrich in einem Labelnamen verwenden müssen, fügen Sie einen zweiten umgekehrten Schrägstrich hinzu (\\), damit er nicht als Befehl interpretiert wird.
5. Klicken Sie auf **Service Desk** > **Konfiguration** > **Warteschlangen**, um die Seite *Service Desk-Warteschlangen* anzuzeigen.
6. Klicken Sie auf den Namen einer Warteschlange, um die Seite *Warteschlangen-Detail* anzuzeigen.
7. Deaktivieren Sie im Abschnitt *Benutzereinstellungen* das Kontrollkästchen *Alle Benutzer als genehmigende Person zulassen* und klicken Sie dann auf **Speichern**.
8. Klicken Sie im Abschnitt *Standardwerte für Tickets* auf **Diese Werte anpassen**, um die Seite *Anpassung von Warteschlange* anzuzeigen.
9. Klicken Sie im Abschnitt *Ticketlayout* in der Zeile *APPROVAL_INFO* auf die Schaltfläche **Bearbeiten**: .

   Die bearbeitbare Zeile *APPROVAL_INFO* wird angezeigt.
10. Geben Sie im Feld *Label* den Namen des Labels ein, das Sie in 4 für Genehmiger erstellt haben.
11. Wählen Sie im Feld *Erforderlich* die Option **Bei Abschluss erforderlich** aus.

Wenn Sie **Bei Abschluss erforderlich** oder **Stets erforderlich** auswählen, ist für alle Tickets in dieser Warteschlange eine Genehmigung erforderlich. Für ein Ticket muss ein Genehmiger angegeben werden, bevor es – je nach ausgewählter Option – bearbeitet oder abgeschlossen werden kann.

12. Klicken Sie in der Zeile auf **Speichern** und anschließend unten auf der Seite auf **Speichern**.

Die Genehmigungsfunktion ist aktiviert und die von Ihnen ausgewählten Genehmigungsoptionen werden auf die Tickets in der Warteschlange angewendet.

Tickets per E-Mail genehmigen

Wenn die Ticketgenehmigung konfiguriert ist, kann der festgelegte Ticketgenehmiger das Ticket per E-Mail genehmigen, einen Genehmigungsvermerk hinzufügen oder einen anderen Genehmiger bestimmen.

Weitere Informationen zum Ändern von Tickets per E-Mail finden Sie unter Erstellen und Verwalten von Tickets per E-Mail. Eine Liste der Felder, die zum Ändern der Genehmigungsfelder verwendet werden, finden Sie unter Ticketgenehmigungsfelder per E-Mail ändern.

Konfigurieren von SMTP-E-Mail-Servern

Sie können Ihr Service Desk für die Verwendung von SMTP-E-Mail-Servern konfigurieren.

Anweisungen zum Einrichten eines POP3-E-Mail-Servers finden Sie unter Konfigurieren der E-Mail-Einstellungen.

E-Mail-Server mit der Appliance verbinden

Sie können Ihren E-Mail-Server mit der Appliance verbinden, damit der Service Desk E-Mails von Ihrem E-Mail-Server empfangen kann. Die Vorgehensweise zum Verbinden hängt von Ihrer E-Mail-Konfiguration ab.

Falls Sie Microsoft Exchange Server verwenden, lesen Sie die Microsoft-Dokumentation zu Transportregeln.

1. Öffnen Sie den Exchange Server-Manager.
2. **Optional**: Erstellen Sie einen virtuellen SMTP-Server. Dies ist nicht erforderlich, wenn Sie über einen SMTP-Server verfügen.
3. Erstellen Sie einen virtuellen SMTP-Connector mit dem Namen appliance_HelpDesk.
4. Klicken Sie auf **Administrative Gruppen** > **Connectors** > **appliance_HelpDesk**, um die Seite *appliance_HelpDesk Eigenschaften* anzuzeigen.
5. Klicken Sie auf **Allgemein**.
6. Klicken Sie auf **DNS für Weiterleitung über Connector zu jedem Adressraum verwenden**.

   Der Abschnitt *Lokale Bridgeheads* wird verfügbar.
7. Füllen Sie die Felder unter *Lokale Bridgeheads* aus:

Server	Virtueller Server
Ihr_Exchange_Servername	Virtueller Standardserver für SMTP

8. Klicken Sie auf die Registerkarte **Adressraum**.
9. Klicken Sie auf **Hinzufügen**, um einen Adressraum für den SMTP-Server der Appliance hinzuzufügen. Verwenden Sie die folgenden Einstellungen:
   - **Typ**: SMTP
   - **Adresse**: Geben Sie den vollständigen, gültigen Servernamen der Appliance ein. Die Syntax lautet k1000.**meinedomain**.com.
   - **Kosten**: Legen Sie diese Einstellung auf eine Ebene über den anderen Connectors fest. Dadurch werden E-Mail-Nachrichten der Appliance zuerst gefiltert. Außerdem können E-Mails der Appliance nicht versehentlich das Netzwerk verlassen.
10. Klicken Sie unter *Connector-Bereich* auf **Gesamte Organisation**.
11. Lassen Sie **Relay von Nachrichten an diese Domäne zulassen** deaktiviert.
12. Klicken Sie zum Speichern auf **OK** und schließen Sie die Seite *appliance_HelpDesk Eigenschaften*.

Ihr E-Mail-Server ist nun mit der Appliance verbunden.

Verwenden eines internen und externen SMTP-Servers

Je nach Anforderungen Ihrer Umgebung können Sie für Ihren E-Mail-Verkehr den internen SMTP-Server oder einen externen SMTP-Server konfigurieren.

Die Appliance umfasst einen internen SMTP-Server. Wenn der E-Mail-Verkehr für die Appliance hauptsächlich von den Service Desk-Mitarbeitern ausgeht und an diese gerichtet ist, ist es möglicherweise sinnvoll, diesen internen Server zu verwenden. Informationen zur Einrichtung finden Sie unter Internen SMTP-Server verwenden.

Falls alle E-Mails über einen bestimmten externen SMTP-Server gesendet werden müssen, konfigurieren Sie die Appliance zur Verwendung dieses Servers. Siehe Externen SMTP-Server oder sicheren SMTP-Server verwenden.

Internen SMTP-Server verwenden

Sie können die Netzwerkeinstellungen der Appliance zur Verwendung des internen SMTP-E-Mail-Servers konfigurieren.

1. Navigieren Sie zur *Systemsteuerung* der Appliance:
   - **Wenn die Organisationskomponente nicht für die Appliance aktiviert ist, melden Sie sich bei der Administratorkonsole an: `https://appliance_hostname/admin`, und wählen Sie dann Einstellungen > Systemsteuerung aus.**
   - **Wenn die Organisationskomponente für die Appliance aktiviert ist, melden Sie sich bei der Systemverwaltungskonsole der Appliance an: `https://appliance_hostname/system`. Oder wählen Sie in der Dropdown-Liste rechts oben auf der Seite den Eintrag System aus, und klicken Sie dann auf Einstellungen > Systemsteuerung.**
2. Klicken Sie auf **Netzwerkeinstellungen**, um die Seite *Netzwerkeinstellungen* anzuzeigen.
3. Deaktivieren Sie im Abschnitt *E-Mail-Konfiguration* das Kontrollkästchen **SMTP-Server aktivieren**. Diese Einstellung bezieht sich auf einen externen SMTP-Server.
4. Klicken Sie auf **Speichern**.
5. Klicken Sie an der entsprechenden Eingabeaufforderung auf **Ja**, um die Appliance neu zu starten und die Änderungen zu übernehmen.

Der interne SMTP-Server kann nun ausgehende E-Mail-Nachrichten verarbeiten. Weitere Informationen zum Konfigurieren von SMTP-Einstellungen für Warteschlangen finden Sie unter POP3-E-Mail-Konten erstellen und konfigurieren.

Externen SMTP-Server oder sicheren SMTP-Server verwenden

Wenn Sie einen externen SMTP-Server verwenden möchten, müssen Sie in den Netzwerkeinstellungen der Appliance ein Konto für den SMTP-Server und auf dem SMTP-Server ein Konto für jede Service Desk-Warteschlange einrichten.

Zur Verwendung von sicherem SMTP (SSMTP) wählen Sie die SSL-Einstellung in jeder Warteschlange aus. Dies ist notwendig, weil Microsoft kein Aliasing von Adressen im Exchange 365-Dienst zulässt.

1. Vergewissern Sie sich, dass der externe Router und die Firewall der Appliance die Verwendung von Port 25 zum Senden von E-Mails zulassen.
2. Navigieren Sie zur *Systemsteuerung* der Appliance:
   - **Wenn die Organisationskomponente nicht für die Appliance aktiviert ist, melden Sie sich bei der Administratorkonsole an: `https://appliance_hostname/admin`, und wählen Sie dann Einstellungen > Systemsteuerung aus.**
   - **Wenn die Organisationskomponente für die Appliance aktiviert ist, melden Sie sich bei der Systemverwaltungskonsole der Appliance an: `https://appliance_hostname/system`. Oder wählen Sie in der Dropdown-Liste rechts oben auf der Seite den Eintrag System aus, und klicken Sie dann auf Einstellungen > Systemsteuerung.**
3. Klicken Sie auf **Netzwerkeinstellungen**, um die Seite *Netzwerkeinstellungen* anzuzeigen.
4. Um einen externen SMTP-Server zu verwenden, wählen Sie **SMTP-Server aktivieren** im Abschnitt *E-Mail-Konfiguration* und geben dann die SMTP-Server-Optionen an:

Option	Beschreibung
Server	Geben Sie den Hostnamen oder die IP-Adresse eines externen SMTP-Servers an, beispielsweise **smtp.gmail.com**. Externe SMTP-Server müssen die anonyme (nicht authentifizierte) Übermittlung ausgehender E-Mails unterstützen. Vergewissern Sie sich, dass es Ihre Netzwerkrichtlinien der Appliance gestatten, den SMTP-Server direkt zu kontaktieren. Der E-Mail-Server muss zudem für die Weiterleitung von E-Mails von der Appliance ohne Authentifizierung konfiguriert sein. Wenn Sie eine IP-Adresse angeben, setzen Sie sie in eckige Klammern. Beispiel: `[10.10.10.10]`.
Port	Geben Sie die für den externen SMTP-Server zu verwendende Port-Nummer ein. Für Standard-SMTP verwenden Sie Port 25. Für sicheres SMTP verwenden Sie Port 587.
Anmeldung	Geben Sie den Benutzernamen für ein Konto ein, das Zugriff auf den externen SMTP-Server hat, beispielsweise **Ihr_Kontoname**@gmail.com.

Option	Beschreibung
„Kennwort“ und „Kennwort bestätigen“	Geben Sie das Kennwort für das angegebene Serverkonto ein.

5. Testen Sie die SMTP-Konfiguration.
   a. Klicken Sie auf **Verbindungstest**.
   b. Geben Sie im nun angezeigten Dialogfeld *Verbindungstest SMTP* die E-Mail-Adresse ein, an die Sie eine Test-E-Mail mit dem neu konfigurierten SMTP-Server senden möchten, und klicken Sie dann auf **Test-E-Mail senden**.

      Das Dialogfeld *Verbindungstest SMTP* wird aktualisiert und zeigt die Testergebnisse der E-Mail-Operation an. Wenn der Test fehlschlägt, überprüfen Sie Ihre Konfiguration und probieren es erneut.
6. **Optional**: Zum Konfigurieren eines anderen SMTP- oder POP3-Servers für jede Warteschlange rufen Sie die Seite *Service Desk Warteschlange-E-Mail-Einstellungen konfigurieren* auf:
   a. Klicken Sie in der linken Navigationsleiste auf **Service Desk** und anschließend auf **Konfiguration**.
   b. Klicken Sie im Fensterbereich **Konfiguration** im Abschnitt *E-Mail-Konfiguration* auf **Service Desk Warteschlange-E-Mail-Einstellungen konfigurieren**.

   Die Seite *Service Desk Warteschlange-E-Mail-Einstellungen* wird angezeigt.
7. Falls Sie einen externen SMTP-Server für eingehende E-Mails in Verbindung mit dieser Warteschlange verwenden möchten, verwenden Sie die Einstellungen im Abschnitt *Outbound Email Setting (Einstellungen für ausgehende E-Mail)*.
   a. Aktivieren Sie das Kontrollkästchen *Warteschlangen-spezifische SMTP-Einstellungen konfigurieren*.
   b. Legen Sie die folgenden Optionen fest:

Option	Beschreibung
SMTP-Server	Geben Sie den Hostnamen oder die IP-Adresse eines externen SMTP-Servers an, beispielsweise **smtp.gmail.com**. Externe SMTP-Server müssen die anonyme (nicht authentifizierte) Übermittlung ausgehender E-Mails unterstützen. Vergewissern Sie sich, dass es Ihre Netzwerkrichtlinien der Appliance gestatten, den SMTP-Server direkt zu kontaktieren. Der E-Mail-Server muss zudem für die Weiterleitung von E-Mails von der Appliance ohne Authentifizierung konfiguriert sein.
SMTP-Port	Geben Sie die für den externen SMTP-Server zu verwendende Port-Nummer ein. Für Standard-SMTP verwenden Sie Port 25. Für sicheres SMTP verwenden Sie Port 587.
SMTP-Benutzername	Geben Sie den Benutzernamen für ein Konto ein, das Zugriff auf den externen SMTP-Server hat, beispielsweise **Ihr_Kontoname**@gmail.com.
SMTP-Kennwort	Geben Sie das Kennwort für das angegebene Serverkonto ein.

8. Klicken Sie auf **Speichern**.

Die Appliance ist nun für die Weiterleitung von E-Mails an den angegebenen SMTP-Server konfiguriert. Wenn Sie mehrere Warteschlangen haben, wiederholen Sie die vorherigen Schritte für jede Warteschlange.

TIPP: Standardmäßig akzeptiert die Appliance Service Desk-E-Mails nur, wenn die E-Mail-Adresse des Absenders einem Benutzerkonto in der Appliance entspricht. Informationen zum Ändern dieser Einstellung finden Sie in der Beschreibung der Einstellung *E-Mails von unbekannten Benutzern annehmen* im Abschnitt Konigurieren von Service Desk-Ticketwarteschlangen.

Wartung und Fehlerbehebung

Die Appliance verfügt über automatische Sicherungsfunktionen, Protokolle und Tools zur Fehlerbehebung, mit deren Hilfe Administratoren den Systemzustand überwachen und Wartungsaktivitäten durchführen können.

Warten der Appliance

Die Wartung der Appliance umfasst das Einrichten eines Sicherungszeitplans, Überprüfen des Systemzustands und Anwenden von Aktualisierungen auf Appliance-Software.

Nachverfolgen von Änderungen der Einstellungen

Wenn Verlaufsabonnements zur Aufbewahrung von Informationen konfiguriert wurden, können Sie Details zu den an Einstellungen, Assets und Objekten vorgenommenen Änderungen anzeigen.

Diese Informationen beinhalten auch das Datum der Änderung und den Benutzer, der diese vorgenommen hat. Dies kann bei der Fehlerbehebung nützlich sein. Siehe Informationen zu den Verlaufseinstellungen.

Informationen zu Appliance-Sicherungen

Appliance-Sicherungen sind Dateien, die im Falle eines Datenverlusts oder eines Ausfalls für die Wiederherstellung Ihrer Appliance verwendet werden.

Es gibt zwei Arten von Appliance-Sicherungsdateien:

- **Basis**: Eine Sicherungskopie des Dateisystems. Basissicherungsdateien werden im Allgemeinen einmal pro Woche erstellt.
- **Differenziell**: Eine Sicherungskopie der Basisdateien (Dateisystem), die seit der letzten Basissicherung geändert worden sind, und eine Sicherung der Datenbankdateien. Differenzielle Sicherungen beziehen sich auf die zuletzt erstellte, verfügbare Basissicherungsdatei.

Um Dateien wiederherzustellen, müssen Sie über ein passendes Paar von differenziellen und Basissicherungsdateien verfügen. Sicherungsdateipaare beziehen sich auf dieselbe Appliance-Versionsnummer und dasselbe Datum. Nur Sicherungsdateipaare können zur Wiederherstellung der Appliance verwendet werden.

HINWEIS: Sicherungen werden erstellt, während die Appliance ausgeführt wird. Die Appliance wird während des Sicherungsvorgangs nicht offline genommen. Für eine Wiederherstellung der Appliance mithilfe einer Sicherung und die Zurücksetzung der Appliance auf die Werkseinstellungen ist es jedoch weiterhin erforderlich, die Appliance offline zu nehmen.

Darüber hinaus gibt es drei Arten von Sicherungsvorgängen:

- **Geplante tägliche Sicherungen**: In den meisten Fällen enthalten tägliche Sicherungen ausschließlich differenzielle Sicherungsdateien. Wenn keine Basissicherung vorhanden oder die letzte Basissicherung älter als sieben Tage ist, enthält die tägliche Sicherung sowohl Basis- als auch differenzielle Sicherungsdateien. Diese Sicherung wird als vollständige Sicherung oder Full Backup bezeichnet. Tägliche Sicherungen werden standardmäßig um 02:00 Uhr durchgeführt. Sie können diesen Zeitplan

jedoch ändern. Siehe Zeitplan der täglichen Sicherung und die Anzahl der beizubehaltenden Sicherungen einrichten.

- **Geplante monatliche Sicherungen**: Monatliche Sicherungen werden am letzten Tag des Monats ausgeführt. Dieser Zeitplan kann nicht geändert werden. Diese Sicherung umfasst die neueste Basissicherung und die neuesten differenziellen Sicherungsdateien, die nach der Basissicherung gesammelt wurden.
- **Mit dem Befehl "Jetzt ausführen" initiierte Sicherungen**: Wenn Sie auf **Jetzt ausführen** auf der Seite *Sicherungseinstellungen* klicken, erstellt die Appliance eine vollständige Sicherung, die sowohl Basis- als auch differenzielle Sicherungsdateien enthält.

Sie können Sicherungen deaktivieren. Hierdurch wird eine Löschung der vorhandenen Sicherungsdaten geplant und die täglichen und monatlichen Sicherungen werden deaktiviert. Siehe Appliance-Sicherungen aktivieren oder deaktivieren.

TIPP: Sichern Sie die Appliance-Daten stets, bevor Sie Aktualisierungen installieren oder ein Upgrade der Appliance-Software durchführen.

Zeitplan der täglichen Sicherung und die Anzahl der beizubehaltenden Sicherungen einrichten

Sie können den Zeitplan der täglichen Sicherung und die Anzahl der beizubehaltenden Sicherungen konfigurieren.

1. Navigieren Sie zur *Systemsteuerung* der Appliance:
   - **Wenn die Organisationskomponente nicht für die Appliance aktiviert ist, melden Sie sich bei der Administratorkonsole an: `https://appliance_hostname/admin`, und wählen Sie dann Einstellungen > Systemsteuerung aus.**
   - **Wenn die Organisationskomponente für die Appliance aktiviert ist, melden Sie sich bei der Systemverwaltungskonsole der Appliance an: `https://appliance_hostname/system`. Oder wählen Sie in der Dropdown-Liste rechts oben auf der Seite den Eintrag System aus, und klicken Sie dann auf Einstellungen > Systemsteuerung.**
2. Klicken Sie auf **Sicherungseinstellungen**, um die Seite *Sicherungseinstellungen* anzuzeigen.
3. Geben Sie im Abschnitt *Aufbewahrung* folgende Einstellungen an:

Option	Beschreibung
Täglich	Die Anzahl der täglichen Sicherungen, die in der Appliance beibehalten werden sollen. Sie können bis zu sieben tägliche Sicherungen beibehalten.
Monatlich	Die Anzahl der monatlichen Sicherungen, die in der Appliance beibehalten werden sollen. Sie können bis zu zwei monatliche Sicherungen beibehalten. Monatliche Sicherungen werden am letzten Tag des Monats ausgeführt. Dieser Zeitplan kann nicht geändert werden.

4. Geben Sie im Abschnitt *Zeitplanung* den Zeitplan für die Ausführung **täglicher** Sicherungen an.

   Die Uhrzeiten sind im 24-Stunden-Format angegeben und Sie können Intervalle von 5 Minuten auswählen. Um beispielsweise die Zeit für die tägliche Sicherung auf 5 Minuten nach Mitternacht zu setzen, wählen Sie **0:05** aus.

   TIPP: Damit keine Sicherungsprotokolle während der täglichen Protokollwartung übergangen werden, planen Sie die Ausführung von täglichen Sicherungen nach Mitternacht.
5. Klicken Sie auf **Speichern**.

Die Einstellungen werden übernommen. Bei Ausführung der nächsten geplanten Sicherung werden ältere Sicherungsdateien gelöscht, wenn die Anzahl der Sicherungen in der Appliance größer ist als die im Abschnitt *Aufbewahrung* angegebene Anzahl.

Appliance manuell sichern

Sie können jederzeit eine manuelle Sicherung der Appliance durchführen. Außerdem sollten Sie eine manuelle Sicherung der Appliance durchführen, bevor Sie Appliance-Aktualisierungen installieren oder Upgrades durchführen.

1. Navigieren Sie zur *Systemsteuerung* der Appliance:
   - **Wenn die Organisationskomponente nicht für die Appliance aktiviert ist, melden Sie sich bei der Administratorkonsole an: `https://appliance_hostname/admin`, und wählen Sie dann Einstellungen > Systemsteuerung aus.**
   - **Wenn die Organisationskomponente für die Appliance aktiviert ist, melden Sie sich bei der Systemverwaltungskonsole der Appliance an: `https://appliance_hostname/system`. Oder wählen Sie in der Dropdown-Liste rechts oben auf der Seite den Eintrag System aus, und klicken Sie dann auf Einstellungen > Systemsteuerung.**
2. Klicken Sie auf **Sicherungseinstellungen**, um die Seite *Sicherungseinstellungen* anzuzeigen.
3. Klicken Sie unten auf der Seite auf **Jetzt ausführen** und dann zur Bestätigung auf **Ja**.

   Das System führt eine vollständige Sicherung durch, die sowohl Dateien der Basis- als auch der differenziellen Sicherung beinhaltet.

Nach dem Abschluss der Sicherung wird die Seite *Protokolle* angezeigt.

Wenn Sie eine Appliance sichern, weil Sie sie auf eine andere Appliance migrieren möchten, schalten Sie die alte Appliance aus. Wenn die alte Appliance eingeschaltet bleibt, kann es zu Konflikten kommen, wenn die gleichen Einstellungen auf die neue Appliance übertragen werden.

Administratorkonsole Sicherungsdateien herunterladen

Wenn Sie ein größeres Maß an Wiederherstellbarkeit wünschen, können Sie die Sicherungsdateien von der **Administratorkonsole** herunterladen und an einem anderen Ort speichern.

Sie können auch über FTP auf die Sicherungsdateien zugreifen. Siehe Auf Sicherungsdateien über FTP zugreifen.

HINWEIS: Um Dateien wiederherzustellen, müssen Sie über ein passendes Paar von differenziellen und Basissicherungsdateien verfügen. Sicherungsdateipaare beziehen sich auf dieselbe Appliance-Versionsnummer und dasselbe Datum. Nur Sicherungsdateipaare können zur Wiederherstellung der Appliance verwendet werden.

1. Navigieren Sie zur *Systemsteuerung* der Appliance:
   - **Wenn die Organisationskomponente nicht für die Appliance aktiviert ist, melden Sie sich bei der Administratorkonsole an: `https://appliance_hostname/admin`, und wählen Sie dann Einstellungen > Systemsteuerung aus.**
   - **Wenn die Organisationskomponente für die Appliance aktiviert ist, melden Sie sich bei der Systemverwaltungskonsole der Appliance an: `https://appliance_hostname/system`. Oder wählen Sie in der Dropdown-Liste rechts oben auf der Seite den Eintrag System aus, und klicken Sie dann auf Einstellungen > Systemsteuerung.**
2. Klicken Sie auf **Sicherungseinstellungen**, um die Seite *Sicherungseinstellungen* anzuzeigen.
3. Laden Sie im Abschnitt *Integrierte Sicherungskopien* ein Dateipaar differenzieller und Basis-Sicherungsdateien herunter:
   a. Wählen Sie das Datum aus, das dem Sicherungsdateipaar zugeordnet ist.

Die differenzielle Datei weist `incr` im Dateinamen auf und die Basisdatei `base`. Beispiel: `<date>_k1_incr_<version>.tgz` und `<date>_k1_base_<version>.tgz`.

SHA256-Prüfsummen werden ebenfalls für jede Sicherungsdatei angezeigt. Die Prüfsummen werden zum Zeitpunkt der Sicherung berechnet. Wenn die Prüfsumme einer heruntergeladenen Sicherungsdatei nicht mit der auf dieser Seite angezeigten Prüfsumme übereinstimmt, wurde die Übertragung möglicherweise unterbrochen (was zu beschädigten Daten führte), oder die Daten auf der Festplatte wurden möglicherweise manipuliert.

b. Wenn Sie dazu aufgefordert werden, wählen Sie einen Speicherort für die einzelnen Dateien aus.

HINWEIS: Die gespeicherten Sicherungsdateien spiegeln die Appliance-Daten der letzten automatischen Sicherungszeit (standardmäßig 2:00 Uhr) für ein ausgewähltes Datum wider. Wenn Sie eine Sicherung benötigen, die den aktuellen Appliance-Status widerspiegelt, können Sie eine manuelle Sicherung durchführen. Weitere Informationen hierzu finden Sie unter Appliance manuell sichern.

Auf Sicherungsdateien über FTP zugreifen

Sie können FTP verwenden, um auf Appliance-Sicherungsdateien zuzugreifen. Das ist hilfreich, wenn Sie auf einem anderen Server einen Prozess zum Zugriff auf die Sicherungsdateien erstellen möchten oder Ihre Sicherungsdateien größer als 1 GB sind und der Zugriff auf die Sicherungsdateien über die **Administratorkonsole** Timeouts des Browsers verursacht.

1. Überprüfen Sie, ob die Sicherheitseinstellungen den FTP-Zugriff auf Sicherungsdateien ermöglichen.

   Siehe Sicherheitseinstellungen für die Appliance konfigurieren.

2. Führen Sie einen der folgenden Schritte aus:

   - **Windows Gerät: Öffnen Sie eine Eingabeaufforderung und geben Sie unter `C:\` Folgendes ein: `ftp k1000`.**
   - **Greifen Sie mithilfe eines beliebigen FTP-Clients auf `ftp k1000` zu.**

3. Geben Sie die Anmeldeinformationen ein.

   Die Standard-Anmeldeinformationen sind:

   Benutzername: kbftp

   Kennwort: getbxf

   HINWEIS: Informationen zum Ändern des FTP-Kennworts finden Sie unter Sicherheitseinstellungen für die Appliance konfigurieren. Der FTP-Benutzername kann nicht geändert werden.

4. Geben Sie die folgenden Befehle ein, um aus einer Eingabeaufforderung auf die Sicherungsdateien zuzugreifen:

```
> type binary
> get k1_base.tg
> get k1_base.tgz
> get k1_incr.tgz
>close
>quit
```

Informationen zum Löschen von Appliance-Sicherungsdaten

Sie können Appliance-Sicherungsdaten löschen, indem Sie die Appliance-Sicherungen deaktivieren.

Die Deaktivierung der Sicherungen kann hilfreich sein, wenn Sie die Menge der Daten reduzieren möchten, die von der Appliance gespeichert wird. Wenn Sie z. B. über eine virtuelle Appliance verfügen und Snapshots der virtuellen Maschine verwenden, um die Appliance-Daten zu speichern, anstatt die Appliance-Sicherungsdateien

zu nutzen, können Sie die Appliance-Sicherungen deaktivieren, um die Größe der virtuellen Maschine zu reduzieren.

> **WICHTIG: Die Deaktivierung der Sicherungen verhindert die Notfallwiederherstellung von Appliance-Einstellungen und -Daten über die Administratorkonsole. Sie sollten die Appliance-Sicherungen also nur deaktivieren, wenn Sie eine alternative Methode zur Datensicherung verwenden, wie z. B. Snapshots der virtuellen Maschine für die virtuelle Appliance. Das Deaktivieren von Backups wird für physische Appliances nicht empfohlen.**

Appliance-Sicherungen aktivieren oder deaktivieren

Standardmäßig sind Appliance-Sicherungen aktiviert. Sie können Appliance-Sicherungen bei Bedarf deaktivieren und aktivieren.

Wenn Sie die Appliance-Sicherungen deaktivieren, werden vorhandene Sicherungsdateien für den nächsten geplanten Sicherungszeitpunkt zum Löschen vorgemerkt.

> **WICHTIG: Die Deaktivierung der Sicherungen verhindert die Notfallwiederherstellung von Appliance-Einstellungen und -Daten über die Administratorkonsole. Sie sollten die Appliance-Sicherungen also nur deaktivieren, wenn Sie eine alternative Methode zur Datensicherung verwenden, wie z. B. Snapshots der virtuellen Maschine für die virtuelle Appliance. Die Deaktivierung der Sicherungen wird für physische Versionen der Appliance nicht empfohlen.**

1. **Optional**: Um weiterhin über eine Notfallwiederherstellung von Daten und Einstellungen zu verfügen, laden Sie die neuesten Sicherungsdateien von der Administratorkonsole herunter und speichern sie an einen anderen Speicherort, bevor Sie die Sicherungen deaktivieren. Siehe Administratorkonsole Sicherungsdateien herunterladen.
2. Navigieren Sie zur *Systemsteuerung* der Appliance:
   - **Wenn die Organisationskomponente nicht für die Appliance aktiviert ist, melden Sie sich bei der Administratorkonsole an: `https://appliance_hostname/admin`, und wählen Sie dann Einstellungen > Systemsteuerung aus.**
   - **Wenn die Organisationskomponente für die Appliance aktiviert ist, melden Sie sich bei der Systemverwaltungskonsole der Appliance an: `https://appliance_hostname/system`. Oder wählen Sie in der Dropdown-Liste rechts oben auf der Seite den Eintrag System aus, und klicken Sie dann auf Einstellungen > Systemsteuerung.**
3. Klicken Sie auf **Sicherungseinstellungen**, um die Seite *Sicherungseinstellungen* anzuzeigen.
4. Wählen Sie im Abschnitt *Aufbewahrung* die Option **Sicherungen deaktivieren** aus.
5. Klicken Sie auf **Speichern**.

   Folgendes wird ausgeführt:
   - Alle Sicherungsoptionen werden deaktiviert.
   - Die Einstellungen für die Aufbewahrung von Sicherungskopien werden auf "1" für tägliche Backups und auf "0" für monatliche Sicherungen gesetzt.
   - Vorhandene Sicherungsdateien werden für den nächsten geplanten Sicherungszeitpunkt als von der Appliance zu löschen vorgemerkt.
6. Zum Aktivieren von Appliance-Sicherungen wählen Sie das Kontrollkästchen **Sicherungen deaktivieren** ab und klicken dann auf **Speichern**.
7. **Optional**: Klicken Sie auf **Jetzt ausführen**, um eine vollständige Sicherung des Systems vorzunehmen, die sowohl Dateien der Basis- als auch der differenziellen Sicherung beinhaltet.

Offboard-Backup-Übertragung konfigurieren

Mithilfe von Appliance-Sicherungen wird Ihre Appliance bei einem Datenverlust oder einem anderen Notfall wiederhergestellt. Wenn Sie auf ein Problem mit dem Betriebssystem der Appliance oder der Datenbank stoßen und aufgefordert werden, ein Re-Image des Geräte auszuführen, können die Backups nicht wiederhergestellt

werden, wenn Sie die Sicherungsdateien vor dem Re-Image nicht an einen sicheren Speicherort kopieren. Auf der Seite *Sicherungseinstellungen* können Sie die Übertragung von Sicherungsdaten an einen externen Speicherort automatisch konfigurieren. Wenn diese Option konfiguriert ist, kopiert das Gerät die nächtlichen Sicherungsdateien jedes Mal an einen externen Speicherort, wenn der Sicherungsprozess abgeschlossen ist.

1. Navigieren Sie zur *Systemsteuerung* der Appliance:
   - **Wenn die Organisationskomponente nicht für die Appliance aktiviert ist, melden Sie sich bei der Administratorkonsole an: `https://appliance_hostname/admin`, und wählen Sie dann Einstellungen > Systemsteuerung aus.**
   - **Wenn die Organisationskomponente für die Appliance aktiviert ist, melden Sie sich bei der Systemverwaltungskonsole der Appliance an: `https://appliance_hostname/system`. Oder wählen Sie in der Dropdown-Liste rechts oben auf der Seite den Eintrag System aus, und klicken Sie dann auf Einstellungen > Systemsteuerung.**
2. Klicken Sie auf **Sicherungseinstellungen**, um die Seite *Sicherungseinstellungen* anzuzeigen.
3. Deaktivieren Sie im Abschnitt *Offboard-Sicherungsübertragungseinstellungen* die Option **Offboard-Sicherungsübertragung deaktivieren**.
4. Klicken Sie auf **Offboard-Sicherungsübertragungsprotokoll** und wählen Sie das Protokoll aus, das Sie zum Übertragen der Sicherungsdateien verwenden möchten: **Samba**, **FTP** oder **Secure FTP**.

Option	Beschreibung
Offboard-Sicherungsübertragung deaktivieren	Gibt an, ob Offboard-Sicherungsübertragung deaktiviert oder aktiviert ist. Deaktivieren Sie dieses Kontrollkästchen, um die Offboard-Sicherungsübertragung zu aktivieren.
Offboard-Sicherungsübertragungsprotokoll	Das Protokoll, das Sie zum Übertragen der Sicherungsdateien verwenden möchten: **Samba**, **FTP**, **Secure FTP**, **Azure Blob Storage** oder **Amazon S3**. Wenn Sie Azure Blob Storage oder Amazon S3 verwenden möchten, müssen Sie ein Speicherkonto eingerichtet haben. Weitere Informationen finden Sie in der Dokumentation zu MS Azure und Amazon. **WICHTIG: Secure FTP (SFTP)-, Azure Blob Storage- und Amazon S3-Protokolle sind die Best-Practices-Empfehlungen für sichere Übertragungen mit integrierter Integritätsprüfung. FTP- und Samba-Optionen sind zwar ebenfalls verfügbar, werden jedoch aufgrund von inhärenten Schwachstellen in diesen Protokollen und unverschlüsselter Datenübertragung nicht empfohlen.**
Offboard-Sicherungsübertragungsserver	Der Hostname oder die IP-Adresse der Maschine, auf die die Sicherungsdateien kopiert werden sollen.
Pfad oder Freigabename	Der Pfad des Verzeichnisses auf dem Computer, auf den Sie die Sicherungsdateien kopieren möchten.
Benutzername	Der Name des Benutzerkontos, das Sie verwenden möchten, um auf den Zielcomputer zuzugreifen.

Option	Beschreibung
Benutzerkennwort	Das mit dem Benutzernamen verknüpfte Kennwort.

5. Um zu überprüfen, ob Sie mit der angegebenen Adresse und den Anmeldeinformationen auf den Zielcomputer zugreifen können, klicken Sie auf **Test**.

   Es wird eine Meldung angezeigt, die den Erfolg des Vorgangs bestätigt. Wenn der Zugriff auf den Zielserver fehlschlägt, wird dies in der Meldung angegeben. Überprüfen Sie die Konfiguration und nehmen Sie gegebenenfalls Änderungen vor.
6. Klicken Sie auf **Speichern**.

Wiederherstellen der Appliance

Sie können die Appliance-Daten mithilfe von Sicherungsdateien wiederherstellen, sofern Sicherungen aktiviert sind und ein passendes Paar von differenziellen und Basissicherungsdateien vorhanden ist. Darüber hinaus können Sie die Appliance zu jedem beliebigen Zeitpunkt auf die Werkseinstellungen zurücksetzen.

Durch das Wiederherstellen der Appliance werden die aktuell auf der Appliance konfigurierten Daten gelöscht. Quest KACE empfiehlt, zunächst eine externe Sicherung aller Sicherungsdateien oder Daten durchzuführen, die Sie aufbewahren möchten, bevor Sie die Appliance wiederherstellen. Darüber hinaus ist es für die Wiederherstellung der Appliance erforderlich, dass sie offline genommen wird. Die **Administratorkonsole** und die **Benutzerkonsole** sind während des Wiederherstellungsvorgangs nicht verfügbar.

HINWEIS: Um Dateien wiederherzustellen, müssen Sie über ein passendes Paar von differenziellen und Basissicherungsdateien verfügen. Sicherungsdateipaare beziehen sich auf dieselbe Appliance-Versionsnummer und dasselbe Datum. Nur Sicherungsdateipaare können zur Wiederherstellung der Appliance verwendet werden.

Appliance anhand der letzten Sicherung wiederherstellen

Die Appliance verfügt über eine integrierte Funktion, mit der Einstellungen aus der letzten Sicherung direkt vom Sicherungslaufwerk der Appliance wiederhergestellt werden können.

Die Appliance-Sicherungen sind aktiviert und ein passendes Paar von differenziellen und Basissicherungsdateien ist verfügbar. Siehe Appliance-Sicherungen aktivieren oder deaktivieren.

1. Navigieren Sie zur *Systemsteuerung* der Appliance:
   - **Wenn die Organisationskomponente nicht für die Appliance aktiviert ist, melden Sie sich bei der Administratorkonsole an: `https://appliance_hostname/admin`, und wählen Sie dann Einstellungen > Systemsteuerung aus.**
   - **Wenn die Organisationskomponente für die Appliance aktiviert ist, melden Sie sich bei der Systemverwaltungskonsole der Appliance an: `https://appliance_hostname/system`. Oder wählen Sie in der Dropdown-Liste rechts oben auf der Seite den Eintrag System aus, und klicken Sie dann auf Einstellungen > Systemsteuerung.**
2. Klicken Sie auf **Sicherungseinstellungen**, um die Seite *Sicherungseinstellungen* anzuzeigen.
3. Wählen Sie im Abschnitt *Sicherungen integrieren* die neuesten Sicherungsdateien aus.
4. Klicken Sie auf **Wiederherstellen aus Sicherung** und dann zur Bestätigung auf **Ja**.

   Die Appliance wird wiederhergestellt und neu gestartet. Die **Administratorkonsole** und die **Benutzerkonsole** sind während des Wiederherstellungsvorgangs nicht verfügbar. Der Status wird im Browserfenster angezeigt.

Sicherungsdateien in die Appliance hochladen

Wenn sich Ihre Sicherungsdateien an einem externen Speicherort befinden, können Sie diese Dateien manuell auf die Appliance per **Administratorkonsole**, FTP oder Client Drop hochladen. Das Hochladen von externen Speicherorten per FTP oder Client Drop ist nützlich, wenn Ihre Sicherungsdateien größer als 1 GB sind und der Browser beim Hochladen über die **Administratorkonsole** Timeouts meldet.

Sie haben die Sicherungsdateien an einen Speicherort außerhalb der Appliance kopiert.

> **HINWEIS:** Um Dateien wiederherzustellen, müssen Sie über ein passendes Paar von differenziellen und Basissicherungsdateien verfügen. Sicherungsdateipaare beziehen sich auf dieselbe Appliance-Versionsnummer und dasselbe Datum. Nur Sicherungsdateipaare können zur Wiederherstellung der Appliance verwendet werden.

- So laden Sie Dateien über die Administratorkonsole hoch:

  1. Navigieren Sie zur *Systemsteuerung* der Appliance:

     - Wenn die Organisationskomponente nicht für die Appliance aktiviert ist, melden Sie sich bei der Administratorkonsole an: `http://`**appliance_hostname**`/admin`. Klicken Sie dann auf **Einstellungen**.
     - Wenn die Organisationskomponente für die Appliance aktiviert ist, melden Sie sich bei der Systemadministratorkonsole an: `http://`**appliance_hostname**`/system`. Oder wählen Sie in der Dropdown-Liste rechts oben auf der Seite den Eintrag **System** aus und klicken dann auf **Einstellungen**.

  2. Klicken Sie auf **Sicherungseinstellungen**, um die Seite *Sicherungseinstellungen* anzuzeigen.
  3. Klicken Sie im Abschnitt *Hochzuladende Dateien* unter der Überschrift *Differenziell* auf **Durchsuchen** oder **Datei auswählen**, um die hochzuladende differenzielle Datei zu bestimmen.

  Dateien, die größer als 1,5 GB sind, können nur über FTP hochgeladen werden. Weitere Informationen finden Sie im nachstehenden Verfahren. Wenn Dateien über FTP hochgeladen werden, stehen Sie im Abschnitt *Wiederherstellen* zur Verfügung.

  4. Klicken Sie im Abschnitt *Hochzuladende Dateien* unter der Überschrift *Basis* auf **Durchsuchen** oder **Datei auswählen**, um die hochzuladende Basisdatei zu bestimmen.

     > **HINWEIS:** Um Dateien wiederherzustellen, müssen Sie ein passendes Dateipaar der differenziellen und Basissicherung hochladen. Sicherungsdateipaare beziehen sich auf dieselbe Appliance-Versionsnummer und dasselbe Datum. Nur Sicherungsdateipaare können zur Wiederherstellung der Appliance verwendet werden.

  5. Klicken Sie auf **Dateien hochladen**.

     Die hochgeladenen Dateien werden auf der Seite *Sicherungseinstellungen* im Abschnitt *Sicherungen* angezeigt.

- So laden Sie Ihre Sicherungsdateien per FTP auf die Appliance:

  1. Überprüfen Sie, ob die Sicherheitseinstellungen den FTP-Zugriff auf Sicherungsdateien ermöglichen.

  Siehe Sicherheitseinstellungen für die Appliance konfigurieren.

  2. Führen Sie einen der folgenden Schritte aus:

     - Windows Gerät: Öffnen Sie eine Eingabeaufforderung und geben Sie unter `C:\` Folgendes ein: `ftp k1000`.
     - Greifen Sie mithilfe eines beliebigen FTP-Clients auf `ftp k1000` zu.

  3. Geben Sie die FTP-Anmeldeinformationen ein.

  Die Standard-Anmeldeinformationen sind:

Benutzername: kbftp

Kennwort: getbxf

> **HINWEIS:** Informationen zum Ändern des FTP-Kennworts finden Sie unter Sicherheitseinstellungen für die Appliance konfigurieren. Der FTP-Benutzername kann nicht geändert werden.

Die hochgeladenen Dateien werden auf der Seite *Sicherungseinstellungen* im Abschnitt *Sicherungen* angezeigt.

- Wenn Sie Sicherungsdateien per Client Drop hochladen wollen, verschieben Sie die Sicherungsdateien an den Client-Drop-Speicherort auf der Appliance.

  Am Client-Drop-Speicherort abgelegte Dateien werden automatisch als Sicherungsdateien erkannt und innerhalb von fünf Minuten auf der Seite *Sicherungseinstellungen* für die Auswahl verfügbar. Siehe Dateien kopieren und auf dem Client-Drop-Speicherort der Appliance ablegen.

Nehmen Sie die Wiederstellung der Appliance mithilfe der hochgeladenen Sicherungsdateien vor. Siehe Appliance von Sicherungskopien wiederherstellen.

Appliance von Sicherungskopien wiederherstellen

Sie können Sie die Appliance bei Bedarf von Sicherungsdateien wiederherstellen.

Wenn Sie Dateien von einem externen Appliance-Speicherort wiederherstellen, müssen Sie ein passendes Paar von differenziellen und Basissicherungsdateien hochgeladen haben. Siehe Sicherungsdateien in die Appliance hochladen.

Wenn Sie eine Appliance auf eine neue Appliance migrieren, müssen die beiden Appliances dieselbe Version aufweisen. Wenn dies nicht der Fall ist, müssen Sie die alte Appliance auf die Version aktualisieren, die auf der neuen Appliance ausgeführt wird.

1. Navigieren Sie zur *Systemsteuerung* der Appliance:
   - **Wenn die Organisationskomponente nicht für die Appliance aktiviert ist, melden Sie sich bei der Administratorkonsole an: `https://appliance_hostname/admin`, und wählen Sie dann Einstellungen > Systemsteuerung aus.**
   - **Wenn die Organisationskomponente für die Appliance aktiviert ist, melden Sie sich bei der Systemverwaltungskonsole der Appliance an: `https://appliance_hostname/system`. Oder wählen Sie in der Dropdown-Liste rechts oben auf der Seite den Eintrag System aus, und klicken Sie dann auf Einstellungen > Systemsteuerung.**
2. Klicken Sie auf **Sicherungseinstellungen**, um die Seite *Sicherungseinstellungen* anzuzeigen.
3. Wählen Sie im Abschnitt *Sicherungen integrieren* das Dateienpaar aus, das Sie wiederherstellen möchten.
4. Wenn Sie die Netzwerkkonfiguration aus den Sicherungsdateien ignorieren und unter *Wiederherstellungsoptionen* eine neue Konfiguration angeben möchten, wählen Sie **Override Network Configuration (Netzwerkkonfiguration überschreiben)**, und geben Sie die entsprechenden Optionen an.

   Wenn Sie dieses Kontrollkästchen aktivieren, wird auf dieser Seite eine Reihe von Optionen angezeigt. Sie sind identisch mit den Netzwerkeinstellungen der Appliance, die Sie während einer Erstkonfiguration einrichten müssen. Weitere Informationen hierzu finden Sie unter Netzwerkeinstellungen der Appliance ändern.
5. Klicken Sie auf **Wiederherstellen aus Sicherung** und dann zur Bestätigung auf **Ja**.

   Die Appliance wird wiederhergestellt und neu gestartet. Die **Administratorkonsole** und die **Benutzerkonsole** sind während des Wiederherstellungsvorgangs nicht verfügbar. Der Status wird im Browserfenster angezeigt.

   Dieser Vorgang kann bis zu eine Stunde dauern und die Appliance ist während dieser Zeit nicht verfügbar. Die Zeit für eine Wiederherstellung hängt von der Größe der Sicherungsdateien ab. Sobald die Wiederherstellung abgeschlossen ist, wird die Appliance neu gestartet. Nach dem Neustart

befindet sich die Appliance im gleichen Zustand wie die Sicherungsdateien. Dazu gehören die gleichen Authentifizierungseinstellungen, Netzwerkeinstellungen usw.

Wenn die IP-Einstellungen beim Neustart nicht gesetzt werden, versuchen Sie noch ein- oder zweimal einen Neustart, um die IP-Einstellungen richtig festzulegen. Wenn Sie nicht mit dieser Methode festgelegt werden, verwenden Sie das Konsolenanmelde-Dienstprogramm `netdiag/netdiag` und aktualisieren Sie die IP-Adresse.

Die Appliance wird wiederhergestellt und neu gestartet.

Werkseinstellungen der Appliance wiederherstellen

Die Appliance verfügt über eine integrierte Funktion zur Wiederherstellung der Werkseinstellungen. Dies ist hilfreich, wenn Probleme auftreten und Sie alle benutzerdefinierten Konfigurationen entfernen müssen.

1. Navigieren Sie zur *Systemsteuerung* der Appliance:
   - **Wenn die Organisationskomponente nicht für die Appliance aktiviert ist, melden Sie sich bei der Administratorkonsole an: `https://appliance_hostname/admin`, und wählen Sie dann Einstellungen > Systemsteuerung aus.**
   - **Wenn die Organisationskomponente für die Appliance aktiviert ist, melden Sie sich bei der Systemverwaltungskonsole der Appliance an: `https://appliance_hostname/system`. Oder wählen Sie in der Dropdown-Liste rechts oben auf der Seite den Eintrag System aus, und klicken Sie dann auf Einstellungen > Systemsteuerung.**
2. Klicken Sie auf **Sicherungseinstellungen**, um die Seite *Sicherungseinstellungen* anzuzeigen.
3. Am Ende der Seite und klicken Sie auf **Auf Werkseinstellungen zurücksetzen** und anschließend zur Bestätigung auf **Ja**.

   Die Appliance wird wiederhergestellt und neu gestartet.
4. Konfigurieren Sie die Appliance nach Bedarf neu.

   Siehe Konfigurieren der Appliance.

Aktualisieren der Appliance-Software

Sie können nach Softwareaktualisierungen für die Appliance suchen und diese installieren. Wenn Sie die Appliance aktualisieren, werden benutzerdefinierte Konfigurationen wie Anpassungen am Service Desk und Assets erhalten.

Auf beworbene Appliance-Aktualisierungen prüfen und diese anwenden

Die Appliance meldet sich täglich bei den Servern von Quest an, um zu überprüfen, ob Aktualisierungen der Appliance-Software verfügbar sind. Diese Aktualisierungen werden als beworbene Aktualisierungen bezeichnet.

Wenn Aktualisierungen verfügbar sind, wird eine Benachrichtigung auf der *Startseite* angezeigt, sobald Sie sich das nächste Mal mit einem Konto mit Administratorrechten anmelden.

TIPP: Sichern Sie die Appliance-Daten stets, bevor Sie Aktualisierungen installieren oder ein Upgrade der Appliance-Software durchführen. Anleitungen dazu finden Sie unter Informationen zu Appliance-Sicherungen.

1. Navigieren Sie zur *Systemsteuerung* der Appliance:
   - **Wenn die Organisationskomponente nicht für die Appliance aktiviert ist, melden Sie sich bei der Administratorkonsole an: `https://appliance_hostname/admin`, und wählen Sie dann Einstellungen > Systemsteuerung aus.**
   - **Wenn die Organisationskomponente für die Appliance aktiviert ist, melden Sie sich bei der Systemverwaltungskonsole der Appliance an: `https://appliance_hostname/system`. Oder wählen Sie in der Dropdown-Liste rechts oben auf der Seite den Eintrag System aus, und klicken Sie dann auf Einstellungen > Systemsteuerung.**
2. Klicken Sie auf der linken Navigationsleiste auf **Appliance-Aktualisierungen**, um die Seite *Appliance-Aktualisierungen* anzuzeigen.
3. Klicken Sie im Abschnitt *Server* auf **Auf Aktualisierungen prüfen**, um die Seite *Protokolle* anzuzeigen.

   Die Ergebnisse der Überprüfung werden im Protokoll angezeigt.
4. Wenn eine Aktualisierung verfügbar ist, sichern Sie Ihre Datenbank und Ihre Dateien.

   Siehe Informationen zu Appliance-Sicherungen.
5. Klicken Sie auf **Aktualisieren**.

Die Aktualisierung wurde angewendet. Die **Administratorkonsole** ist nicht verfügbar, bis die Aktualisierung abgeschlossen ist. Der Bearbeitungsstatus wird im Browserfenster und in der **Administratorkonsole** angezeigt.

Aktualisierungsdatei manuell in die Appliance hochladen

Wenn Sie eine Aktualisierungsdatei von Quest erhalten haben, können Sie diese manuell in die Appliance hochladen.

Stellen Sie vor der manuellen Aktualisierung der Appliance sicher, dass Ihre Appliance die Anforderungen an die Mindest-Serverversion erfüllt. Diese finden Sie in den Versionsinformationen der Aktualisierung. Wenn Ihre Appliance diese Anforderungen nicht erfüllt, müssen Sie ein Upgrade auf die mindestens erforderliche Version durchführen, bevor Sie die Appliance-Software aktualisieren können. Siehe Version, Modell und Lizenzinformationen der Appliance anzeigen.

1. Sichern Sie Ihre Datenbank und die entsprechenden Dateien. Siehe Informationen zu Appliance-Sicherungen.
2. Laden Sie die Datei `k1000_upgrade_server_`**`XXXX`**`.kbin` herunter und speichern Sie sie lokal.
3. Navigieren Sie zur *Systemsteuerung* der Appliance:
   - **Wenn die Organisationskomponente nicht für die Appliance aktiviert ist, melden Sie sich bei der Administratorkonsole an: `https://appliance_hostname/admin`, und wählen Sie dann Einstellungen > Systemsteuerung aus.**
   - **Wenn die Organisationskomponente für die Appliance aktiviert ist, melden Sie sich bei der Systemverwaltungskonsole der Appliance an: `https://appliance_hostname/system`. Oder wählen Sie in der Dropdown-Liste rechts oben auf der Seite den Eintrag System aus, und klicken Sie dann auf Einstellungen > Systemsteuerung.**
4. Klicken Sie auf der linken Navigationsleiste auf **Appliance-Aktualisierungen**, um die Seite *Appliance-Aktualisierungen* anzuzeigen.
5. Im Abschnitt *Manuell aktualisieren*:
   a. Klicken Sie auf **Durchsuchen** oder auf **Datei auswählen** und suchen Sie nach der Aktualisierungsdatei.
   b. Klicken Sie auf **Aktualisieren** und zur Bestätigung auf **Ja**.

Die Aktualisierung wurde angewendet. Die **Administratorkonsole** ist nicht verfügbar, bis die Aktualisierung abgeschlossen ist. Der Bearbeitungsstatus wird im Browserfenster und in der **Administratorkonsole** angezeigt.

Aktualisierungen überprüfen

Nach der Aktualisierung können Sie im Aktualisierungsprotokoll überprüfen, ob die Aktualisierung erfolgreich abgeschlossen wurde.

1. Navigieren Sie zur *Systemsteuerung* der Appliance:
   - **Wenn die Organisationskomponente nicht für die Appliance aktiviert ist, melden Sie sich bei der Administratorkonsole an: `https://appliance_hostname/admin`, und wählen Sie dann Einstellungen > Systemsteuerung aus.**
   - **Wenn die Organisationskomponente für die Appliance aktiviert ist, melden Sie sich bei der Systemverwaltungskonsole der Appliance an: `https://appliance_hostname/system`. Oder wählen Sie in der Dropdown-Liste rechts oben auf der Seite den Eintrag System aus, und klicken Sie dann auf Einstellungen > Systemsteuerung.**
2. Klicken Sie auf **Protokolle**, um die Seite *Protokolle* anzuzeigen.
3. Wählen Sie in der Dropdown-Liste *Protokoll* die Option **Aktualisierungen** aus.
4. Überprüfen Sie das Protokoll auf Fehlermeldungen und Warnungen.
5. Klicken Sie oben rechts auf **Benötigen Sie Hilfe?** und dann unten im Bereich *Hilfe* auf **Info**, um die aktuelle Version zu überprüfen. Siehe Version, Modell und Lizenzinformationen der Appliance anzeigen.

Lizenzschlüssel der Appliance aktualisieren

Sie müssen möglicherweise den Lizenzschlüssel für die Appliance aktualisieren, wenn Sie Ihre Lizenzfunktionen erweitern oder zusätzliche Komponenten wie die Organisationskomponente erwerben möchten.

1. Navigieren Sie zur *Systemsteuerung* der Appliance:
   - **Wenn die Organisationskomponente nicht für die Appliance aktiviert ist, melden Sie sich bei der Administratorkonsole an: `https://appliance_hostname/admin`, und wählen Sie dann Einstellungen > Systemsteuerung aus.**
   - **Wenn die Organisationskomponente für die Appliance aktiviert ist, melden Sie sich bei der Systemverwaltungskonsole der Appliance an: `https://appliance_hostname/system`. Oder wählen Sie in der Dropdown-Liste rechts oben auf der Seite den Eintrag System aus, und klicken Sie dann auf Einstellungen > Systemsteuerung.**
2. Klicken Sie auf der linken Navigationsleiste auf **Appliance-Aktualisierungen**, um die Seite *Appliance-Aktualisierungen* anzuzeigen.
3. Geben Sie im Abschnitt *Lizenzinformationen* Ihren Lizenzschlüssel ein.
4. Klicken Sie auf **Aktualisieren**.

Appliance neu starten oder herunterfahren

Sie müssen die Appliance möglicherweise im Rahmen der Fehlerbehebung oder bei der Ausführung von Wartungsaufgaben von Zeit zu Zeit neu starten oder herunterfahren.

Außerdem müssen Sie die Appliance herunterfahren, bevor Sie sie vom Netz trennen.

TIPP: Um die physische Appliance sofort herunterzufahren, drücken Sie einmal schnell den Netzschalter.

1. Navigieren Sie zur *Systemsteuerung* der Appliance:
   - **Wenn die Organisationskomponente nicht für die Appliance aktiviert ist, melden Sie sich bei der Administratorkonsole an: `https://appliance_hostname/admin`, und wählen Sie dann Einstellungen > Systemsteuerung aus.**
   - **Wenn die Organisationskomponente für die Appliance aktiviert ist, melden Sie sich bei der Systemverwaltungskonsole der Appliance an: `https://appliance_hostname/system`. Oder wählen Sie in der Dropdown-Liste rechts oben auf der Seite den Eintrag System aus, und klicken Sie dann auf Einstellungen > Systemsteuerung.**
2. Klicken Sie auf der linken Navigationsleiste auf **Appliance-Aktualisierungen**, um die Seite *Appliance-Aktualisierungen* anzuzeigen.
3. Führen Sie im Abschnitt *Appliance-Bedienelemente* einen der folgenden Schritte aus:
   - **Klicken Sie auf Neustart. Die Appliance wird neu gestartet.**
   - **Klicken Sie auf Datenbank neu starten und prüfen. Die Appliance wird neu gestartet und die Datenbank wird überprüft.**
   - **Klicken Sie auf Herunterfahren. Die Appliance wird heruntergefahren und Sie können die Hardware der Appliance sicher ausschalten.**

OVAL-Definitionen über KACE aktualisieren

Die Definitionen für OVAL-Tests (Open Vulnerability Assessment Language, Offener Mitre-Standard für Sicherheitslücken) werden zwar regelmäßig automatisch aktualisiert, Sie können jedoch die neuesten Dateien auch manuell über die Seite *Appliance-Aktualisierungen* abrufen.

Weitere Informationen zu OVAL-Definitionen finden Sie unter Aufrechterhalten der Geräte- und Appliance-Sicherheit.

1. Navigieren Sie zur *Systemsteuerung* der Appliance:
   - **Wenn die Organisationskomponente nicht für die Appliance aktiviert ist, melden Sie sich bei der Administratorkonsole an: `https://appliance_hostname/admin`, und wählen Sie dann Einstellungen > Systemsteuerung aus.**
   - **Wenn die Organisationskomponente für die Appliance aktiviert ist, melden Sie sich bei der Systemverwaltungskonsole der Appliance an: `https://appliance_hostname/system`. Oder wählen Sie in der Dropdown-Liste rechts oben auf der Seite den Eintrag System aus, und klicken Sie dann auf Einstellungen > Systemsteuerung.**
2. Klicken Sie auf der linken Navigationsleiste auf **Appliance-Aktualisierungen**, um die Seite *Appliance-Aktualisierungen* anzuzeigen.
3. Klicken Sie im Abschnitt *OVAL-Katalog* auf **Auf Aktualisierungen prüfen** und anschließend auf **Ja**.

Informationen zu "Daily Run Output"

Daily Run Output (Täglicher Systembericht) der Appliance ist ein Bericht, der Informationen zum Status der Appliance (beispielsweise Datenträger- und Netzwerkschnittstellenstatus) sowie zur durchschnittlichen Betriebszeit enthält.

Der Bericht wird dem Systemadministrator automatisch täglich um 2:00 Uhr per E-Mail zugesendet. Informationen zum Ändern der E-Mail-Adresse des Systemadministrators finden Sie unter Allgemeine Appliance-Einstellungen bei aktivierter Organisationskomponente konfigurieren oder Allgemeine Appliance-Einstellungen ohne aktivierte Organisationskomponente konfigurieren.

Status des Datenträgers

Der Bericht *Daily run output*, der jeden Tag automatisch per E-Mail an den Systemadministrator gesendet wird, enthält die Tabelle *Datenträgerstatus*.

Filesystem	Größe	Verwendet	Avail	Kapazität	Mounted on
/dev/twed0s1a	38 G	3,6 G	32 G	10%	/
devfs	1,0 K	1,0 K	0B	100%	/dev
fdescfs	1,0 K	1,0 K	0B	100%	/dev/fd
procfs	4,0 K	4,0 K	0B	100%	/proc

Die folgenden Spalten werden in der Tabelle *Datenträgerstatus* angezeigt.

Spaltenüberschrift	Beschreibung
Filesystem	Der Name des Betriebssystems.
Größe	Die Menge an dem angegebenen Dateisystem zugewiesenen Datenträger-Speicherplatz.
Verwendet	Die Menge an vom angegebenen Dateisystem verwendeten Datenträger-Speicherplatz.
Avail	Die Menge an für das angegebene Dateisystem verfügbarem Datenträger-Speicherplatz.
Kapazität	Der prozentual für das angegebene Dateisystem verfügbare Datenträger-Speicherplatz.
Mounted on	Die Datenträgerpartition, auf der sich das angegebene Dateisystem befindet.

Netzwerkschnittstellen-Status der Appliance

Der Bericht *Daily run output*, der jeden Tag automatisch per E-Mail an den Systemadministrator gesendet wird, enthält die Tabelle *Netzwerkschnittstellenstatus*.

Vergewissern Sie sich, dass die Werte für *Ierrs/Oerrs* gleich Null sind. Andere Werte weisen auf Netzwerkfehler hin.

Wenn ständig Fehler auftreten, sollten Sie sich an den **Quest Support** unter https://support.quest.com/contact-support wenden.

```
Network interface status:
Name    Mtu Network       Address              Ipkts Ierrs    Opkts Oerrs  Coll
em0    1500 <Link#1>      00:0c:29:83:85:63 30383751     0 29509710     0     0
em0    1500 192.168.200.0 MyK1              30379356     - 29509310     -     -
plip0  1500 <Link#2>                               0     0        0     0     0
lo0   16384 <Link#3>                          392328     0   392328     0     0
lo0   16384 fe80:3::1     fe80:3::1               0     -        0     -     -
lo0   16384 localhost     ::1                   216     -      216     -     -
lo0   16384 your-net      localhost          392112     -   392112     -     -
```

Betriebszeit und durchschnittliche Belastung der Appliance

Die Betriebszeit und der Lastdurchschnitt der Appliance werden im Bericht *Daily Run Output* angezeigt, der jeden Tag automatisch per E-Mail an den Systemadministrator gesendet wird.

Die durchschnittliche Belastung variiert, je nachdem, wie hoch die Belastung der Appliance bei Ausführung des Berichts war.

Die folgenden Angaben informieren darüber, wie lange die Appliance aktiv ist, seit sie zuletzt ausgeschaltet wurde. In diesem Beispiel sind keine Benutzer bei der Appliance angemeldet.

```
Local system status:
 2:01AM up 7 days, 4:12, 0 users, load averages: 0,05, 0,20, 0,15
```

Zustand der E-Mail-Systeme

Der Zustand der E-Mail-Systeme wird im Bericht *Daily Run Output* angezeigt, der jeden Tag automatisch per E-Mail an den Systemadministrator gesendet wird.

Bei den folgenden Meldungen handelt es sich um die FreeBSD-Standardmeldungen, die sich auf den Zustand der E-Mail-Systeme beziehen.

Es sollten keine E-Mails in den Warteschlangen enthalten sein. Wenn in den Warteschlangen Nachrichten angezeigt werden, finden Sie entsprechende Informationen unter SMTP-Einstellungen überprüfen.

```
Mail in local queue:
/var/spool/mqueue is empty
      Total requests: 0
Mail in submit queue:
/var/spool/clientmqueue is empty
      Total requests: 0
Security check:
    (output mailed separately)
Checking for rejected mail hosts:
Checking for denied zone transfers (AXFR and IXFR):
tar: Removing leading /' from member names
```

SMTP-Einstellungen überprüfen

Wenn in den Warteschlangen E-Mail-Nachrichten angezeigt werden, überprüfen Sie bitte Ihre SMTP-Einstellungen.

1. Navigieren Sie zur *Systemsteuerung* der Appliance:
   - **Wenn die Organisationskomponente nicht für die Appliance aktiviert ist, melden Sie sich bei der Administratorkonsole an: `https://appliance_hostname/admin`, und wählen Sie dann Einstellungen > Systemsteuerung aus.**
   - **Wenn die Organisationskomponente für die Appliance aktiviert ist, melden Sie sich bei der Systemverwaltungskonsole der Appliance an: `https://appliance_hostname/system`. Oder wählen Sie in der Dropdown-Liste rechts oben auf der Seite den Eintrag System aus, und klicken Sie dann auf Einstellungen > Systemsteuerung.**
2. Klicken Sie auf **Netzwerkeinstellungen**, um die Seite *Netzwerkeinstellungen* anzuzeigen.

Sicherungsstatus der Appliance

Der Sicherungsstatus der Appliance wird im Bericht *Daily Run Output* angezeigt, der jeden Tag automatisch per E-Mail an den Systemadministrator gesendet wird.

Die folgende anwendungsspezifische Meldung informiert Sie darüber, dass die Sicherungen erfolgreich abgeschlossen wurden und sich auf dem Datenträger /kbackup befinden, auf den über FTP zugegriffen werden kann.

Siehe Auf Sicherungsdateien über FTP zugreifen.

```
[21.06.2015 02:01:24 -0700] Backup: Abgeschlossen.
```

Status der RAID-Laufwerke

Bei physischen KACE SMAs wird der Status von RAID-Laufwerken in den Serverprotokollen angezeigt. Der Status ist nur für physische KACE SMAs verfügbar.

Folgende Protokollmeldung gibt an, dass die RAID-Laufwerke ordnungsgemäß funktionieren:

```
Logisches Laufwerk 0 (RAID 5) Informationen
zum Status des RAID-Arrays: Das logische Laufwerk 0 wird nicht neu erstellt: Der Status lautet Opt
Status: Online. Hochgefahren
```

Wenn RAID-Laufwerke heruntergestuft oder nicht ordnungsgemäß neu erstellt werden, wenden Sie sich an den **Quest Support** unter https://support.quest.com/contact-support.

Fehlerbehebung auf der Appliance

Die Appliance enthält Tools, Protokolle und Berichte, mit deren Hilfe Sie den Systemzustand überwachen und Probleme beheben können.

Verwenden von Tools zur Fehlerbehebung

Sie können Tools zur Fehlerbehebung zum Ermitteln und Beheben von Problemen verwenden.

Status von Geräten im Netzwerk überprüfen

Sie können den Status von Geräten im Netzwerk mit dem Ping-Dienstprogramm zur Fehlerbehebung überprüfen.

1. Navigieren Sie zur *Systemsteuerung* der Appliance:
   - **Wenn die Organisationskomponente nicht für die Appliance aktiviert ist, melden Sie sich bei der Administratorkonsole an: `https://appliance_hostname/admin`, und wählen Sie dann Einstellungen > Systemsteuerung aus.**
   - **Wenn die Organisationskomponente für die Appliance aktiviert ist, melden Sie sich bei der Systemverwaltungskonsole der Appliance an: `https://appliance_hostname/system`. Oder**

wählen Sie in der Dropdown-Liste rechts oben auf der Seite den Eintrag System aus, und klicken Sie dann auf Einstellungen > Systemsteuerung.

2. Klicken Sie auf der linken Navigationsleiste auf **Support**, um die Seite *Support* anzuzeigen.
3. Klicken Sie im Abschnitt *Tools zur Fehlerbehebung* auf **Diagnosedienstprogramme ausführen**, um die Seite *Diagnosedienstprogramme* anzuzeigen.
4. Geben Sie im Textfeld die IP-Adresse eines Geräts ein.
5. Wählen Sie in der Dropdown-Liste die Option **ping** aus.
6. Klicken Sie auf **Jetzt ausführen**.

   Die Ergebnisse werden angezeigt.
7. Um andere Dienstprogramme zu verwenden, wählen Sie diese in der Dropdown-Liste aus und klicken Sie anschließend auf **Jetzt ausführen**.

Identifizieren von Geräteproblemen

Verwenden Sie die Liste *Geräteprobleme*, um zu sehen, ob eines Ihrer verwalteten Geräte Probleme bei der Verbindung mit dem Agenten oder andere Probleme hat.

Die Appliance nutzt den KACE Agent, um Informationen von den von Agenten verwalteten Geräten in Ihrem Unternehmen zu sammeln. Wenn ein Gerät Probleme bei der Verbindung mit dem Agenten oder andere Probleme in seiner Umgebung feststellt, kann die Appliance keine Inventarinformationen für dieses Gerät abrufen.

Auf der Listenseite *Geräteprobleme* werden alle von Agenten verwalteten Geräte identifiziert, deren Informationen aufgrund eines der folgenden Probleme nicht in der Bestandsaufnahme angezeigt werden:

- WMI(Windows Management Instrumentation)-Beschädigung.
- Auslastung des Desktop-Heaps.

  TIPP: In den meisten Fällen kann dieses Problem durch einen einfachen Neustart des Geräts behoben werden.
- Fehler beim Schreiben in `amp.conf`.

Weitere Informationen zu diesen Problemen finden Sie unter https://support.quest.com/kace-systems-management-appliance/kb.

1. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
2. Wählen Sie **Einstellungen** > **Support** aus, um die Seite *Support* anzuzeigen.
3. Klicken Sie im Abschnitt *Tools zur Fehlerbehebung* auf **Geräteprobleme**, um die Seite *Geräteprobleme* anzuzeigen.
4. Überprüfen Sie die Liste der fehlerhaften Geräte auf der Seite *Geräteprobleme* und ergreifen Sie ggf. die erforderlichen Maßnahmen, um diese Probleme zu beheben.

Tether zum Support von Quest KACE aktivieren

Sie können auf das Quest Support-Portal zugreifen, um einen Tether zu Ihrer Appliance anzufordern, damit Fehler vom technischen Support von Quest KACE behoben werden können.

Wenden Sie sich unter https://support.quest.com/contact-support an **Quest Support**, um einen Tether-Schlüssel zu erhalten.

Aktivieren Sie den Remote-Zugriff auf die Appliance aus Sicherheitsgründen erst dann, wenn Sie vom Supportteam dazu aufgefordert werden.

1. Navigieren Sie zur *Systemsteuerung* der Appliance:
   - **Wenn die Organisationskomponente nicht für die Appliance aktiviert ist, melden Sie sich bei der Administratorkonsole an: `https://appliance_hostname/admin`, und wählen Sie dann Einstellungen > Systemsteuerung aus.**
   - **Wenn die Organisationskomponente für die Appliance aktiviert ist, melden Sie sich bei der Systemverwaltungskonsole der Appliance an: `https://appliance_hostname/system`. Oder wählen Sie in der Dropdown-Liste rechts oben auf der Seite den Eintrag System aus, und klicken Sie dann auf Einstellungen > Systemsteuerung.**
2. Klicken Sie in der *Systemsteuerung* der Appliance auf **Sicherheitseinstellungen**, um die gleichnamige Seite anzuzeigen.
3. Stellen Sie sicher, dass das Kontrollkästchen **SSH aktivieren** aktiviert ist.
4. Klicken Sie auf **Dienste speichern und neu starten**.
5. Klicken Sie auf der linken Navigationsleiste auf **Support**, um die Seite *Support* anzuzeigen.
6. Klicken Sie im Abschnitt *Tools zur Fehlerbehebung* auf **Tether-Schlüssel eingeben**, um die Seite *Support Tether-Schlüssel* anzuzeigen.
7. Geben Sie auf der Seite *Support Tether-Schlüssel* im Textfeld die Beschreibung des Problems ein und führen Sie einen der folgenden Schritte aus.
   - **Um den Tether-Schlüssel automatisch zu erhalten und die Meldung an den technischen Support zu senden, klicken Sie auf Tether aktivieren.**

     Wenn der Vorgang fehlschlägt, wählen Sie **Tether aktivieren** aus und geben Sie den Tether-Schlüssel ein, wenn Sie dazu aufgefordert werden. Klicken Sie auf **Speichern**.
   - **Wenn Sie einen vom technischen Support bereitgestellten Tether-Schlüssel verwenden möchten, klicken Sie auf Ich habe bereits einen Tether-Schlüssel, wählen Sie dann Tether aktivieren aus und geben Sie den Tether-Schlüssel ein, wenn Sie dazu aufgefordert werden. Klicken Sie auf Speichern.**

Fehlerbehebung bei Problemen mit der Appliance

Die Appliance bietet verschiedene Serverprotokolle, die Ihnen und dem **Quest Support** bei der Erkennung und Behebung von Fehlern nützlich sein können.

Die Protokolle enthalten die Aktivitäten der letzten sieben Tage und werden jeden Tag kopiert und komprimiert. Komprimierte Protokolle werden gelöscht, wenn sie sieben Tage alt sind.

Die Protokollwartung wird täglich überprüft und es sind keine zusätzlichen administrativen Protokollwartungsvorgänge erforderlich.

Appliance-Protokolle anzeigen

Sie können Appliance-Protokolle in der**Administratorkonsole** anzeigen. Die Appliance-Protokolle enthalten Informationen zu den Appliance-Prozessen und -Fehlern, die im System auftreten.

Wenn Sie die Appliance so konfiguriert haben, dass detaillierte Nutzungsdaten mit Quest KACE ausgetauscht werden, werden Appliance- und Agenten-Ausnahmen oder -Fehler täglich an Quest gemeldet. Siehe:

- Allgemeine Appliance-Einstellungen bei aktivierter Organisationskomponente konfigurieren
- Allgemeine Appliance-Einstellungen ohne aktivierte Organisationskomponente konfigurieren

1. Navigieren Sie zur *Systemsteuerung* der Appliance:
   - **Wenn die Organisationskomponente nicht für die Appliance aktiviert ist, melden Sie sich bei der Administratorkonsole an: `https://appliance_hostname/admin`, und wählen Sie dann Einstellungen > Systemsteuerung aus.**
   - **Wenn die Organisationskomponente für die Appliance aktiviert ist, melden Sie sich bei der Systemverwaltungskonsole der Appliance an: `https://appliance_hostname/system`. Oder wählen Sie in der Dropdown-Liste rechts oben auf der Seite den Eintrag System aus, und klicken Sie dann auf Einstellungen > Systemsteuerung.**
2. Klicken Sie in der linken Navigationsleiste auf **Protokolle**, um die Seite *Protokolle* anzuzeigen.
3. Wählen Sie in der Dropdown-Liste *Protokolle* ein Protokoll aus.

Protokolltyp	Protokollname	Beschreibung
Hardware	**Status des Datenträgers**	Der Status des physischen Appliance-Datenträgers (nicht verfügbar für virtuelle Appliances)
Server	**K1000 Protokoll**	Die auf der Appliance generierten Fehler.
	Zugriff	Die Zugriffsinformationen des HTTP-Servers.
	Serverfehler	Fehler oder Serverwarnungen, die sich auf Appliance-Serverprozesse beziehen.
	Statistik	Die Anzahl der Verbindungen, die die Appliance über einen Zeitraum hinweg verarbeitet.
	Aktualisierungen	Details für Appliance-Patches oder -Upgrades, die auf die Appliance angewendet wurden.
	Berichtsprotokoll	Details über ausgeführte Berichte
	Berichtsfehler	Fehler im Zusammenhang mit ausgeführten Berichten.
	Konductor-Protokoll	Konductor-bezogene Protokolle. Konductor ist eine interne Appliance-Komponente, die die Kommunikation zwischen der Appliance und verwalteten Geräten regelt, um einen reibungslosen Systembetrieb zu gewährleisten. Die Anzahl der von Konductor ausgeführten Aufgaben

Protokolltyp	Protokollname	Beschreibung
		wird im Widget *Aufgaben werden durchgeführt* angezeigt. Außerdem werden Informationen zum Aufgabendurchsatz auf der Seite *Allgemeine Einstellungen* (bei Appliances mit aktivierter Organisationskomponente) oder auf der Seite *Kommunikationseinstellungen* (bei Appliances ohne aktivierte Organisationskomponente) der Appliance angezeigt. Siehe: • Allgemeine Appliance-Einstellungen bei aktivierter Organisationskomponente konfigurieren • Agentenkommunikation und Protokolleinstellungen konfigurieren
	Patch-Download-Protokoll	Informationen über Patches, die auf die Appliance heruntergeladen wurden.
	Protokoll "Dell Aktualisierungen"	Informationen über Dell Hardware-Aktualisierungen, die auf die Appliance heruntergeladen wurden.
	Sicherungsprotokoll	Details zu täglichen und monatlichen Appliance-Sicherungen.
	Protokoll "Sicherung/ Wiederherstellung"	Details zur Wiederherstellung von Informationen aus Appliance-Sicherungen.
	Ermittlungsprotokoll	Informationen zum Erkennungsvorgang.
	Provisionierungsprotokoll	Informationen zur Provisionierung durch den KACE Agent.
	Protokoll der Durchführung ohne Agent	Informationen im Zusammenhang mit Geräteverbindungen mit der Appliance ohne Agent.
	Überwachungsprotokoll	Informationen im Zusammenhang mit überwachten Servern und ihren Verbindungen mit der Appliance.

Protokolltyp	Protokollname	Beschreibung
	Softwareinventar	Informationen im Zusammenhang mit der Softwarekatalog-Inventarverarbeitung.
	Softwareinventarfehler	Verarbeitungsfehler im Zusammenhang mit der Softwarekatalog-Inventarverarbeitung der Appliance.
	Asset-Import-Protokoll	Informationen zum Importieren von Assets.
	Dell Service-Protokoll	Informationen zu Aktualisierungen in Bezug auf den Dell Service.
	Benutzerauthentifizierungsprotokoll	Informationen zur Benutzerauthentifizierung. Jeder Eintrag im Protokoll enthält die folgenden Informationen: • Den Namen des Benutzerkontos, das versucht, sich anzumelden. • Die IP-Adresse des Geräts, von dem der Anmeldeversuch stammt. • Die Konsole, bei der sich der Benutzer anmelden möchte: `userui` (**Benutzerkonsole**), `systemui` (**Systemverwaltungskonsole**), `adminui` (**Administratorkonsole**) oder eine verknüpfte Appliance. • Den Namen der Organisation, für die der Benutzer authentifiziert wird. • Den Typ der verwendeten Authentifizierung: `Lokale Authentifizierung`, `Einfache Anmeldung`, `Systemui Lokale Authentifizierung` oder `LDAP`. • Das Ergebnis des Anmeldeversuchs: `Erfolgreich` oder `Fehlgeschlagen`. Beispiel:

Protokolltyp	Protokollname	Beschreibung
		`[2018-04-26 07:27:06 -0700] AUTH [Info] Admin - 10.1.243.172 - Adminui - Standard - Systemui Lokale Authentifizierung - Erfolg`
E-Mail	**Service Desk-Protokoll eingehende E-Mails**	Informationen im Zusammenhang mit Problemen, die während der Verarbeitung von E-Mails für die Service Desk-Warteschlangen mit dem Exim-Server (Mail Transfer-Agent) aufgetreten sind. Zum Beispiel ungültige E-Mail-Adressen und Probleme mit der Service Desk-Lizenzierung.
	Service Desk-Fehlerprotokoll eingehende E-Mails	Fehler, die bei der Verarbeitung von eingehenden E-Mail-Nachrichten aufgetreten sind.
	Service Desk-Protokoll ausgehende E-Mails	Fehler, die beim Senden ausgehender E-Mail-Nachrichten mit dem E-Mail-Daemon aufgetreten sind. Zum Beispiel ungültige E-Mail-Adressen.
	Service Desk-Fehlerprotokoll ausgehende E-Mails	Fehler, die bei der Verarbeitung von ausgehenden E-Mail-Nachrichten aufgetreten sind.
	KMailServices-Protokoll	Informationen zum `KMailServices`-Prozess.
EXIM	**Haupt-Exim-Protokoll**	Informationen bezüglich der Zustellung der einzelnen Nachrichten am Ziel.
	Exim-Ablehnungsprotokoll	Informationen zu abgelehnten Nachrichten.
Gerät	**Clientzugriff**	Zugriffsprotokolle des KACE Agent.
	Client-Fehler	Ausnahmeprotokolle des KACE Agent.
	Agent-Messaging-Protokoll - Server	Serverbezogene Agent-Messaging-Protokolleinträge.
	Agenten-Messaging-Protokoll – Serverfehler	Serverbezogene Fehlereinträge im Agenten-Messaging-Protokoll.

Protokolltyp	Protokollname	Beschreibung
	Agenten-Messaging-Protokoll - Warteschlange	Warteschlangenbezogene Agenten-Messaging-Protokolleinträge.
	Agenten-Messaging-Protokoll – Warteschlangenfehler	Warteschlangenbezogene Fehlereinträge im Agenten-Messaging-Protokoll.

Wenn die Organisationskomponente in Ihrem System aktiviert ist, können Sie die Anzahl von Tagen ändern, für die Protokolle aufbewahrt werden. Diese Einstellung ist im Abschnitt *Protokollaufbewahrung* auf der Seite *Allgemeine Einstellungen* der Appliance verfügbar. Siehe Allgemeine Appliance-Einstellungen bei aktivierter Organisationskomponente konfigurieren.

Aktivitätsprotokolle der Appliance herunterladen

Sie können Aktivitätsprotokolle der Appliance aus der **Administratorkonsole** herunterladen. Diese Protokolle können bei der Fehlerbehebung nützlich sein.

1. Navigieren Sie zur *Systemsteuerung* der Appliance:
   - **Wenn die Organisationskomponente nicht für die Appliance aktiviert ist, melden Sie sich bei der Administratorkonsole an: `https://appliance_hostname/admin`, und wählen Sie dann Einstellungen > Systemsteuerung aus.**
   - **Wenn die Organisationskomponente für die Appliance aktiviert ist, melden Sie sich bei der Systemverwaltungskonsole der Appliance an: `https://appliance_hostname/system`. Oder wählen Sie in der Dropdown-Liste rechts oben auf der Seite den Eintrag System aus, und klicken Sie dann auf Einstellungen > Systemsteuerung.**
2. Klicken Sie auf der linken Navigationsleiste auf **Support**, um die Seite *Support* anzuzeigen.
3. Klicken Sie auf **Aktivitätsprotokolle der Appliance abrufen**.

   Die Protokolle werden in die Datei `k1000_logs.tgz` heruntergeladen.

   Informationen zu Protokollen, die beim Debugging verwendet werden, finden Sie unter:
   - Provisionierungszeitpläne verwalten
   - Fehlerbehebung und Debuggen des KACE Agent
   - Appliance-Protokolle anzeigen

Wenn die Organisationskomponente in Ihrem System aktiviert ist, können Sie die Anzahl von Tagen ändern, für die Protokolle aufbewahrt werden. Diese Einstellung ist im Abschnitt *Protokollaufbewahrung* auf der Seite *Allgemeine Einstellungen* der Appliance verfügbar. Siehe Allgemeine Appliance-Einstellungen bei aktivierter Organisationskomponente konfigurieren.

"Daily Run Output" (Täglicher Systembericht) anzeigen

Der "Daily Run Output" (Täglicher Systembericht) ist ein Bericht, in dem Appliance-Informationen wie Status des Datenträgers, Status der Netzwerkschnittstelle, Betriebszeit und Lastdurchschnitt, Zustand der E-Mail-Systeme sowie Datenbankstatus enthalten sind. Verwenden Sie diesen Bericht, um den Status des Systems zu überprüfen und Probleme zu ermitteln, die behoben werden müssen.

Dieser Bericht wird täglich ausgeführt und per E-Mail an den Systemadministrator gesendet. Siehe Informationen zu "Daily Run Output" und Security Run Output (Sicherheitsbericht).

Fehlerbehebung und Debuggen des KACE Agent

Verwenden Sie die Debug-Funktionen des Agenten, um Probleme im Zusammenhang mit dem Agenten zu beheben.

Wenn Geräte nicht im Inventar angezeigt werden, stellen Sie sicher, dass die Option **Agent Debug Trace** auf der Seite *Communication Settings* aktiviert ist. Weitere Informationen hierzu finden Sie unter Agentenkommunikation und Protokolleinstellungen konfigurieren.

Weitere Unterstützung erhalten Sie auf der Website vom **Quest Support** unter https://support.quest.com/contact-support. Diese Website enthält eine Knowledge Base zur Fehlerbehebung.

Windows Sicherheitsprobleme beheben, die die Agenten-Provisionierung verhindern

Wenn Windows Sicherheitseinstellungen verhindern, dass die Appliance den Agenten für Windows Geräte bereitstellen kann, können Sie die Einstellungen über eine Eingabeaufforderung neu konfigurieren.

Zum Zulassen der Provisionierung müssen Sie die Firewall öffnen und die Sicherheitseinstellungen konfigurieren.

1. Öffnen Sie eine Eingabeaufforderung auf dem Gerät.
2. Öffnen Sie die Firewall und konfigurieren Sie die Sicherheitseinstellungen:

```
reg add HKLM\SYSTEM\CurrentControlSet\Control\Lsa /v ForceGuest /t REG_DWORD /d
0 /f
```

```
reg add HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\system /v
LocalAccountTokenFilterPolicy /t REG_DWORD /d 1 /f
```

```
reg add "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server" /v
FdenyTSConnections /t REG_DWORD /d 0 /f
```

```
netsh.exe firewall set service type=FILEANDPRINT mode=ENABLE scope=ALL
```

```
netsh.exe firewall set service type=REMOTEADMIN mode=ENABLE scope=ALL
```

Testen der E-Mail-Kommunikation und Fehlerbehebung

Sie können durch bestimmte Schritte sicherstellen, dass die E-Mail-Kommunikation des Service Desks korrekt funktioniert. Die Konfiguration des E-Mail-Systems kann durch eine Prüfung der aus- und eingehenden E-Mails überprüft werden. Außerdem können Sie Telnet zum Testen der E-Mail-Kommunikation verwenden. Für die Fehlerinformationen sind Protokolldateien verfügbar.

Bei den Informationen zum Testen und zur Fehlerbehebung wird davon ausgegangen, dass Sie für die Kommunikation mit der Appliance wie in Konfigurieren der E-Mail-Einstellungen beschrieben einen POP3-E-Mail-Server verwenden.

Ausgehende E-Mail-Nachrichten testen

Sie können ausgehende E-Mails testen, um die Systemkonfiguration zu überprüfen.

1. Navigieren Sie zur *Systemsteuerung* der Appliance:
   - **Wenn die Organisationskomponente nicht für die Appliance aktiviert ist, melden Sie sich bei der Administratorkonsole an: `https://appliance_hostname/admin`, und wählen Sie dann Einstellungen > Systemsteuerung aus.**
   - **Wenn die Organisationskomponente für die Appliance aktiviert ist, melden Sie sich bei der Systemverwaltungskonsole der Appliance an: `https://appliance_hostname/system`. Oder wählen Sie in der Dropdown-Liste rechts oben auf der Seite den Eintrag System aus, und klicken Sie dann auf Einstellungen > Systemsteuerung.**
2. Klicken Sie auf der linken Navigationsleiste auf **Support**, um die Seite *Support* anzuzeigen.
3. Klicken Sie im Abschnitt *Tools zur Fehlerbehebung* auf **Diagnosedienstprogramme ausführen**, um die Seite *Diagnosedienstprogramme* anzuzeigen.
4. Wählen Sie in der Dropdown-Liste Testen die Option **E-Mail senden** aus.
5. Geben Sie im Textfeld eine gültige E-Mail-Adresse ein.
6. Klicken Sie auf **Jetzt ausführen**, um ein Protokoll des E-Mail-Pfads anzuzeigen.
7. Prüfen Sie die Protokolldatei auf Fehler.
   - **Wenn sie keine Fehler enthält, wurde die ausgehende E-Mail-Nachricht erfolgreich gesendet.**
   - **Führen Sie bei einem Fehler folgende Schritte aus:**
     - Prüfen Sie Ihre E-Mail- und Spam-Filter.
     - Prüfen Sie die Netzwerkeinstellungen der Appliance. Falls Sie Ihren eigenen SMTP-Server verwenden, sendet die Appliance E-Mails über diesen Server. Viele SMTP-Server erfordern dazu eine spezifische Berechtigung. Fügen Sie die IP-Adresse der Appliance zur Liste akzeptierter Server hinzu.
     - Prüfen Sie die Router-Einstellungen. Stellen Sie sicher, dass die Appliance den SMTP-Port (25) verwenden kann.
     - Prüfen Sie die Firewalleinstellungen. Stellen Sie sicher, dass die Appliance den SMTP-Port (25) verwenden kann.
     - Falls Sie das Problem nicht beheben können, wenden Sie sich an den **Quest Support** unter https://support.quest.com/contact-support.

Eingehende E-Mails testen

Sie können eingehende E-Mails testen, um die Systemkonfiguration zu überprüfen.

1. Melden Sie sich bei Ihrem SMTP-Server an und erstellen Sie ein Service Desk-Ticket, indem Sie eine E-Mail an die Support-E-Mail-Adresse Ihrer Appliance senden.
2. Rufen Sie die Seite *Tickets* des Service Desks auf:
   a. Melden Sie sich bei der Administratorkonsole der Appliance an: `https://`**appliance_hostname**`/admin`. Oder wählen Sie, wenn in den allgemeinen Einstellungen der Appliance die Option *Organisationsmenü in Verwaltungskopfzeile anzeigen* aktiviert ist, in der Dropdown-Liste oben rechts auf der Seite neben den Anmeldeinformationen eine Organisation aus.
   b. Klicken Sie in der linken Navigationsleiste auf **Service Desk** und anschließend auf **Tickets**.
3. Bestätigen Sie, dass ein Ticket angezeigt wird.

   Wenn Sie die E-Mail von einem gültigen Konto der Appliance senden, wird automatisch ein Ticket erstellt.

Telnet zum Testen eingehender E-Mails verwenden

Sie können Telnet verwenden, um mit dem SMTP-Server der Appliance zu kommunizieren und eine Test-E-Mail zu senden.

1. Geben Sie die folgenden Befehle ein:

   ```
   >telnet k1000.meinedomäne.com 25
   >EHLO meinedomäne.com
   >MAIL FROM:<admin@meinedomäne.com>
   >RCPT TO:<servicedesk@k1000.meinedomäne.com
   >DATA
   >Testdaten hier eingeben
   >QUIT
   .
   ```

   Diese Befehle starten die Kommunikation, teilen dem Server mit, von wem die Nachricht stammt und an wen sie übermittelt werden soll, bereiten das Senden der Daten vor und beenden Telnet.

2. Prüfen Sie im Service Desk-Posteingang, ob Sie eine E-Mail von admin@**meinedomäne**.com erhalten haben.

Zum Anzeigen von Microsoft Exchange Server-Fehlern auf Appliance-Protokolle zugreifen

Informationen zu Microsoft Exchange Server-Fehlern sind den Protokollen der Appliance verfügbar, wenn die Protokollierung auf dem Exchange Server aktiviert ist.

1. Öffnen Sie in Microsoft Exchange Server das *Eigenschaftenfenster für den virtuellen SMTP-Server*.
2. Stellen Sie auf der Registerkarte *Allgemein* sicher, dass das Kontrollkästchen *Protokollierung aktivieren* aktiviert ist. Aktivieren Sie andernfalls dieses Kontrollkästchen und senden eine Test-E-Mail an die Appliance.
3. Navigieren Sie zur *Systemsteuerung* der Appliance:
   - **Wenn die Organisationskomponente nicht für die Appliance aktiviert ist, melden Sie sich bei der Administratorkonsole an: `https://appliance_hostname/admin`, und wählen Sie dann Einstellungen > Systemsteuerung aus.**
   - **Wenn die Organisationskomponente für die Appliance aktiviert ist, melden Sie sich bei der Systemverwaltungskonsole der Appliance an: `https://appliance_hostname/system`. Oder wählen Sie in der Dropdown-Liste rechts oben auf der Seite den Eintrag System aus, und klicken Sie dann auf Einstellungen > Systemsteuerung.**
4. Klicken Sie in der linken Navigationsleiste auf **Protokolle**, um die Seite *Protokolle* anzuzeigen.
5. Wählen Sie aus der Dropdown-Liste *Protokolle* ein Protokoll aus.
6. Überprüfen Sie, ob in den Dateien `exim_mainlog_*` und `exim_paniclog_*` Probleme aufgeführt sind.

   Folgende Probleme sind möglich:

   - Fehler und fehlgeschlagene Schritte
   - Hostnamen und andere Variablen, die nicht aufgelöst wurden
7. Prüfen Sie das Protokoll `Debug_*` auf weitere "Exim"-Probleme wie unkontrollierbare "EExim"-Prozesse.

Die folgenden Protokolle enthalten möglicherweise ebenfalls Hinweise zur Problemlösung:

- `khelpdeskmailhandler_output`
- `khelpdeskmailnotifier_error`
- `khelpdeskmailnotifier_output`

8. Prüfen Sie die Protokolle des Microsoft Exchange-SMTP-Dienstes unter `C:\windows\system32\ologFiles\*SMTP` auf Fehler.

E-Mail-Fehler beheben

Für einige typische E-Mail-Fehler sind Lösungen verfügbar.

E-Mail-Fehler	Lösung
550 Unbekannter Benutzer	• Vergewissern Sie sich, dass die Adresse korrekt ist. • Überprüfen Sie, ob die Adresse der vom Service Desk verwendeten Adresse entspricht. • Schalten Sie den externen SMTP-Server aus und löschen Sie die Adresse aus den Netzwerkeinstellungen. Führen Sie einen Neustart aus und geben Sie die Adresse erneut ein. Führen Sie einen weiteren Neustart aus.
451 Absender kann nicht überprüft werden	Prüfen Sie die DNS-Einstellungen.

Über die Zweifaktor-Authentifizierung der Diagnosekonsole

Zweifaktor-Authentifizierung (auch als 2FA bezeichnet) ermöglicht Ihnen, den Zugriff auf das Appliance-Backend zu steuern. Wenn Sie den Zugriff auf die Appliance per SSH aktivieren und einen Tether erstellen, kann sich das **Quest Support**-Team mithilfe des root-Kennworts der Appliance und einem Zugangstoken beim Backend der Appliance anmelden. Tokens werden im *Assistenten für die Ersteinrichtung* erstellt. Sie können auf der Seite *System unterstützt Zweifaktor-Authentifizierung* in der Appliance angezeigt und erneut erstellt werden Systemkonsole. Jedes Token kann nur einmal verwendet werden und muss an den **Quest Support**-Kontakt weitergeleitet werden, bevor sich dieser über den Tether oder die Konsole bei der Appliance anmelden kann.

Um zu dieser Seite zu navigieren, melden Sie sich bei der Systemkonsole der Appliance an. Klicken Sie in der linken Navigationsleiste unter *Einstellungen* auf **Support** und auf der Seite *Support* unter *Problembehebungstools* auf **Zweifaktor-Authentifizierung**.

Der Sicherheitsschlüssel und Offline-Token, die beim ersten Setup der Appliance bereitgestellt werden, müssen an einem sicheren Ort protokolliert und gespeichert werden, nicht auf dem Appliance-Computer. Möglicherweise müssen Sie diese Informationen bei Bedarf dem Support mitteilen.

Wenn nach dem Upgrade von einer früheren Version eine Meldung angezeigt wird, dass die Zweifaktor-Authentifizierung der Diagnosekonsole deaktiviert ist und Sie diese für erweiterte Sicherheit aktivieren möchten, befolgen Sie die Anweisungen in der Nachricht, um sie zu aktivieren.

- Um den geheimen Schlüssel zu ersetzen und die Offline-Token erneut zu generieren, klicken Sie auf **Geheimen Schlüssel ersetzen**.
- Um Offline-Token erneut zu generieren, klicken Sie auf **Offline-Token erneut generieren**.

Anhang

Namen von Datenbanktabellen

Namen von Datenbanktabellen können in Berichten und anderen Datenbankabfragen verwendet werden.

In der folgenden Tabelle sind die aktuellen Namen der Datenbanktabellen und die Tabellennamen aufgeführt, die sich zwischen Version 6.3 und Version 6.4 der Appliance geändert haben:

- Datenbanktabellen auf Organisationsebene (ORG1)
- Datenbanktabellen auf Systemebene (KBSYS)

Datenbanktabellen auf Organisationsebene (ORG1)

In der folgenden Tabelle sind die Namen der Datenbanktabellen auf Organisationsebene (ORG1) aufgeführt. Verwenden Sie diese Tabellennamen, wenn Sie benutzerdefinierte Berichte mithilfe von SQL-Abfragen erstellen. Siehe Berichte mithilfe von SQL-Abfragen erstellen.

ORG1-Datenbanktabellen und -Komponenten

Tabelle	Komponente
ADVISORY	Service Desk: Knowledge Base
ADVISORY_LABEL_JT	Service Desk: Knowledge Base
ADVISORY_RATINGS	Service Desk: Knowledge Base
AGENTLESS_TASK_LOG	Appliance-Administration: Erkennung
ASSET	Asset Management
ASSET_ASSOCIATION	Asset Management
ASSET_CATALOG_ASSOCIATION	Asset Management
ASSET_CLASS	Asset Management: Asset-Untertypen
ASSET_DATA_1	Asset Management: Assets importieren
ASSET_DATA_2	Asset Management: Assets importieren
ASSET_DATA_3	Asset Management: Assets importieren
ASSET_DATA_4	Asset Management: Assets importieren
ASSET_DATA_5	Asset Management: Assets importieren
ASSET_DATA_6	Asset Management: Assets importieren

Tabelle	Komponente
ASSET_DATA_7	Asset Management: Assets importieren
ASSET_FIELD_DEFINITION	Einstellungen: Asset-Verlauf
ASSET_FILTER	Asset Management: Labeling
ASSET_HIERARCHY	Asset Management
ASSET_HISTORY	Einstellungen: Asset-Verlauf
ASSET_TYPE	Asset Management: Asset-Typen
AUTHENTICATION	Appliance-Administration
CLIENTDIST_LABEL_JT	Appliance-Administration: KACE Agent
CLIENT_DISTRIBUTION	Appliance-Administration: KACE Agent
CREDENTIAL	Einstellungen: Anmeldeinformationen
CUSTOM_FIELD_DEFINITION	Appliance-Administration
CUSTOM_VIEW	Appliance-Administration: Service Desk-Konfiguration
DASHBOARD	Dashboard
DASHBOARD_CACHE	Dashboard
DELL_ASSET	Sicherheit: Dell Aktualisierungen
DELL_INVENTORY	Sicherheit: Dell Aktualisierungen
DELL_INVENTORY_APPLICATION_DEVICE_JT	Sicherheit: Dell Aktualisierungen
DELL_INVENTORY_DEVICE_JT	Sicherheit: Dell Aktualisierungen
DELL_INVENTORY_LOG	Sicherheit: Dell Aktualisierungen
DELL_MACHINE_PKG_UPDATE_STATUS	Sicherheit: Dell Aktualisierungen
DELL_MACHINE_STATUS	Sicherheit: Dell Aktualisierungen
DELL_PKG_LABEL_JT	Sicherheit: Dell Aktualisierungen
DELL_PKG_STATUS	Sicherheit: Dell Aktualisierungen
DELL_PKG_UPDATE_HISTORY	Sicherheit: Dell Aktualisierungen

Tabelle	Komponente
DELL_SCHEDULE	Sicherheit: Dell Aktualisierungen
DELL_SCHEDULE_LABEL_JT	Sicherheit: Dell Aktualisierungen
DELL_SCHEDULE_MACHINE_STATUS	Sicherheit: Dell Aktualisierungen
DELL_SCHEDULE_OS_JT	Sicherheit: Dell Aktualisierungen
DELL_SCHEDULE_UPDATE_LABEL_JT	Sicherheit: Dell Aktualisierungen
DELL_WARRANTY	Sicherheit: Dell Aktualisierungen
DEVICE_DETAIL_FIELD	Inventar: Geräte
DEVICE_DETAIL_GROUP	Inventar: Geräte
DEVICE_DETAIL_GROUP_ASSET_CLASS_JT	Inventar: Geräte
DEVICE_DETAIL_SECTION	Inventar: Geräte
DEVICE_DETAIL_SECTION_ASSET_CLASS_JT	Inventar: Geräte
DEVP_PROFILE_APPLIED	Skripterstellung: Mac Profile
DEVP_PROFILE_APPLIED_MACHINE	Skripterstellung: Mac Profile
DEVP_PROFILE_APPLIED_PAYLOAD	Skripterstellung: Mac Profile
DEVP_PROFILE_APPLIED_PAYLOAD_ATTRIBUTE	Skripterstellung: Mac Profile
FILTER	Labels
FS	Dateisynchronisierungen
FS_LABEL_JT	Dateisynchronisierungen
FS_MACHINE_JT	Dateisynchronisierungen
GLOBAL_OPTIONS	Appliance-Administration
GRID_COLUMNS_OVERRIDES	Appliance-Administration
HD_ANNOUNCEMENT	Service Desk: Ankündigungen
HD_ANNOUNCEMENT_LABEL_JT	Service Desk: Ankündigungen
HD_ARCHIVE_ATTACHMENT	Service Desk: Ticket-Archiv

Tabelle	Komponente
HD_ARCHIVE_TICKET	Service Desk: Ticket-Archiv
HD_ARCHIVE_TICKET_CHANGE	Service Desk: Ticket-Archiv
HD_ARCHIVE_TICKET_CHANGE_FIELD	Service Desk: Ticket-Archiv
HD_ARCHIVE_WORK	Service Desk: Ticket-Archiv
HD_ATTACHMENT	Service Desk: Tickets
HD_CATEGORY	Service Desk: Tickets
HD_CUSTOM_FIELDS	Service Desk: Tickets
HD_EMAIL_EVENT	Service Desk: Tickets
HD_FIELD	Service Desk: Tickets
HD_HOME_PAGE_WIDGET	Service Desk: Startseite der Benutzerkonsole
HD_IMPACT	Service Desk: Tickets
HD_LINK	Service Desk: Startseite der Benutzerkonsole
HD_MAILTEMPLATE	Service Desk: Tickets
HD_PRIORITY	Service Desk: Tickets
HD_QUEUE	Service Desk: Warteschlangen
HD_QUEUE_APPROVER_LABEL_JT	Service Desk: Warteschlangen
HD_QUEUE_OWNER_LABEL_JT	Service Desk: Warteschlangen
HD_QUEUE_SUBMITTER_LABEL_JT	Service Desk: Warteschlange
HD_SERVICE	Service Desk: Tickets
HD_SERVICE_TICKET	Service Desk: Tickets
HD_SERVICE_USER_LABEL_JT	Service Desk: Tickets
HD_SLA_BUSINESS_HOURS	Service Desk: Service Level-Vereinbarung
HD_SLA_HOLIDAYS	Service Desk: Service Level-Vereinbarung
HD_STATUS	Service Desk: Tickets

Tabelle	Komponente
HD_TICKET	Service Desk: Tickets
HD_TICKET_CHANGE	Service Desk: Tickets
HD_TICKET_CHANGE_FIELD	Service Desk: Tickets
HD_TICKET_FILTER	Service Desk: Tickets
HD_TICKET_RELATED	Service Desk: Tickets
HD_TICKET_RULE	Service Desk: Tickets
HD_WORK	Service Desk: Tickets
IM_CRON	Appliance-Administration
KBOT	Skripterstellung
KBOT_CRON_SCHEDULE	Skripterstellung
KBOT_DEPENDENCY	Skripterstellung
KBOT_EVENT_SCHEDULE	Skripterstellung
KBOT_FORM	Skripterstellung
KBOT_FORM_DATA	Skripterstellung
KBOT_LABEL_JT	Skripterstellung
KBOT_LOG	Skripterstellung
KBOT_LOG_DETAIL	Skripterstellung
KBOT_LOG_LATEST	Skripterstellung
KBOT_OS_FAMILY_JT	Skripterstellung
KBOT_OS_JT	Skripterstellung
KBOT_RUN	Skripterstellung
KBOT_RUN_MACHINE	Skripterstellung
KBOT_RUN_TOKEN	Skripterstellung
KBOT_SHELL_SCRIPT	Skripterstellung

Tabelle	Komponente
KBOT_UPLOAD	Skripterstellung
KBOT_VERIFY	Skripterstellung
KBOT_VERIFY_STEPS	Skripterstellung
KMON_ALERT	Überwachung
KMON_CONDITION	Überwachung
KMON_CONFIG	Überwachung
KMON_CONFIG_DEFAULT	Überwachung
KMON_CONFIG_DETAIL	Überwachung
KMON_CONFIG_DEVICE_JT	Überwachung
KMON_INSTALL_LEP_DEVICE_JT	Überwachung: Log Enablement Packages
KMON_LEP	Überwachung: Log Enablement Package (LEP)
KMON_LEP_INSTALL	Überwachung: Log Enablement Package (LEP)
KMON_LOG_CONFIG	Überwachung
KMON_MAINT_CONFIG	Überwachung
KMON_MONITORED_DEVICE	Überwachung
LABEL	Labels
LABEL_LABEL_JT	Labels
LDAP_FILTER	Labels: LDAP
LDAP_IMPORT_USER	Labels: LDAP
MACHINE	Inventar: Geräte
MACHINE_ACTIONS	Inventar: Geräte
MACHINE_BITLOCKER_VOLUME	Inventar: Geräte
MACHINE_CHROMEOS_DETAILS	Inventar: Geräte
MACHINE_CUSTOM_INVENTORY	Inventar: Geräte

Tabelle	Komponente
MACHINE_DAILY_UPTIME	Inventar: Geräte
MACHINE_DCM_AMT_SETTINGS	Inventar: Geräte
MACHINE_DCM_BATTERY	Inventar: Geräte
MACHINE_DCM_DESKTOP_MONITOR	Inventar: Geräte
MACHINE_DCM_FLAT_PANEL	Inventar: Geräte
MACHINE_DCM_LOG_ENTRY	Inventar: Geräte
MACHINE_DCM_PHYSICAL_MEMORY	Inventar: Geräte
MACHINE_DCM_PROCESSOR	Inventar: Geräte
MACHINE_DCM_VPRO_SETTINGS	Inventar: Geräte
MACHINE_DDPE	Inventar: Geräte
MACHINE_DDPE_VOLUME	Inventar: Geräte
MACHINE_DISKS	Inventar: Geräte
MACHINE_DRIVE_ENCRYPTION_SUMMARY	Inventar: Geräte
MACHINE_FIELD_DEFINITION	Inventar: Geräte
MACHINE_FILEVAULT_VOLUME	Inventar: Geräte
MACHINE_INTEL_AMT	Inventar: Geräte
MACHINE_LABEL_JT	Inventar: Geräte
MACHINE_LOCATION	Inventar: Geräte
MACHINE_MOBILE	Inventar: Geräte
MACHINE_NICS	Inventar: Geräte
MACHINE_NTSERVICE_JT	Inventar: Geräte
MACHINE_PROCESS_JT	Inventar: Geräte
MACHINE_REPLITEM	Inventar: Geräte
MACHINE_SNMP_DATA	Inventar: Geräte

Tabelle	Komponente
MACHINE_SOFTWARE_JT	Inventar: Geräte
MACHINE_STARTUPPROGRAM_JT	Inventar: Geräte
MACHINE_TPM	Inventar: Geräte
MESSAGE	Verteilung: Warnungen
MESSAGE_LABEL_JT	Verteilung: Warnungen
MI	Verteilung: Verwaltete Installationen
MI_ATTEMPT	Verteilung: Verwaltete Installationen
MI_LABEL_JT	Verteilung: Verwaltete Installationen
NODE	Inventar: Erkennung
NODE_LABEL_JT	Inventar: Erkennung
NODE_PORTS	Inventar: Erkennung
NODE_SNMP_IF	Inventar: Erkennung
NODE_SNMP_SYSTEM	Inventar: Erkennung
NOTIFICATION	Berichterstellung: Benachrichtigungen
NOTIFICATION_USER_JT	Berichterstellung: Benachrichtigungen
NTSERVICE	Inventar: Dienste
NTSERVICE_LABEL_JT	Inventar: Dienste
OBJECT_FIELD_DEFINITION	Einstellungen: Verlauf
OBJECT_HISTORY	Einstellungen: Verlauf
OBJECT_HISTORY_CONFIGURATION	Einstellungen: Verlauf
OPERATING_SYSTEMS	Inventar: Geräte
OVAL_STATUS	Sicherheit: OVAL
PATCH_FILTER	Sicherheit: Patch-Verwaltung
PATCH_LABEL_JT	Sicherheit: Patch-Verwaltung

Tabelle	Komponente
PATCH_MACHINE_REMEDIATION_STATUS	Sicherheit: Patch-Verwaltung
PATCH_MACHINE_STATUS	Sicherheit: Patch-Verwaltung
PATCH_PATCH_COUNT	Sicherheit: Patch-Verwaltung
PATCH_SCHEDULE	Sicherheit: Patch-Zeitpläne
PATCH_SCHEDULE_DEPLOY_LABEL_JT	Sicherheit: Patch-Zeitpläne
PATCH_SCHEDULE_DETECT_LABEL_JT	Sicherheit: Patch-Zeitpläne
PATCH_SCHEDULE_LABEL_JT	Sicherheit: Patch-Zeitpläne
PATCH_SCHEDULE_MACHINE_STATUS	Sicherheit: Patch-Zeitpläne
PATCH_SCHEDULE_OS_JT	Sicherheit: Patch-Zeitpläne
PATCH_SCHEDULE_ROLLBACK_LABEL_JT	Sicherheit: Patch-Zeitpläne
PATCH_SCHEDULE_RUN	Sicherheit: Patch-Zeitpläne
PATCH_SCHEDULE_RUN_COUNTS	Sicherheit: Patch-Zeitpläne
PATCH_SCHEDULE_RUN_LOG	Sicherheit: Patch-Zeitpläne
PATCH_SCHEDULE_RUN_MACHINE	Sicherheit: Patch-Zeitpläne
PATCH_SETTINGS	Sicherheit: Abonnements
PATCH_STATUS	Sicherheit: Patch-Verwaltung
PORTAL	Service Desk: **Benutzerkonsole**
PORTAL_LABEL_JT	Service Desk: **Benutzerkonsole**
PROCESS	Inventar: Prozesse
PROCESS_LABEL_JT	Inventar: Prozess
PROVISION_CONFIG	Einstellungen: Agenten-Provisionierung
PROVISION_NODE	Einstellungen: Agenten-Provisionierung
REMOTE_CHROMEOS_HOST	Einstellungen: Provisionierung ohne Agent
REMOTE_DMM_HOST	Einstellungen: Ohne Agent: Dell Mobility Manager

Tabelle	Komponente
REMOTE_HOST	Einstellungen: Provisionierung ohne Agent
REMOTE_HOST_KUID	Einstellungen: Provisionierung ohne Agent
REMOTE_SHELL_HOST	Einstellungen: Provisionierung ohne Agent
REMOTE_SNMP_HOST	Einstellungen: Provisionierung ohne Agent
REMOTE_WSMAN_HOST	Einstellungen: Provisionierung ohne Agent
REPLICATION_LANGUAGE	Verteilung: Replikation
REPLICATION_PLATFORM	Verteilung: Replikation
REPLICATION_SCHEDULE	Verteilung: Replikation
REPLICATION_SHARE	Verteilung: Replikation
REPORT_FIELD	Berichterstellung
REPORT_FIELD_GROUP	Berichterstellung
REPORT_JOIN	Berichterstellung
REPORT_OBJECT	Berichterstellung
REPORT_OBJECT_JOIN	Berichterstellung
REPORT_SCHEDULE	Berichterstellung
SAM_CATALOG_FILTER	Inventar: Softwarekatalog
SAM_CATALOG_LABEL_JT	Inventar: Softwarekatalog
SAM_COMPLIANCE_DETAIL	Asset Management: Lizenz-Compliance
SAM_COMPLIANCE_SUMMARY	Asset Management: Lizenz-Compliance
SAM_COUNT	Inventar: Softwarekatalog
SAM_MACHINE_JT	Inventar: Softwarekatalog
SAM_MACHINE_TERMINATED_APPS	Inventar: Softwarekatalog
SAM_METER	Inventar: Softwarekatalog
SAM_METER_DATA	Inventar: Softwarekatalog

Tabelle	Komponente
SAM_METER_TITLED_APPLICATION	Inventar: Softwarekatalog
SAM_NOT_ALLOWED	Inventar: Softwarekatalog
SAVED_SEARCH	Appliance-Administration
SCAN_FILTER	Inventar: Erkennung
SCAN_SETTINGS	Inventar: Erkennung
SCAP_BENCHMARK	Sicherheit: SCAP
SCAP_GROUP	Sicherheit: SCAP
SCAP_PROFILE	Sicherheit: SCAP
SCAP_RESULT	Sicherheit: SCAP
SCAP_RESULT_RULE	Sicherheit: SCAP
SCAP_RESULT_SCORE	Sicherheit: SCAP
SCAP_RULE	Sicherheit: SCAP
SCAP_RULE_IDENT	Sicherheit: SCAP
SETTINGS	Einstellungen
SETTINGS_HISTORY	Einstellungen: Verlauf
SETTINGS_HISTORY_CONFIGURATION	Einstellungen: Verlauf
SETTINGS_HISTORY_FIELD_DEFINITION	Einstellungen: Verlauf
SMARTY_REPORT	Berichterstellung
SNMP_INVENTORY_OIDS	Inventar: SNMP
SNMP_INVENTORY_SETTINGS	Inventar: SNMP
SNMP_INVENTORY_SETTINGS_JT	Inventar: SNMP
SNOOZE_ALERT	Patch-Zeitpläne
SOFTWARE	Inventar: Software
SOFTWARE_LABEL_JT	Inventar: Software

Tabelle	Komponente
SOFTWARE_OS_JT	Inventar: Software
STARTUPPROGRAM	Inventar: Startprogramme
STARTUPPROGRAM_LABEL_JT	Inventar: Startprogramme
THROTTLE	Appliance-Administration
USER	Einstellungen: Benutzer
USERIMPORT_SCHEDULE	Einstellungen: Benutzerauthentifizierung
USER_AUTO_REFRESH	Einstellungen: Benutzer
USER_HISTORY	Einstellungen: Benutzer
USER_KEYS	Einstellungen: Benutzer
USER_LABEL_JT	Einstellungen: Benutzer
USER_ROLE	Einstellungen: Benutzer
USER_ROLE_PERMISSION_VALUE	Einstellungen: Benutzer

Datenbanktabellen auf Systemebene (KBSYS)

In der folgenden Tabelle sind die Namen der Datenbanktabellen auf Systemebene (KBSYS) aufgeführt. Verwenden Sie diese Tabellennamen, wenn Sie benutzerdefinierte Berichte mithilfe von SQL-Abfragen erstellen. Siehe Berichte mithilfe von SQL-Abfragen erstellen.

KBSYS-Datenbanktabellen und -Komponenten

Tabelle	Komponente
ACCESS_STATS	Appliance-Administration (zum Nachverfolgen von Seitenansichten)
AGENTLESS_TASK	Inventar
APPLE_MODEL	Inventar: Geräte
AUTHENTICATION	Einstellungen: Benutzer
CLIENT_CRASH	Appliance-Administration
COUNTRYCODE_MAPPING	Inventar: Geräte (verwendet für Dell Geräte)
CREDENTIAL_CONSUMER	Einstellungen: Anmeldeinformationen
DASHBOARD	Dashboard

Tabelle	Komponente
DASHBOARD_BASE_WIDGETS	Dashboard
DASHBOARD_CACHE	Dashboard
DASHBOARD_CUSTOM_WIDGETS	Dashboard
DASHBOARD_DATASOURCES	Dashboard
DASHBOARD_WIDGET_TYPES	Dashboard
DELL_CATALOG	Sicherheit: Dell Aktualisierungen
DELL_CRITICALITY	Sicherheit: Dell Aktualisierungen
DELL_ERROR_CODE	Sicherheit: Dell Aktualisierungen
DELL_PKG	Sicherheit: Dell Aktualisierungen
DELL_PKG_DEVICE	Sicherheit: Dell Aktualisierungen
DELL_PKG_DEVICE_DEPENDENCY	Sicherheit: Dell Aktualisierungen
DELL_PKG_DEVICE_PCI	Sicherheit: Dell Aktualisierungen
DELL_PKG_DEVICE_PNP	Sicherheit: Dell Aktualisierungen
DELL_PKG_DEVICE_VERSION	Sicherheit: Dell Aktualisierungen
DELL_PKG_OS	Sicherheit: Dell Aktualisierungen
DELL_PKG_OS_LANG	Sicherheit: Dell Aktualisierungen
DELL_PKG_SYSTEM	Sicherheit: Dell Aktualisierungen
DELL_RESOURCE	Sicherheit: Dell Aktualisierungen
DELL_SUPPORTED_MODELS	Sicherheit: Dell Aktualisierungen
DELL_UPDATE_STATUS	Sicherheit: Dell Aktualisierungen
GLOBAL_OPTIONS	Appliance-Administration
GRID_COLUMNS_BASE	Appliance-Administration
GRID_COLUMNS_OVERRIDES	Appliance-Administration
HD_EMAIL_EXCLUSION	Service Desk: E-Mail-Ausschlussliste

Tabelle	Komponente
HISTORY_FIELD_VALUE_LABEL_MAP	Einstellungen: Verlauf
IM_CRON	Appliance-Administration (für geplante Prozesse)
INVENTORY	Inventar
INVENTORY_FAILURES	Inventar
KBOT_GRAMMAR	Skripterstellung
KBOT_GRAMMAR_ATTRIBUTE	Skripterstellung
KBOT_UPLOAD_TOKENS	Skripterstellung
K1000	Skripterstellung
KBOX_VERSION	Skripterstellung
KONDUCTOR_TASK	Appliance-Administration
KUID_MACHINE	Appliance-Administration
KUID_ORGANIZATION	Appliance-Administration
LICENSE_MODE	Appliance-Administration
LINKED_APPLIANCE	Einstellungen: Appliance-Verknüpfung
LINKED_USER_TOKEN	Einstellungen: Appliance-Verknüpfung
LOCALE_BROWSER	Appliance-Administration
LOCALE_COLLATION_RULES	Appliance-Administration
LOCALE_SERVER	Appliance-Administration
LOCALE_TIME_FORMAT	Appliance-Administration
MSI_ERROR_CODES	Verteilung
NETWORK_SETTINGS	Appliance-Administration
ORGANIZATION	Organisationen
ORGANIZATION_FILTER	Organisationen: Filter
ORGANIZATION_FILTER_CRITERIA	Organisationen: Filter

Tabelle	Komponente
ORGANIZATION_FILTER_CRITERIA_LDAP	Organisationen: Filter
ORG_ROLE	Organisationen: Rollen
ORG_ROLE_PERMISSION_VALUE	Organisationen: Rollen
OS_FAMILY	Inventar: Geräte
OVAL_DEFINITION	Sicherheit: OVAL
OVAL_UPDATE_STATUS	Sicherheit: OVAL
PATCH_ATTRIBUTE	Sicherheit: Patch-Verwaltung
PATCH_CATALOG_RUN_STATUS	Sicherheit: Patch-Verwaltung
PATCH_CATALOG_UPDATE_STATUS	Sicherheit: Patch-Verwaltung
PATCH_ERROR_CODE	Sicherheit: Patch-Verwaltung
PATCH_LANGUAGE	Sicherheit: Patch-Verwaltung
PATCH_OS	Sicherheit: Patch-Verwaltung
PATCH_PACKAGE	Sicherheit: Patch-Verwaltung
PATCH_PAYLOAD_DOWNLOAD_STATUS	Sicherheit: Patch-Verwaltung
PATCH_PRODUCT	Sicherheit: Patch-Verwaltung
PATCH_PRODUCT_JT	Sicherheit: Patch-Verwaltung
PATCH_PRODUCT_OS_JT	Sicherheit: Patch-Verwaltung
PATCH_PRODUCT_TITLED_APPLICATION_JT	Sicherheit: Patch-Verwaltung
PATCH_PRODUCT_TITLED_SUITE_JT	Sicherheit: Patch-Verwaltung
PATCH_RESOURCE	Sicherheit: Patch-Verwaltung
PATCH_SUPERCEDES_JT	Sicherheit: Patch-Verwaltung
PERMISSION_DEFINITION	Einstellungen: Rollen
PORT_SERVICES	Inventar: Erkennung
PROVISIONING_ERRORS	Einstellungen: Provisionierung

Tabelle	Komponente
REPORT_FIELD	Berichterstellung
REPORT_FIELD_GROUP	Berichterstellung
REPORT_JOIN	Berichterstellung
REPORT_OBJECT	Berichterstellung
REPORT_OBJECT_JOIN	Berichterstellung
REPORT_SCHEDULE	Berichterstellung
RESOURCE_EXPORTED	Einstellungen: Ressourcen
RESOURCE_QUEUE	Einstellungen: Ressourcen
SAM_APPLICATION	Softwarekatalog
SAM_HARDWARE	Softwarekatalog
SAM_LINUX_APPLICATION	Softwarekatalog
SAM_MUI_CACHE_DATA	Softwarekatalog
SAM_PUBLISHER	Softwarekatalog
SAM_SOFTWARE_TAG	Softwarekatalog
SAM_TITLE_REQUEST	Softwarekatalog
SAM_VIEW_ALL_SOFTWARE	Softwarekatalog
SAM_VIEW_DISCOVERED_APPLICATIONS	Softwarekatalog
SAM_VIEW_DISCOVERED_SOFTWARE	Softwarekatalog
SAM_VIEW_DISCOVERED_SUITES	Softwarekatalog
SAM_VIEW_INVENTORY_ADD_REMOVE_ PROGRAMS	Softwarekatalog
SAM_VIEW_INVENTORY_MOBILE_APPS	Softwarekatalog
SAM_VIEW_MACHINE_DISCOVERED_SOFTWARE	Softwarekatalog
SAM_VIEW_TITLED_SOFTWARE	Softwarekatalog

Tabelle	Komponente
SERVER_CRASH	Appliance-Administration (zum Nachverfolgen von internen Fehlern)
SERVICE_LEVEL_MAPPING	Inventar: Geräte (verwendet für Dell Geräte)
SETTINGS	Einstellungen
SETTINGS_HISTORY	Einstellungen: Verlauf
SETTINGS_HISTORY_CONFIGURATION	Einstellungen: Verlauf
SETTINGS_HISTORY_FIELD_DEFINITION	Einstellungen: Verlauf
SHAPING_METADATA	Inventar: API
SMARTY_REPORT	Berichterstellung
SMMP_CONNECTION	Erkennung
SMMP_CONNECTION_PLUGIN_JT	Erkennung
SMMP_MSG_Q	Erkennung
SMMP_NIC	Erkennung
SMMP_PLUGIN	Erkennung
SOFTWARE_INVENTORY	Inventar
SOFTWARE_INVENTORY_FAILURES	Inventar
SSL_CERT	Einstellungen: Sicherheitseinstellungen
SSL_CSR	Einstellungen: Sicherheitseinstellungen
SSL_PRIVATEKEY	Einstellungen: Sicherheitseinstellungen
SYSTEM_DEFINED_ROLES	Organisationen: Rollen
TIME_SETTINGS	Einstellungen: Datum- und Uhrzeiteinstellungen
USER	Einstellungen: Authentifizierung
USER_AUTH	Einstellungen: Authentifizierung
USER_AUTO_REFRESH	Einstellungen: Authentifizierung

Hinzufügen von Schritten zu Aufgabenbereichen von Skripten

Sie können in der Skripterstellungskomponente Skripten Schritte hinzufügen.

In den folgenden Tabellen sind die Schritte aufgeführt, die den Aufgabenbereichen von Skripten hinzugefügt werden können. Die Aufgabenabschnitte sind auf der Seite *Skriptdetail* verfügbar, wenn Sie eine Aufgabe hinzufügen. Siehe Hinzufügen und Bearbeiten von Skripten.

Die Spaltenüberschriften *Ü*, *E*, *W*, *WHS* und *WHF* geben an, ob ein bestimmter Schritt in den entsprechenden Aufgabenbereichen verfügbar ist: *Überprüfen*, *Erfolg*, *Wiederherstellung*, *Wiederherstellungserfolg* und *Wiederherstellungsfehler*.

- Schritte für Windows Geräte
- Schritte für Mac OS X Geräte
- Schritte für Red Hat Enterprise Linux Geräte

Schritte für Windows Geräte

HINWEIS: Die bei der Angabe von Registrierungspfaden zu verwendende Syntax finden Sie unter Angeben von Windows Registrierungspfaden.

Hinzufügen von Schritten zu auf Windows-Geräten verwendeten Skripten

Schritt	Beschreibung	V	Betriebssystem	R	WHS	WHF
Immer Fehler		X		X		
Benutzerdefinierte DLL-Funktion aufrufen	Funktion "%{procName}" aus "%{path}\%{file}" aufrufen.	X	X	X		
Benutzerdefiniertes DLL-Objekt erstellen	Objekt "%{className}" aus "%{path}\%{file}" erstellen.	X	X	X		
Nachrichtenfenster erstellen	Nachrichtenfenster mit der Bezeichnung "%{name}", dem Titel "%{title}", der Nachricht "%{message}" und dem Timeout "%{timeout}" Sekunden erstellen.	X	X	X	X	X

Schritt	Beschreibung	V	Betriebssystem	R	WHS	WHF
Registrierungsschlüssel löschen	"%{key}" aus Registrierung löschen. Siehe Angeben von Windows Registrierungspfaden.	X	X	X		
Registrierungswert löschen	"%{key}! %{name}" aus Registrierung löschen. Siehe Angeben von Windows Registrierungspfaden.	X	X	X		
Nachrichtenfenster löschen	Nachrichtenfenster mit der Bezeichnung "%{name}" löschen.	X	X	X	X	X
Anwendungspaket installieren	"%{name}" mit den Argumenten "%{install_cmd}" installieren.	X	X	X		

Schritt	Beschreibung	V	Betriebssystem	R	WHS	WHF
	HINWEIS: In diesem Schritt müssen Sie mithilfe der Funktion auf der Seite *Inventar* > *Software* Anwendungen aus einer Liste bereits hochgeladener Anwendungspakete auswählen. Siehe Hinzufügen und Löschen von Anwendungen im Inventar der Seite "Software".					
Prozess beenden	Den Prozess "%{name}" beenden.	X	X	X	X	X
Programm starten	"%{path}\%{program}" mit Parameter "%{parms}" starten.	X	X	X	X	X
Registrierungswert protokollieren	"%{key}!%{name}" protokollieren.			X		
Dateiinformationen protokollieren	"%{attrib}" wird aus ""%{path}\%{file}" protokolliert.			X	X	X

Schritt	Beschreibung	V	Betriebssystem	R	WHS	WHF
Nachricht protokollieren	"%{message}" in "%{type}" protokollieren.			X		
Dienst neu starten	Dienst "%{name}" neu starten			X		
Batchdatei ausführen	Batchdatei "%{_fake_name}" mit den Parametern "%{parms}" ausführen. **HINWEIS:** In diesem Schritt müssen Sie die Batch-Datei nicht hochladen. Sie erstellen die Batch-Datei, indem Sie das Skript an die vorgegebene Stelle kopieren.	X	X	X		
Registrierungsschlüssel setzen	"%{key}" festlegen.	X	X			
Registrierungswert setzen	"%{key}! %{name}" auf "%{newValue}" festlegen.	X	X			
Dienst starten	Dienst "%{name}" neu starten.			X		
Dienst beenden	Dienst "%{name}" beenden			X		

Schritt	Beschreibung	V	Betriebssystem	R	WHS	WHF
Datei entpacken	"%{path}\%{file}" nach "%{target}" entpacken.	X		X	X	X
Text im Nachrichtenfenster aktualisieren	Text im Nachrichtenfenster mit der Bezeichnung "%{name}" auf "%{text}" festlegen.	X		X	X	X
Zeitplan für Richtlinie und Job aktualisieren	Zeitplan für Richtlinie und Job über die Appliance aktualisieren.	X				
Datei hochladen	"%{path}\%{file}" auf den Server hochladen.		X	X		
Überprüfen, ob ein Verzeichnis vorhanden ist	Überprüfen, ob das Verzeichnis "%{path}" existiert.	X				
Überprüfen, ob eine Datei vorhanden ist	Überprüfen, ob die Datei "%{path}\%{file}" vorhanden ist.	X				
Überprüfen, ob eine Dateiversion exakt ... entspricht	Überprüfen, ob die Datei "%{path}\%{file}" die Version "%{expectedValue}" aufweist.	X				
Überprüfen, ob eine Dateiversion größer als ... ist	Überprüfen, ob die Version der Datei "%{path}\%{file}" größer ist als "%{expectedValue}".	X				

Schritt	Beschreibung	V	Betriebssystem	R	WHS	WHF
Überprüfen, ob eine Dateiversion größer als oder gleich ... ist	Überprüfen, ob die Version der Datei "%{path}\%{file}" größer oder gleich "%{expectedValue}" ist.	X				
Überprüfen, ob eine Dateiversion kleiner als ... ist	Überprüfen, ob die Version der Datei "%{path}\%{file}" kleiner ist als "%{expectedValue}".	X				
Überprüfen, ob eine Dateiversion kleiner als oder gleich ... ist	Überprüfen, ob die Version der Datei "%{path}\%{file}" kleiner oder gleich "%{expectedValue}" ist.	X				
Bestätigen, dass eine Dateiversion nicht ... entspricht	Überprüfen, ob die Datei "%{path}\%{file}" nicht die Version "%{expectedValue}" aufweist.	X				
Überprüfen, ob eine Datei geändert wurde seit	Überprüfen, ob die Datei "%{path}\%{file}" seit "%{expectedValue}" geändert wurde.	X				
Bestätigen, dass ein Prozess nicht ausgeführt wird	Überprüfen, ob der Prozess "%{name}" nicht ausgeführt wird.	X				

Schritt	Beschreibung	V	Betriebssystem	R	WHS	WHF
Überprüfen, ob ein Prozess ausgeführt wird	Überprüfen, ob der Prozess "%{name}" ausgeführt wird.	X				
Überprüfen, ob eine Produktversion exakt ... entspricht	Überprüfen, ob das Produkt "%{path}\%{file}" die Version "%{expectedValue}" aufweist.	X				
Überprüfen, ob eine Produktversion größer als ... ist	Überprüfen, ob die Version des Produkts "%{path}\%{file}" größer ist als "%{expectedValue}".	X				
Überprüfen, ob eine Produktversion größer als oder gleich ... ist	Überprüfen, ob die Version des Produkts "%{path}\%{file}" größer oder gleich "%{expectedValue}" ist.	X				
Überprüfen, ob eine Produktversion kleiner als ... ist	Überprüfen, ob die Version des Produkts "%{path}\%{file}" kleiner ist als "%{expectedValue}".	X				
Überprüfen, ob eine Produktversion kleiner als oder gleich ... ist	Überprüfen, ob die Version des Produkts "%{path}\%{file}" kleiner oder gleich "%{expectedValue}" ist.	X				

Schritt	Beschreibung	V	Betriebssystem	R	WHS	WHF
Bestätigen, dass eine Produktversion nicht ... entspricht	Überprüfen, ob das Produkt "%{path}\%{file}" nicht die Version "%{expectedValue}" aufweist.	X				
	HINWEIS: Die bei der Angabe von Registrierungspfaden zu verwendende Syntax finden Sie unter Angeben von Windows Registrierungspfaden.					
Bestätigen, dass ein Registrierungsschlüssel nicht vorhanden ist	Überprüfen, ob "%{key}" nicht existiert.	X				
Überprüfen, ob ein Registrierungsschlüssel vorhanden ist	Überprüfen, ob "%{key}" existiert.	X				
Überprüfen, ob das Unterschlüsselvolumen eines Registrierungswertes exakt ... entspricht	Überprüfen, ob "%{key}" genau "%{expectedValue}" Unterschlüssel hat.	X				
Überprüfen, ob das Unterschlüsselvolumen eines Registrierungswertes größer als ... ist	Überprüfen, ob "%{key}" mehr als "%{expectedValue}" Unterschlüssel hat.	X				
Überprüfen, ob das Unterschlüsselvolumen eines Registrierungswertes größer als oder gleich ... ist	Überprüfen, ob "%{key}" mindestens "%{expectedValue}" Unterschlüssel hat.	X				

Schritt	Beschreibung	V	Betriebssystem	R	WHS	WHF
Überprüfen, ob das Unterschlüsselvolumen eines Registrierungswerts kleiner als ... ist	Überprüfen, ob "%{key}" weniger als "%{expectedValue}" Unterschlüssel hat.	X				
Überprüfen, ob das Unterschlüsselvolumen eines Registrierungswerts kleiner als oder gleich ... ist	Überprüfen, ob "%{key}" höchstens "%{expectedValue}" Unterschlüssel hat.	X				
Bestätigen, dass das Unterschlüsselvolumen eines Registrierungswerts nicht ... entspricht	Überprüfen, ob "%{key}" nicht genau "%{expectedValue}" Unterschlüssel hat.	X				
Überprüfen, ob das Wertvolumen eines Registrierungswerts exakt ... entspricht	Überprüfen, ob "%{key}" genau "%{expectedValue}" Werte aufweist.	X				
Überprüfen, ob das Wertvolumen eines Registrierungswerts größer als ... ist	Überprüfen, ob "%{key}" mehr als "%{expectedValue}" Werte aufweist.	X				
Überprüfen, ob das Wertvolumen eines Registrierungswerts größer als oder gleich ... ist	Überprüfen, ob "%{key}" mindestens "%{expectedValue}" Werte aufweist.	X				
Überprüfen, ob das Wertvolumen eines Registrierungswerts	Überprüfen, ob "%{key}" weniger als "%{expectedValue}"	X				

Schritt	Beschreibung	V	Betriebssystem	R	WHS	WHF
kleiner als ... ist	Werte aufweist.					
Überprüfen, ob das Wertvolumen eines Registrierungswerts kleiner als oder gleich ... ist	Überprüfen, ob "%{key}" höchstens "%{expectedValue}" Werte aufweist.	X				
Bestätigen, dass das Wertvolumen eines Registrierungswerts nicht ... entspricht	Überprüfen, ob "%{key}" nicht genau "%{expectedValue}" Werte aufweist.	X				
Bestätigen, dass ein Registrierungsmerkmal nicht übereinstimmt	Überprüfen, ob "%{key}!%{name}= %{expectedValue}" nicht übereinstimmt.	X				
Übereinstimmung eines Registrierungsmerkmals überprüfen	Überprüfen, ob "%{key}!%{name}= %{expectedValue}" übereinstimmt.	X				
Bestätigen, dass ein Registrierungswert nicht vorhanden ist	Überprüfen, ob "%{key}!%{name}" nicht existiert.	X				
Überprüfen, ob ein Registrierungswert vorhanden ist	Überprüfen, ob "%{key}!%{name}" existiert.	X				
Überprüfen, ob ein Registrierungswert exakt ... entspricht	Überprüfen, ob "%{key}!%{name}" gleich "%{expectedValue}" ist.	X				
Überprüfen, ob ein Registrierungswert	Überprüfen, ob "%{key}!%{name}"	X				

Schritt	Beschreibung	V	Betriebssystem	R	WHS	WHF
größer als ... ist	größer ist als "%{expectedValue}".					
Überprüfen, ob ein Registrierungswert größer als oder gleich ... ist	Überprüfen, ob "%{key}!%{name}" größer oder gleich "%{expectedValue}" ist.	X				
Überprüfen, ob ein Registrierungswert kleiner als ... ist	Überprüfen, ob "%{key}!%{name}" kleiner ist als "%{expectedValue}".	X				
Überprüfen, ob ein Registrierungswert kleiner als oder gleich ... ist	Überprüfen, ob "%{key}!%{name}" kleiner oder gleich "%{expectedValue}" ist.	X				
Bestätigen, dass ein Registrierungswert nicht ... entspricht	Überprüfen, ob "%{key}!%{name}" nicht gleich "%{expectedValue}" ist.	X				
Überprüfen, ob ein Dienst vorhanden ist	Überprüfen, ob der Dienst "%{name}" existiert.	X				
Überprüfen, ob ein Dienst ausgeführt wird	Überprüfen, ob der Dienst "%{name}" ausgeführt wird.	X				

Angeben von Windows Registrierungspfaden

Verwenden Sie bei der Angabe von Windows Registrierungspfaden den Basisschlüssel und geben Sie an, ob sich die Registrierung auf einem Gerät mit 32-Bit- oder 64-Bit-Betriebssystem und -Hardware befindet.

Base key	Short version
HKEY_CLASSES_ROOT	HKCR
HKEY_CURRENT_USER	HKCU
HKEY_LOCAL_MACHINE	HKLM

HKEY_USERS	HKU
HKEY_PERFORMANCE_DATA	HKPD
HKEY_PERFORMANCE_TEXT	HKPT
HKEY_PERFORMANCE_NLSTEXT	HKPN
HKEY_CURRENT_CONFIG	HKCC
HKEY_DYN_DATA	HKDD

Geben Sie beispielsweise den Pfad für HKEY_LOCAL_MACHINE auf Geräten mit 32- bzw. 64-Bit-Versionen von Windows wie folgt an:

- `HKLM\Software\32BitProgramA\installDate`
- `HKLM64\Software\64BitProgramB\installDate`

Schritte für Mac OS X Geräte

Hinzufügen von Schritten zu auf Mac OS X Geräten verwendeten Skripten

Schritt	Beschreibung	V	Betriebssystem	R	WHS	WHF
Immer Fehler		X		X		
Nachrichtenfenster erstellen	Nachrichtenfenster mit der Bezeichnung "%{name}", dem Titel "%{title}", der Nachricht "%{message}" und dem Timeout "%{timeout}" Sekunden erstellen.	X	X	X	X	X
Nachrichtenfenster löschen	Nachrichtenfenster mit der Bezeichnung "%{name}" löschen.	X	X	X	X	X
Prozess beenden	Den Prozess "%{name}" beenden.	X	X	X	X	X
Programm starten	"%{path}\%{program}" mit Parameter "%{parms}" starten.	X	X	X	X	X

Schritt	Beschreibung	V	Betriebssystem	R	WHS	WHF
PLIST-Wert protokollieren	"%{key}! %{name};" protokollieren			X		
Nachricht protokollieren	"%{message}" in "%{type}" protokollieren.			X		
Dateisystem durchsuchen	Nach "%{name}" in "%{startingDirectory}" unter "%{drives}" und "%{action}" suchen.	X				
Datei entpacken	"%{path}\ %{file}" nach "%{target}" entpacken.	X		X	X	X
Text im Nachrichtenfenster aktualisieren	Text im Nachrichtenfenster mit der Bezeichnung "%{name}" auf "%{text}" festlegen.	X		X	X	X
Zeitplan für Richtlinie und Job aktualisieren	Zeitplan für Richtlinie und Job über die Appliance aktualisieren.	X				
Datei hochladen	"%{path}\ %{file}" auf den Server hochladen.		X	X		
Überprüfen, ob ein Verzeichnis vorhanden ist	Überprüfen, ob das Verzeichnis "%{path}" existiert.	X				
Überprüfen, ob eine Datei vorhanden ist	Überprüfen, ob die Datei "%{path}\ %{file}" vorhanden ist.	X				

Schritt	Beschreibung	V	Betriebssystem	R	WHS	WHF
Überprüfen, ob eine Datei geändert wurde seit	Überprüfen, ob die Datei "%{path}\%{file}" seit "%{expectedValue}" geändert wurde.	X				
Bestätigen, dass ein Prozess nicht ausgeführt wird	Überprüfen, ob der Prozess "%{name}" nicht ausgeführt wird.	X				
Überprüfen, ob ein Prozess ausgeführt wird	Überprüfen, ob der Prozess "%{name}" ausgeführt wird.	X				
Überprüfen, ob ein PLIST-Wert ... entspricht		X				
Überprüfen, ob ein PLIST-Wert vorhanden ist	Überprüfen, ob "%{key}" existiert.	X				
Überprüfen, ob ein PLIST-Wert größer als ... ist		X				
Überprüfen, ob ein PLIST-Wert kleiner als ... ist		X				
Überprüfen, ob eine Umgebungsvariable ... entspricht		X				
Überprüfen, ob eine Umgebungsvariable vorhanden ist		X				
Überprüfen, ob eine		X				

Schritt	Beschreibung	V	Betriebssystem	R	WHS	WHF
Umgebungsvariable größer als ... ist						
Überprüfen, ob eine Umgebungsvariable kleiner als ... ist		X				
Überprüfen, ob mindestens eine Dateiübereinstimmung mit regex vorhanden ist		X				
Überprüfen, ob Anzahl der Dateinamenübereinstimmungen mit regex größer als ... ist		X				
Überprüfen, ob Anzahl der Dateinamenübereinstimmungen mit regex kleiner als ... ist		X				
Überprüfen, ob Anzahl der Dateinamenübereinstimmungen mit regex ... entspricht		X				
Überprüfen, ob Dateiinfo ... entspricht		X				
Überprüfen, ob Dateiinfo größer als ... ist		X				
Überprüfen, ob Dateiinfo kleiner als ... ist		X				

Schritte für Red Hat Enterprise Linux Geräte

Hinzufügen von Schritten zu Skripten für RHEL

Schritt	Beschreibung	V	Betriebssystem	R	WHS	WHF
Immer Fehler		X		X		
Prozess beenden	Den Prozess "%{name}" beenden.	X	X	X	X	X
Programm starten	"%{path}\%{program}" mit Parameter "%{parms}" starten.	X	X	X	X	X
Nachricht protokollieren	"%{message}" in "%{type}" protokollieren.			X		
Dateisystem durchsuchen	Nach "%{name}" in "%{startingDirectory}" unter "%{drives}" und "%{action}" suchen.	X				
Datei entpacken	"%{path}\%{file}" nach "%{target}" entpacken.	X		X	X	X
Zeitplan für Richtlinie und Job aktualisieren	Zeitplan für Richtlinie und Job über die Appliance aktualisieren.	X				
Datei hochladen	"%{path}\%{file}" auf den Server hochladen.		X	X		
Überprüfen, ob ein Verzeichnis vorhanden ist	Überprüfen, ob das Verzeichnis "%{path}" existiert.	X				

Schritt	Beschreibung	V	Betriebssystem	R	WHS	WHF
Überprüfen, ob eine Datei vorhanden ist	Überprüfen, ob die Datei "%{path}\%{file}" vorhanden ist.	X				
Überprüfen, ob eine Datei geändert wurde seit	Überprüfen, ob die Datei "%{path}\%{file}" seit "%{expectedValue}" geändert wurde.	X				
Bestätigen, dass ein Prozess nicht ausgeführt wird	Überprüfen, ob der Prozess "%{name}" nicht ausgeführt wird.	X				
Überprüfen, ob ein Prozess ausgeführt wird	Überprüfen, ob der Prozess "%{name}" ausgeführt wird.	X				
Überprüfen, ob eine Umgebungsvariable kleiner als ... ist		X				
Überprüfen, ob mindestens eine Dateiübereinstimmung mit regex vorhanden ist		X				
Überprüfen, ob Anzahl der Dateinamenübereinstimmungen mit regex größer als ... ist		X				
Überprüfen, ob Anzahl der		X				

Schritt	Beschreibung	V	Betriebssystem	R	WHS	WHF
Dateinamenübereinstimmungen mit regex kleiner als ... ist						
Überprüfen, ob Anzahl der Dateinamenübereinstimmungen mit regex ... entspricht		X				
Überprüfen, ob Dateiinfo ... entspricht		X				
Überprüfen, ob Dateiinfo größer als ... ist		X				
Überprüfen, ob Dateiinfo kleiner als ... ist		X				

LDAP-Variable

Die Appliance unterstützt Variablen für die Verwendung in LDAP-Labels und -Datenbankabfragen.

Geräte- oder Computervariablen

Geräte- oder Computervariablen können in LDAP-Labels und -Abfragen verwendet werden, um Geräte automatisch nach Name, Beschreibung und anderen LDAP-Kriterien zu gruppieren. Während der LDAP-Label-Verarbeitung ersetzt die Appliance alle als `KBOX_` definierten Variablen durch ihre entsprechenden Laufzeitwerte. Die folgende Tabelle zeigt die unterstützten Geräte- oder Computervariablen sowie ihre Zuordnung zu den Spalten in der Datenbanktabelle „MACHINE“ sowie zu den LDAP-Attributen.

Geräte- oder Computervariablen und -zuordnungen

Appliance-Variable	Spalte der Appliance-Datenbanktabelle MACHINE	LDAP-Attributzuordnung
KBOX_COMPUTER_NAME	NAME	cn | name
KBOX_COMPUTER_DESCRIPTION	Systembeschreibung	Beschreibung
KBOX_COMPUTER_MAC	MAC	macAddress
KBOX_COMPUTER_IP	IP	ipHostNumber

Appliance-Variable	Spalte der Appliance-Datenbanktabelle MACHINE	LDAP-Attributzuordnung
KBOX_USER	USER_NAME	
KBOX_USER_DOMAIN	USER_DOMAIN	
KBOX_DOMAINUSER	USER	
KBOX_CUSTOM_INVENTORY_*	CUSTOM_INVENTORY	

Die Variable „KBOX_CUSTOM_INVENTORY_*“ kann verwendet werden, um den Wert einer benutzerdefinierten Inventarisierung zu prüfen. Das Sternchen (*) wird durch den Anzeigenamen der Regel für benutzerdefinierte Inventarisierung ersetzt. Die zulässigen Zeichen sind [a-z0-9.-]. Alle anderen Zeichen werden durch einen Unterstrich (_) ersetzt.

Benutzervariablen

Benutzervariablen können in LDAP-Labels und -Abfragen verwendet werden, um Benutzer automatisch nach Domain, Standort, Budgetcode oder anderen LDAP-Kriterien zu gruppieren. Während der LDAP-Label-Verarbeitung ersetzt die Appliance alle als `KBOX_` definierten Variablen durch ihre entsprechenden Laufzeitwerte. Die folgende Tabelle zeigt die unterstützten Benutzervariablen und ihre Zuordnung zu den Spalten in der Datenbanktabelle „USER“ sowie zu den LDAP-Attributen.

Benutzervariablen und -zuordnungen

Appliance-Variable	Spalte der Appliance-Datenbanktabelle USER	LDAP-Attributzuordnung
KBOX_USER_NAME	USER_NAME	samAccountName
KBOX_FULL_NAME	FULL_NAME	cn | name
KBOX_EMAIL	EMAIL	mail
KBOX_DOMAIN	DOMAIN	
KBOX_BUDGET_CODE	BUDGET_CODE	
KBOX_LOCATION	LOCATION	1
KBOX_WORK_PHONE	WORK_PHONE	telephoneNumber
KBOX_HOME_PHONE	HOME_PHONE	homePhone
KBOX_MOBILE_PHONE	MOBILE_PHONE	mobile
KBOX_PAGER_PHONE	PAGER_PHONE	pager
KBOX_CUSTOM_1	CUSTOM_1	
KBOX_CUSTOM_2	CUSTOM_2	

Appliance-Variable	Spalte der Appliance-Datenbanktabelle USER	LDAP-Attributzuordnung
KBOX_CUSTOM_3	CUSTOM_3	
KBOX_CUSTOM_4	CUSTOM_4	
KBOX_ROLE_ID	ROLE_ID	
KBOX_API_ENABLED	API_ENABLED	• Kein Wert: Deaktivieren des Benutzerzugriffs auf die KACE GO App
KBOX_AMS_ID	AMS_ID	Kein Wert. Diese Variable wird nicht verwendet.
KBOX_LOCALE_BROWSER_ID	LOCALE_BROWSER_ID	
KBOX_HD_DEFAULT_QUEUE_ID	HD_DEFAULT_QUEUE_ID	
KBOX_LDAP_UID	LDAP_UID	objectGUID

Glossar

A

Administratorkonsole

Die **Administratorkonsole** ist die webbasierte Oberfläche zur Steuerung der Appliance. Auf die **Administratorkonsole** können Sie unter `http://<appliance_hostname>/admin` zugreifen, wobei `<appliance_hostname>` der Hostname Ihrer Appliance ist. Wenn die Organisationskomponente aktiviert ist, können Sie über die **Administratorkonsole** unter `http://<appliance_hostname>/system` auf die Einstellungen auf Systemebene zugreifen. Um die vollständigen Pfade von URLs in der **Administratorkonsole** anzuzeigen, fügen Sie der URL, die Sie zur Anmeldung verwenden, ui hinzu. Dies kann nützlich sein, wenn Sie die Datenbank durchsuchen oder Links freigeben. Zum Beispiel: `http://appliance_hostname/admin`.

Agent

Der KACE Agent ist eine Anwendung, die auf Geräten installiert werden kann, um die Geräteverwaltung über die Appliance zu ermöglichen. Auf verwalteten Geräten installierte Agenten kommunizieren über das AMP (Agenten-Messaging-Protokoll) mit der Appliance. Agenten führen geplante Aufgaben durch, beispielsweise das Erfassen von Inventarinformationen auf verwalteten Geräten und das Verteilen von Software an verwaltete Geräte. Die Verwaltung ohne Agent ist bei Geräten verfügbar, auf denen die Agenten-Software nicht installiert werden kann, beispielsweise bei Druckern und Geräten mit vom Agenten nicht unterstützten Betriebssystemen. Siehe Provisionierung des KACE Agent.

alternative Download-Quelle

Eine alternative Download-Quelle kann jeder beliebige Netzwerkspeicherort sein, an dem sich alle erforderlichen Dateien zur Installation einer bestimmten Anwendung befinden. Sie können Pakete von alternativen Download-Quellen bereitstellen, beispielsweise von einer UNC-Adresse oder einer DFS-Quelle. Die CIFS- und SMB-Protokolle, Samba-Server und Dateiserver-Appliances werden unterstützt. Sie müssen den Speicherort angeben, wenn Sie eine verwaltete Installation erstellen. Siehe Verwenden verwalteter Installationen.

Anforderung "Zu Katalog hinzufügen"

Eine Katalogisierungsanforderung ist ein Formular, mit dem Sie anfordern können, dass eine nicht im Softwarekatalog enthaltene (nicht katalogisierte) Anwendung in den öffentlichen Softwarekatalog aufgenommen wird. Wenn Quest eine Katalogisierungsanforderung erhält, wird überprüft, ob die Anwendung in den öffentlichen Softwarekatalog aufgenommen werden soll. Außerdem werden Anwendungen, für die eine Katalogisierungsanforderung übermittelt wird, automatisch zur lokalen Version des Softwarekatalogs auf der Appliance hinzugefügt. Siehe Hinzufügen von Anwendungen zum Softwarekatalog.

Anwendungen von Drittanbietern

Anwendungen, die von Drittanbietern entwickelt und für die Verwendung in Quest KACE Produkten lizenziert wurde.

Anwendungssteuerung

Mit der Anwendungssteuerung können Sie Anwendungen als "Nicht zulässig" kennzeichnen und sie blockieren oder verhindern, dass diese Anwendungen auf vom Agenten verwalteten Windows- und Mac-Geräten ausgeführt werden. Dies ist hilfreich, wenn Sie die Ausführung spezifischer Anwendungen in Ihrer Umgebung einschränken möchten. Siehe Anwendungssteuerungslabel zu Geräten zuweisen.

App

Siehe KACE GO.

AppDeploy Live

Siehe ITNinja.

Appliance-Verknüpfung

Durch Appliance-Verknüpfung können Sie sich bei einer Appliance anmelden und über die Dropdown-Liste in der rechten oberen Ecke der **Administratorkonsole** auf alle verknüpften Appliances zugreifen, ohne dass Sie sich separat bei jeder Appliance anmelden müssen. Sie können alle Quest Appliances der K-Serie verknüpfen, die Sie verwalten. Siehe Verknüpfen von Quest KACE Appliances.

Appliances der KACE SDA Serie

Die K2000 Serie umfasst Systembereitstellungs-Appliances, die entwickelt wurden, um die Bereitstellung von Betriebssystemen (BS) vollständig zu automatisieren. Weitere Informationen zur KACE SMA Serie finden Sie auf der Website zu Quest unter https://quest.com/products/kace-systems-deployment-appliance/.

Appliances der Appliance-Serie

Die Appliance-Serie umfasst Systemverwaltungs-Appliances, die entwickelt wurden, um Systemverwaltungsaufgaben wie Anwendungsbereitstellung oder Asset Management vollständig zu automatisieren. Weitere Informationen zur Appliance-Serie finden Sie auf der Website zu Quest unter https://quest.com/products/kace-systems-management-appliance/.

Appliance oder Virtual Appliance

Die Appliance ist als physische oder hardwarebasierte Appliance und als virtuelle Appliance erhältlich. Die Virtual Appliance verwendet eine VMware Infrastruktur. Für die physische und die virtuelle Appliance stehen jeweils die gleichen Systemverwaltungsfunktionen zur Verfügung. Siehe Informationen zu Appliance-Komponenten.

Assets, Asset-Typen und Asset-Untertypen, die in der Asset Management-Komponente verwenden werden.

Zu den in der Asset Management-Komponente verwendeten Assets und Asset-Typen zählen physische und logische Elemente, beispielsweise Geräte, Anwendungen, Drucker, Lizenzen, Abteilungen, Standorte und Anbieter. Die Komponente Asset Management ermöglicht Ihnen die Herstellung von Beziehungen zwischen Assets, die Nachverfolgung von Inventardaten, das Anzeigen von Änderungsdatensätzen und die Erstellung von Berichten zu Veränderungen von Assets. Assets basieren auf Asset-Typen. Sie können nach Bedarf Standard-Asset-Typen ändern, benutzerdefinierte Asset-Typen erstellen sowie Asset-Informationen importieren. Siehe Informationen zu Asset-Typen. Asset-Untertypen sind Unterkategorien von Assets, die Sie zu jedem Asset-Typ hinzufügen können, einschließlich benutzerdefinierter Asset-Typen. So können Sie Untertypen von Assets, z. B. Geräte-Assets wie Computer, Drucker und Router sowie Software-Assets, die auf Windows, Mac oder Linux-Systemen im Appliance-Inventar ausgeführt werden, erkennen und verwalten. Siehe Informationen zu Asset-Untertypen, benutzerdefinierten Feldern und Gerätedetail-Voreinstellungen.

Assets, die auf das Lizenzlimit der Appliance angerechnet werden

Die Appliance-Lizenzvereinbarung berechtigt Sie zur Verwaltung einer bestimmten Anzahl an Geräten, die als Assets klassifiziert sind. Diese Assets unterscheiden sich von den in der Asset Management-Komponente verwendeten Assets. Zu den Assets, die auf das Lizenzlimit angerechnet werden, zählen Geräte, die 1) dem KACE SMA Inventar hinzugefügt wurden, aber nicht der Definition verwalteter Computer oder überwachter Server entsprechen, und 2) dem Inventar nicht manuell, über die WSAPI oder mithilfe der Verwaltung von Mobilgeräten hinzugefügt wurden. Beispiele für Assets: Drucker, Projektoren, Netzwerkausrüstung und Speichergeräte.

HINWEIS: Die mit der Asset Management-Komponente erstellten und verwalteten Assets werden nicht auf das Lizenzlimit angerechnet.

Siehe Produktlizenzinformationen anzeigen.

Asset Management

Unterstützung komplexer Lizenz-Compliance-Berichte, die auf dem Framework der über den Appliance-Inventarprozess gesammelten Daten aufbauen. Das Asset Management bietet Ihnen zudem die Möglichkeit, weitere Daten zu den verwalteten Geräten zu erfassen, einschließlich Bestelldatum, Support-Verträge, Asset-Kennungen usw. Siehe Informationen zur Komponente Asset Management.

Aufgabendurchsatz

Die Aufgabenlast auf der Appliance. Siehe Konductor.

AUP

Siehe Nutzungsrichtlinie.

Ausstehend

Computer oder Geräte, die von der Appliance verwaltet werden, jedoch nicht rechtzeitig inventarisiert wurden, werden als ausstehende Geräte (MIA, Missing in Action) bezeichnet. Siehe Verwalten ausstehender Geräte.

Automatische Labels

Labels, die automatisch angewendet werden, wie beispielsweise Smart Labels. Siehe Einrichten und Verwenden von Labels für die Verwaltung von Elementgruppen.

Ä

Änderungsverwaltung

Die Möglichkeit, Änderungen an Elementen in der **Administratorkonsole** nachzuverfolgen, beispielsweise an Skripten, Berichten, Assets und Einstellungen. Siehe Konfigurieren der Verlaufseinstellungen.

B

Bedrohungsstufen

Mithilfe von Bedrohungsstufen können Sie die relative Sicherheit von Elementen und die Anzahl der Geräte anzeigen, auf denen diese Elemente installiert sind. Diese Informationen dienen nur Nachverfolgungszwecken. Die Appliance erzwingt basierend auf den Bedrohungsstufen keine Richtlinien. Siehe Verwenden von Bedrohungsstufen und Kategorien für Software.

Befehlszeilenkonsole

Die **Befehlszeilenkonsole** ist ein Terminalfenster für die Appliance. Die Schnittstelle ist hauptsächlich für die Konfiguration der Appliance und die Richtlinienerzwingung gedacht, sofern auf die **Administratorkonsole** nicht zugegriffen werden kann. Siehe Einschalten der Appliance und Anmelden bei der Administratorkonsole.

Benachrichtigungen

Bei Benachrichtigungen handelt es sich um E-Mail-Nachrichten, die von der Appliance an Administratoren gesendet werden, wenn Geräte, Scan-Ergebnisse und Assets bestimmte Kriterien erfüllen. Sie können zum Beispiel E-Mail-Benachrichtigungen basierend auf der Datenträgernutzung einrichten, wenn Sie Administratoren benachrichtigen möchten, sobald ein bestimmtes Speicherlimit auf einem Datenträger erreicht ist. Die Benachrichtigungen werden gesendet, wenn die Geräte die angegebenen Kriterien erfüllen.

Die Appliance überprüft das Inventar anhand der Kriterien gemäß der in den Benachrichtigungszeitplänen angegebenen Häufigkeit. Wenn ein Element den Kriterien entspricht, sendet die Appliance eine E-Mail an die angegebenen Empfänger.

Nachrichten, die anhand von bestimmten Kriterien und zu festgelegten Intervallen per E-Mail versendet werden. Siehe Zeitplanung für Benachrichtigungen.

Benchmark

Bei einem SCAP-Benchmark handelt es sich um eine Prüfliste für die Sicherheitskonfiguration mit einer Reihe von Regeln zur Bewertung von Sicherheitslücken eines Geräts in einer bestimmten Betriebsumgebung. Das NIST (National Institute of Standards and Technology) verwaltet das National Checklist Repository, das verschiedene Prüflisten für Sicherheitskonfigurationen für bestimmte IT-Produkte sowie Kategorien von IT-Produkten enthält. Siehe Informationen zu Benchmarks.

Benutzerdownloads

Benutzerdownloads sind Software-Installationspakete, wie z. B. Druckertreiber und andere Anwendungen, die über die **Benutzerkonsole** an Benutzer verteilt werden. Siehe Verwalten von Benutzerdownloads.

Benutzerkonsole

Die **Benutzerkonsole** ist die webbasierte Oberfläche, die Benutzern Software, Skripte und andere herunterladbare Elemente auf Self-Service-Basis zur Verfügung stellt. Außerdem ermöglicht sie Benutzern den Zugriff auf Knowledge Base-Artikel und das Einsenden von Service Desk-Support-Tickets, mit denen sie Hilfe anfordern oder Fehler melden können. Sie können auf die **Benutzerkonsole** unter `http://<appliance_hostname>/user` zugreifen, wobei `<appliance_hostname>` der Hostname der Appliance ist. Siehe Informationen zum Service Desk.

Berichterstellung

Die Möglichkeit zur Sammlung von Informationen zu Hardware, Software und Lizenz-Compliance, aufgeschlüsselt nach Gerät. Sie können Standardberichte ausführen oder mithilfe eines Berichts-Assistenten, der Sie Schritt für Schritt durch den Erstellungsvorgang führt, benutzerdefinierte Berichte erstellen. Außerdem können Sie die automatische Ausführung von Berichten und deren Versand per E-Mail planen. Fortgeschrittene Benutzer können zudem unter Verwendung einer beliebigen ODBC (Open DataBase Connectivity)-kompatiblen Berichts-Engine Berichte anhand der Appliance-Datenbank erstellen. Siehe Verwenden von Berichten und Zeitplanung für Benachrichtigungen.

C

Charlie Root

Die E-Mail-Adresse für Benachrichtigungen, die von der Appliance versendet werden.

HINWEIS: Benachrichtigungen und tägliche Berichte werden von der Standardadresse "Charlie Root" (root@<appliance_hostname>) versendet. Diese Adresse kann nicht geändert werden.

Client-Drop-Speicherort

Beim Client-Drop-Speicherort handelt es sich um eine Dateifreigabe zum Hochladen großer Dateien, z. B. von Installationsprogrammen für Anwendungen und Appliance-Sicherungsdateien, auf die Appliance. Das Hochladen von Dateien auf den Client-Drop-Speicherort ist eine Alternative zum Hochladen von Dateien über die **Administratorkonsole** mit dem Standard-HTTP-Mechanismus, bei dem es bei großen Dateien zu Browser-Timeouts kommen kann. Siehe Dateien kopieren und auf dem Client-Drop-Speicherort der Appliance ablegen.

Clients

Siehe Geräte.

Computer

Computer sind eine Kategorie von Geräten, die von der Appliance verwaltet werden können. Beispiele für Computer sind Personalcomputer, Server, Laptops, Tablets und Smartphones. Mit Ihrer Appliance-Lizenzvereinbarung können Sie eine festgelegte Anzahl von Computern verwalten. Siehe Verwaltete Computer.

Computer

Siehe Geräte.

Computerfremde Geräte

Computerfremde Geräte sind Assets wie Drucker, Router, Netzwerkgeräte und andere Geräte, die nicht der Definition eines Computers entsprechen. Administratoren können Asset-Untertypen erstellen, um Informationen bestimmter computerfremder Geräte zu verfolgen. Siehe Informationen zu Asset-Untertypen, benutzerdefinierten Feldern und Gerätedetail-Voreinstellungen.

D

Dateisynchronisierungen

Mittels Dateisynchronisierungen können Sie Dateien an verwaltete Geräte verteilen. Im Gegensatz zu verwalteten Installationen werden bei Dateisynchronisierungen jedoch keine Dateien installiert, sondern lediglich verteilt. Mit Dateisynchronisierungen können Sie Dateien jedes Typs auf verwaltete Geräte kopieren. Siehe Dateisynchronisierungen erstellen und verwenden.

Datenaufbewahrung

Die Optionen zum Speichern von Nutzungserfassungsdaten, Gerätelaufzeiten, nicht katalogisierten Anwendungen und Sicherungen auf der Appliance. Siehe Allgemeine Einstellungen auf Verwaltungs- oder organisationsspezifischer Ebene konfigurieren und Zeitplan der täglichen Sicherung und die Anzahl der beizubehaltenden Sicherungen einrichten.

Datenfreigabe

Die Optionen für die Freigabe von Appliance-Informationen an Quest KACE. Siehe Konfigurieren der Datenfreigabeeinstellungen.

Dell Command | Monitor

Dell Command | Monitor ist das Überwachungstool der Dell Command Suite. Es ermöglicht Remote-Managementanwendungen wie der Appliance den Zugriff auf Zugriffsverwaltungsinformationen und den Überwachungsstatus sowie die Statusänderung von Unternehmens-Clientsystemen. Wenn Dell Command | Monitor auf einem verwalteten Gerät erkannt wird, verwendet die Appliance die WMI-Schnittstelle (Windows Management Instrumentation, Windows Verwaltungsinstrumentation) zur Erfassung ausführlicher Daten zum Hardwareinventar und Integritätsstatus. Siehe Informationen zu Dell Command | Monitor.

E

E-Mail-Benachrichtigungen

Siehe Warnungen.

Einmaliges Anmelden für die Administratorkonsole und Benutzerkonsole

Dank der einmaligen Anmeldung können Benutzer, die sich bei der Domäne angemeldet haben, auf die **Administratorkonsole** und die **Benutzerkonsole** der Appliance zugreifen, ohne die Anmeldeinformationen erneut auf der Anmeldeseite der Appliance eingeben zu müssen. Siehe Informationen zur einmaligen Anmeldung (SSO).

Einmalige Anmeldung für Appliances

Siehe Appliance-Verknüpfung.

Erfassung der Nutzung

Durch die Erfassung der Softwarenutzung können Sie Informationen dazu sammeln, wie Anwendungen auf den verwalteten Windows und Mac Geräten installiert und verwendet werden. Dies schließt Windows Store-Anwendungen wie Bing Travel ein. Für Anwendungen, die auf anderen Betriebssystemen wie beispielsweise Linux installiert sind, ist die Erfassung der Nutzung nicht möglich. Im Softwarekatalog kann die Erfassung für erkannte und nicht erkannte Anwendungen sowie für lokal katalogisierte Anwendungen aktiviert werden. Die Erfassung der Nutzung ist nicht möglich, wenn es sich um Betriebssystemsoftware handelt, die Anwendungen auf nicht unterstützten Betriebssystemen wie Linux installiert sind oder die Anwendungen im Softwarekatalog als Nicht katalogisiert aufgeführt werden. Siehe Informationen zur Erfassung der Softwarenutzung.

Erkannte Anwendungen

Erkannte Anwendungen sind ausführbare Dateien im Inventar der Appliance, die den Definitionen von Anwendungen im Softwarekatalog entsprechen. Sie können die Nutzungserfassung für erkannte Anwendungen und Suites aktivieren, diese Anwendungen als Nicht zulässig kennzeichnen und Lizenzinformationen für sie hinzufügen. Zudem können Sie die Liste erkannter Software im CSV-Format exportieren. Sie können die Liste erkannter Software, die Liste nicht katalogisierter Software und die Liste der lokal katalogisierten Software exportieren. Es ist nicht möglich, den gesamten Softwarekatalog zu exportieren.

Siehe Nicht erkannte Anwendungen. Siehe Erkannte Anwendungen.

Erkennung

Erkennung ist der Prozess der Identifikation von Geräten, die mit dem Netzwerk verbunden sind, und das Abrufen von Informationen über diese Geräte. Zu den Geräten, die erkannt werden können, gehören Laptops, Desktops, Server, Mobilgeräte, virtuelle Geräte, Drucker, Netzwerkgeräte, Drahtloszugriffspunkte, Router, Switches und mehr. Diese Geräte können überprüft und identifiziert werden, selbst wenn der KACE Agent nicht installiert ist. Sie können Erkennungsscans nach Bedarf durchführen oder die Ausführung von Scans zu bestimmten Zeiten planen. Siehe Informationen zu Geräteerkennung und -verwaltung.

F

Filter

Siehe Labels und Organisationsfilter.

G

Geräte

Geräte sind Computer oder Endpunkte, die von der Appliance verwaltet werden. Ihre Produktlizenzvereinbarung berechtigt Sie zur Verwaltung einer bestimmten Anzahl von Geräten, die als verwaltete Computer, Assets und überwachte Server klassifiziert sind. Verwaltete Geräte melden Daten wie Informationen zu Software, Hardware und Netzwerk an die Appliance. Siehe Produktlizenzinformationen anzeigen.

Geräteaktionen

Eine Funktion, mit der Sie von der Liste *Geräte* aus Befehle auf verwalteten Geräten ausführen können. Weitere Informationen zum Einrichten von Geräteaktionen finden Sie unter Allgemeine Appliance-Einstellungen ohne aktivierte Organisationskomponente konfigurieren.

I

Inventar

Das Inventar enthält Informationen über die Geräte, Anwendungen, Prozesse, Startprogramme sowie Dienste auf verwalteten Geräten in Ihrem Netzwerk. Das Inventar wird vom auf verwalteten Geräten installierten KACE Agent erfasst, über die Inventar-API hochgeladen oder über Verbindungen mit Geräten ohne Agent abgerufen. Sie können detaillierte Daten zu einzelnen verwalteten Geräten sowie zusammengefasste Daten, die über alle verwalteten Geräte hinweg gesammelt wurden, anzeigen. Außerdem können Sie die Inventarinformationen in Berichten sowie bei Entscheidungen bezüglich Upgrades, Fehlerbehebung, Einkäufen, Richtlinien usw. nutzen. Siehe Provisionierung des KACE Agent.

IP-Scans

Siehe Erkennung.

ITNinja

ITNinja.com (früher AppDeploy.com) ist eine von Quest KACE gesponserte, produktübergreifende Community-Website mit dem Schwerpunkt IT. Sie ist die führende Internet-Ressource für IT-Spezialisten zum Austausch von Informationen und für Fragen auf dem Gebiet der Systemverwaltung. Die Website bietet einen Bereich mit Fragen und Antworten sowie eine Blog-Plattform. Wenn Sie sich entscheiden, anonyme Nutzungsdaten an ITNinja weiterzugeben, wird der ITNinja Feed in der **Administratorkonsole** auf den Detailseiten zu Software, verwalteter Installation oder Dateisynchronisierung angezeigt. Der Feed ist nicht auf der Detailseite des *Softwarekatalogs* verfügbar. Siehe ITNinja-Feed aktivieren.

Quest veröffentlicht auf ITNinja Basisvorlagen für die Windows Zuverlässigkeitsanalyse und den Systemmonitor (PerfMon) sowie Open-Source-Perl-Skripte für Fremdsysteme (nicht Windows), mit deren Hilfe Benutzer Serverüberwachungsfunktionen erweitern und Probleme mit der System- und Anwendungsleistung ermitteln können. Diese nicht verwalteten Vorlagen und Skripte sind zum Download verfügbar, sodass sie nicht neu erstellt werden müssen.

K

KACE GO

KACE GO ist eine App, mit der Administratoren über ihre Smartphones oder Tablets auf Service-Desk-Tickets, Inventarinformationen, Überwachungswarnungen sowie die Anwendungsbereitstellungsfunktionen zugreifen können. Mit der App können auch Benutzer ohne Administratorberechtigungen auf ihrem Mobilgerät Service-Desk-Tickets senden, den Status von gesendeten Tickets anzeigen und Knowledge Base-Artikel lesen. Sie können KACE GO für iOS-Geräte aus dem Apple App Store oder für Android-Geräte aus dem Google Play Store herunterladen. Siehe Konfigurieren des Mobilgerätezugriffs.

Kataloganforderung

Siehe Anforderung "Zu Katalog hinzufügen".

Katalogisierte Anwendungen

Katalogisierte Anwendungen sind ausführbare Dateien, die sich in der offiziellen Softwarekatalog-Datenbank befinden. Hierzu zählen sowohl Anwendungen, die im Appliance-Inventar enthalten sind (Erkannte Anwendungen), als auch Anwendungen, die nicht im Inventar enthalten sind (nicht erkannte Anwendungen). Siehe Informationen zu katalogisierten Anwendungen.

Kategorie

Siehe Softwarekategorie.

Klassische Berichte

Die Berichtsfunktion auf der Appliance-Version 5.2 und älter. Ab Version 5.5 stehen klassische Berichte nicht mehr zur Verfügung.

Klassische Erfassung

Die klassische Erfassung ist ein Erfassungssystem, das auf der Appliance vor der Version 5.5 verfügbar war. Wenn Sie ein Upgrade von Version 5.4 oder niedriger auf Version 5.5 durchgeführt und die Erfassung der Nutzung vor dem Upgrade aktiviert haben, können Sie auch in der Version 5.5 der Appliance auf die klassische Erfassung zugreifen. In der Version 6.0 wurde die klassische Erfassung jedoch durch das Softwarekatalog-Erfassungssystem ersetzt, das ausführlichere Informationen bietet. Ab Version 6.0 steht die klassische Erfassung nicht mehr zur Verfügung. Siehe Erfassung der Nutzung.

Knoten

Siehe Geräte.

Knowledge Base

Quest verfügt über eine Knowledge Base mit Artikeln zu der Appliance, die Ihnen unter https://support.quest.com/kace-systems-management-appliance/kb zur Verfügung steht. Die Knowledge Base wird ständig mit Lösungen zu realen Problemen, die sich für Administratoren stellen, aktualisiert.

Konductor

Konductor ist eine interne Appliance-Komponente, die die Kommunikation zwischen der Appliance und verwalteten Geräten regelt, um einen reibungslosen Systembetrieb zu gewährleisten. Die Anzahl der von Konductor ausgeführten Aufgaben wird im Widget *Aufgaben werden durchgeführt* angezeigt. Außerdem werden Informationen zum Aufgabendurchsatz in den allgemeinen Einstellungen (auf Appliances mit aktivierter Organisationskomponente) oder in den Agenteneinstellungen (auf Appliances ohne aktivierte Organisationskomponente) angezeigt.

Siehe:

- Informationen zu Dashboard-Widgets
- Konfigurieren der allgemeinen Einstellungen auf System- und Verwaltungsebene

KScripts

Siehe Offline-KScripts und Online-KScripts.

L

Labelgruppen

Mit Labelgruppen können Sie Labels organisieren, um sie als Gruppe zu verwalten. Labelgruppen geben ihre Typen an die in ihnen enthaltenen Labels weiter. Eine Labelgruppe kann nicht nur mehrere Labels beinhalten, sondern auch mehreren Labelgruppen zugewiesen sein. Siehe Labelgruppen hinzufügen, anzeigen oder bearbeiten.

Labels

Labels sind Container zum Organisieren und Kategorisieren von Elementen wie Geräten, sodass diese als Gruppe verwaltet werden können. Beispielsweise können Sie Labels verwenden, um Geräte mit dem gleichen Betriebssystem oder am gleichen geografischen Standort zu kennzeichnen. Sie können dann Aktionen initiieren wie das Verteilen von Software oder das Bereitstellen von Patches auf allen Geräten mit dem Label. Labels können entweder spezifischen Elementen manuell zugewiesen werden oder sie können Elementen durch Zuweisung zu Kriterien wie SQL- oder LDAP-Abfragen automatisch zugewiesen werden. Siehe Einrichten und Verwenden von Labels für die Verwaltung von Elementgruppen.

LDAP-Browser

Der LDAP-Browser ist ein Assistent, der es Ihnen ermöglicht, die Daten auf einem LDAP-Server zu suchen und zu durchsuchen, wie zum Beispiel die eines Active Directory-Servers. Siehe LDAP-Browser verwenden.

LDAP-Labels

Bei LDAP-Labels handelt es sich um Labels, die mit dem Active Directory oder einem LDAP-Server (Lightweight Directory Access Protocol) interagieren. Sie können LDAP-Labels verwenden, um Geräte- und Benutzerdatensätzen auf Basis von LDAP- oder Active Directory-Abfragen oder Suchfiltern automatisch Labels zuzuweisen. LDAP-Labels werden auf Geräte angewendet, die den Suchkriterien entsprechen. Siehe Verwalten von LDAP-Labels.

Log Enablement Package (LEP)

Log Enablement Packages (LEPs) ermöglichen die Überwachung von Leistungsschwellenwerten sowie von Anwendungen für Server, wie z. B. Exchange, Internetinformationsdienste (Internet Information Services, IIS) usw. Auf der Listenseite *Log Enablement Packages* veröffentlicht Quest Basisvorlagen für die Windows Zuverlässigkeitsanalyse und den Systemmonitor (PerfMon) sowie Open Source-Perl-Skripte für Fremdsysteme (nicht Windows), mit deren Hilfe Benutzer Überwachungsfunktionen erweitern und Probleme mit der System- und Anwendungsleistung ermitteln können. Die zusätzlichen Vorlagen und Skripte sind nicht erforderlich für die Überwachung in der Appliance, die damit erstellten Profile sind jedoch hilfreich für die Überwachung von Leistungsschwellenwerten. Siehe Konfigurieren der Anwendungs- und Schwellenwertüberwachung mit Log Enablement Packages (LEP).

Lokalisierungskomponente

Eine Komponente der Appliance, mit der Sie die für die **Befehlszeilenkonsole**, **Administratorkonsole** und **Benutzerkonsole** verwendete Sprache auswählen können. Siehe Konfigurieren der Gebietsschema-Einstellungen.

Lokal katalogisierte Anwendungen

Anwendungen, die nicht in der offiziellen Version des Softwarekatalogs enthalten sind, jedoch zur lokalen Version der Appliance hinzugefügt wurden, werden als lokal katalogisierte Anwendungen bezeichnet. Die Nutzung lokal katalogisierter Anwendungen kann erfasst werden und sie können als "Nicht zulässig" gekennzeichnet und mit Lizenz-Assets verknüpft werden. Siehe Informationen zu lokal katalogisierten Anwendungen.

M

Mac Profile

Mac Profile sind Dateien, die zur Konfiguration von Richtlinien auf Benutzer- oder Systemebene auf Mac Geräten verwendet werden. Sie können die Appliance verwenden, um Mac Profile an vom Agenten verwaltete Geräte mit Mac OS X zu verteilen. Siehe Verwalten von Mac Profilen.

Manuelle Labels

Siehe Labels.

Mit Quest teilen

Die Optionen für die Freigabe von Appliance-Informationen an Quest. Siehe Konfigurieren der Datenfreigabeeinstellungen.

Mobilgerätezugriff

Der Mobilgerätezugriff ermöglicht die Interaktion mit der Appliance mithilfe von KACE GO.

KACE GO ist eine App, mit der Administratoren über ihre Smartphones oder Tablets auf Service-Desk-Tickets, Inventarinformationen sowie die Anwendungsbereitstellungsfunktionen zugreifen können. Mit der App können auch Benutzer ohne Administratorberechtigungen auf ihrem Mobilgerät Service-Desk-Tickets senden, den Status von gesendeten Tickets anzeigen und Knowledge Base-Artikel lesen. Sie können KACE GO für iOS-Geräte aus dem Apple App Store oder für Android-Geräte aus dem Google Play Store herunterladen.

Siehe Konfigurieren des Mobilgerätezugriffs.

MSI-Installationsvorlage

Mit dieser Vorlage können Sie ein Skript erstellen, das die grundlegenden Befehlszeilenparameter zum Ausführen MSI-basierter Installationsprogramme festlegt. Informationen zu Befehlszeilenoptionen finden Sie in der Dokumentation zur Microsoft MSI-Befehlszeile unter http://msdn.microsoft.com. Siehe MSI-Installationsskripte hinzufügen.

N

Nicht erkannte Anwendungen

Anwendungen, die nicht im Inventar, aber im Quest KACE Softwarekatalog enthalten sind, werden als nicht erkannte Anwendungen bezeichnet. Sie können die Erfassung für nicht erkannte Anwendungen aktivieren, sie als Nicht zulässig kennzeichnen und Lizenzinformationen hinzufügen. Da die Anwendungen jedoch nicht im lokalen Appliance-Inventar enthalten sind, kann die Liste nicht erkannter Software nicht ins CSV-Format exportiert werden. Siehe Erkannte Anwendungen. Siehe Nicht erkannte Anwendungen.

Nicht katalogisierte Anwendungen

Nicht katalogisierte Anwendungen oder ausführbare Dateien, die sich im Inventar der Appliance befinden, aber nicht im Softwarekatalog aufgeführt sind. Sie können Anwendungen, die als nicht katalogisiert aufgeführt sind, auf der Seite *Softwarekatalog* anzeigen. Allerdings können Sie die Erfassung der Nutzung für nicht katalogisierte Anwendungen nicht aktivieren, sie nicht als Nicht zulässig kennzeichnen und auch keine Lizenzinformationen über sie hinzufügen. Nicht katalogisierte Anwendungen müssen zum lokalen oder öffentlichen Softwarekatalog hinzugefügt werden, bevor ihre Nutzung erfasst werden kann und sie als Nicht zulässig gekennzeichnet oder mit Lizenzinformationen verknüpft werden können. Siehe Nicht katalogisierte Anwendungen.

Nicht zulässige Anwendungen

Nicht zulässige Anwendungen sind Anwendungen, die auf der Seite *Softwarekatalog* als "Nicht zulässig" gekennzeichnet wurden. Windows und Mac Anwendungen können nur dann als Nicht zulässig gekennzeichnet werden, wenn sie als erkannte, nicht erkannte oder lokal katalogisierte Anwendungen klassifiziert sind. Nicht katalogisierte Anwendungen können erst dann als Nicht zulässig gekennzeichnet werden, wenn sie zum Softwarekatalog hinzugefügt wurden. Als "Nicht zulässig" gekennzeichnete Anwendungen können gesperrt werden, um ihre Ausführung auf verwalteten Geräten zu verhindern, falls diesen Geräten ein für die Anwendungssteuerung aktiviertes Label zugewiesen wurde. Siehe Verwenden der Anwendungssteuerung.

Nutzungsrichtlinie

Eine Erklärung oder Richtlinie, die für Benutzer angezeigt wird, wenn sie sich bei der **Administratorkonsole**, **Befehlszeilenkonsole** oder **Benutzerkonsole** anmelden. Siehe Nutzungsrichtlinie aktivieren bzw. deaktivieren.

O

Offline-KScripts

Skripte, die zu einem geplanten Zeitpunkt nach der Uhr des Zielgeräts ausgeführt werden. Offline-KScripts können auch dann ausgeführt werden, wenn die Zielgeräte nicht mit der Appliance verbunden sind, beispielsweise beim Gerätestart oder bei der Benutzeranmeldung. Sie können diese Skripte mit den Skriptvorlagen erstellen. Siehe Hinzufügen und Bearbeiten von Skripten.

Online-KScripts

Skripte, die nur dann ausgeführt werden, wenn ein Zielgerät mit der Appliance verbunden ist. Die Ausführung von Online-KScripts erfolgt zu geplanten Zeitpunkten gemäß der Uhr der Appliance. Sie können diese Skripte mit den Skriptvorlagen erstellen. Siehe Hinzufügen und Bearbeiten von Skripten.

Online-Shellskripts

Skripte, die gemäß der Uhr der Appliance zu geplanten Zeitpunkten ausgeführt werden, jedoch nur, wenn das Zielgerät mit der Appliance verbunden ist. Online-Shellskripts werden mithilfe einfacher textbasierter Skripte (Bash, Perl, Batch und andere) erstellt, die vom Betriebssystem des Zielgeräts unterstützt werden. Windows unterstützt Batchdateien und die verschiedenen vom jeweiligen Betriebssystem der Zielgeräte unterstützten Shellskript-Formate. Siehe Hinzufügen und Bearbeiten von Skripten.

Organisationen

Organisationen sind all die logischen Instanzen einer Appliance, die auf einer einzelnen Appliance ausgeführt werden. Sie können Organisationen erstellen, wenn die Organisationskomponente in Ihrer Appliance aktiviert ist, jede Organisation über eine eigene Datenbank verfügt und Sie das Inventar und andere Komponenten jeder Organisation getrennt voneinander verwalten. Siehe Erstellen und Verwalten von Organisationen.

Organisationsfilter

Organisationsfilter ähneln Labels, sie dienen jedoch einem bestimmten Zweck: Organisationfilter weisen bei der Inventarerfassung von Geräten diese automatisch an Organisationen zu.

Es gibt zwei Arten von Organisationsfiltern:

- **Datenfilter**: Weisen Geräte basierend auf Suchkriterien automatisch Organisationen zu. Bei der Inventarerfassung von Geräten werden diese der Organisation zugewiesen, wenn sie den Kriterien entsprechen. Dieser Filter ähnelt Smart Labels dahingehend, dass er Geräte automatisch Organisationen zuweist, wenn sie den angegebenen Kriterien entsprechen.
- **LDAP-Filter**: Weisen Geräte basierend auf LDAP- oder Active Directory-Interaktionen automatisch Organisationen zu. Bei der Inventarerfassung von Geräten wird die Abfrage an den LDAP-Server gesendet. Wenn Geräte den Kriterien entsprechen, werden sie automatisch der Organisation zugewiesen.

  Siehe Verwalten von Organisationsfiltern.

Organisationskomponente

Eine Komponente der Appliance, mit der Sie Organisationen in der Appliance erstellen und verwalten können. So können Sie Geräte verschiedenen Organisationen zuweisen und Benutzerrollen innerhalb jeder Organisation erstellen, um Zugriffsberechtigungen für Administratoren und Benutzer zu verwalten. Sie können beispielsweise Ihre Organisationen so konfigurieren, dass Administratoren nur Geräte innerhalb ihrer Organisation anzeigen und darauf Aktionen durchführen können; sie können keine Geräte anzeigen, die zu anderen Organisationen gehören.

Siehe Erstellen und Verwalten von Organisationen.

OVAL

OVAL (Open Vulnerability and Assessment Language) ist ein international anerkannter Standard zur Ermittlung von Sicherheitslücken und Konfigurationsproblemen auf Windows-Geräten. OVAL-Sicherheitsprüfungen ermitteln Assets, die Compliance-Bedingungen nicht erfüllen, und ermöglichen Ihnen die Anpassung von Sicherheitsrichtlinien, um Regeln durchzusetzen, Tests für die automatische Ausführung zu planen und Berichte auf Basis der Ergebnisse auszuführen.

OVAL ist mit der CVE-Liste (Common Vulnerabilities and Exposures) bekannter Sicherheitslücken kompatibel. Der CVE-Inhalt wird von der CVE-Redaktion bestimmt, die aus Fachleuten aus der internationalen Community

für Informationssicherheit besteht. Neue Informationen zu Sicherheitsrisiken, die im Forum der Community besprochen wurden, werden für eine mögliche Aufnahme in die Liste an die CVE-Initiative gesendet. Weitere Informationen zu CVE, zur MITRE Corporation und zur OVAL-Redaktion finden Sie unter http://cve.mitre.org.

Dank der Möglichkeit, Sicherheitslücken und Bedrohungen mithilfe eines gemeinsamen Standards zu beschreiben, wird die gemeinsame Nutzung von Sicherheitsdaten mit anderen CVE-kompatiblen Datenbanken und Programmen erleichtert.

Siehe Informationen zu OVAL-Tests und -Definitionen.

P

Patchen

Patchen ist ein Mechanismus zur Bereitstellung sicherheitsbezogener und anderer wichtiger Patches von Microsoft, Apple und sonstigen Drittanbietern wie Adobe. Dies umfasst sowohl Patches für Betriebssysteme als auch für Anwendungen. Wenn Sie Patches in einer Produktionsumgebung bereitstellen, können Sie auswählen, auf welche Betriebssysteme Sie Patches anwenden möchten und außerdem mithilfe von Labels Zeitpläne für den Patchvorgang einrichten. Siehe Informationen zur Patch-Verwaltung.

Protokolle

Siehe Die Skriptprotokolle durchsuchen.

Provisionierung

Der Prozess der Installation des KACE Agent auf verwalteten Geräten. Siehe Provisionierung des KACE Agent.

Provisionierungszeitpläne

Provisionierungszeitpläne geben an, wie und wann der KACE Agent auf Geräten, die Sie mit Agenten-Software verwalten möchten, installiert werden soll. Siehe Provisionierungszeitpläne verwalten.

R

Replikationsfreigaben

Replikationsfreigaben sind Geräte, die Kopien von Dateien zur Verteilung beibehalten. Sie sind insbesondere dann hilfreich, wenn Ihre verwalteten Geräte an mehreren geografischen Standorten bereitgestellt sind. Mit Replikationsfreigaben kann beispielsweise ein Gerät in New York Dateien von einem anderen Gerät im selben Büro herunterladen anstatt von einer Appliance in Los Angeles. Eine Replikationsfreigabe ist eine vollständige Replikation aller digitalen Assets und wird von der Appliance automatisch verwaltet. Sobald eine Replikationsfreigabe für ein Label angegeben wird, rufen Geräte in diesem Label Dateien von dieser Replikationsfreigabe ab. Siehe Verwenden von Replikationsfreigaben.

Ressourcen

Elemente wie Skripte, Berichte, verwaltete Installationen und Software, die importiert oder exportiert und so zwischen Organisationen und Appliances ausgetauscht werden können. Siehe Importieren und Exportieren von Appliance-Ressourcen.

Rolle

Die mit Benutzerkonten und Organisationen zusammenhängenden Berechtigungen. Siehe:

- Verwalten von Benutzerkonten auf Systemebene
- Verwalten von Organisationsbenutzerkonten
- Verwalten von Organisationsrollen und Benutzerrollen
- Überwachungsspezifische Rollen erstellen und zuweisen

S

SAM

SAM ist die Abkürzung von Software Asset Management, eine Methode zur Verwaltung von Anwendungen im Inventar. Siehe Verwalten des Softwarekataloginventars.

Samba Freigabe

Das integrierte Dateifreigabesystem der Appliance. Siehe Dateifreigabe auf Systemebene aktivieren.

SCAP

SCAP (Secure Content Automation Protocol) ist ein offener Standard zur Angabe von Softwareschwachstellen, Überwachung sicherheitsbezogener Konfigurationen und Produktnamen sowie zur Untersuchung von Systemen im Hinblick auf Sicherheitslücken und zur Bewertung (Zahlenwert) der Auswirkungen der ermittelten Sicherheitsprobleme auf Windows-Geräten. SCAP wird vom National Institute of Standards and Technology (NIST) verwaltet und von US-Regierungsbehörden wie dem Office of Management and Budget (US OMB) verbindlich vorgeschrieben.

SCAP verwendet die National Vulnerability Database der US-Regierung NVD, ein auf Standards basierendes Datenrepository der US-amerikanischen Regierung zur Verwaltung von Sicherheitslücken. NVD beinhaltet Datenbanken mit Sicherheitsprüflisten, sicherheitsbezogenen Softwareschwachstellen, fehlerhaften Konfigurationen, Produktnamen und Metriken für die Auswirkungen. Weitere Informationen zu SCAP sowie zur NVD finden Sie auf den Websites des NIST unter http://scap.nist.gov/index.html und http://nvd.nist.gov/.

Siehe Informationen zu SCAP.

Schneller Wechsel von Organisationen und verknüpften Appliances

Hierdurch ist es möglich, über eine Dropdown-Liste in der oberen rechten Ecke der **Administratorkonsole** zwischen Organisationen zu wechseln, anstatt sich bei jeder Organisation separat anmelden zu müssen. Zudem wird es ermöglicht, zwischen verknüpften Appliances der K Serie zu wechseln, ohne sich bei jeder Appliance separat anmelden zu müssen. Siehe Schnellen Wechsel von Organisationen und verknüpften Appliance aktivieren.

Serverüberwachung

Die Appliance bietet ein Modul, mit dem Sie eine grundlegende Leistungsüberwachung für Server im Inventar ausführen können. Die Überwachungsfunktion ist für Serverbetriebssysteme konzipiert und bietet standardmäßige Überwachungsprofile, die Kriterien für Leistungswarnungen für jedes Betriebssystem definieren. Sie können weitere benutzerdefinierte Profile mit ähnlichen oder anderen Kriterien definieren, die auf alternative Ereignisprotokolle oder Protokolle auf Betriebssystemebene verweisen.

Service Desk

Der Standardname des Trouble-Ticket-Erfassungssystems für Endbenutzer, das Teil der Appliance **Benutzerkonsole** ist, lautet Service Desk. Endbenutzer können über Service Desk Trouble-Tickets per E-Mail oder über die **Benutzerkonsole** unter `http://<appliance_hostname>/user` senden, wobei `<appliance_hostname>` der Hostname der Appliance ist. Ihr Helpdesk-Team bearbeitet diese Tickets per E-Mail, über die **Administratorkonsole**, `http://appliance_hostname/admin` oder über die KACE GO App. Sie können die Kategorien und Felder der Tickets nach Bedarf anpassen. Siehe Informationen zum Service Desk.

Skripte

Siehe Offline-KScripts, Online-KScripts und Online-Shellskripts.

Skripterstellung

Die Möglichkeit, eine Reihe von Aktionen auf verwalteten Geräten zu erstellen und auszuführen. Skripte können entwickelt werden, um viele verschiedene Vorgänge auszuführen, vom Installieren bzw. Entfernen von Anwendungen bis hin zum Überprüfen und Ändern von Einstellungen (beispielsweise Firewall-Einstellungen) auf verwalteten Geräten. Skripte werden basierend auf von Ihnen definierten Labels und Zeitplänen bereitgestellt und ausgeführt. Sie funktionieren unabhängig vom zentralen Inventarprozess verwalteter Installationen. Siehe Hinzufügen und Bearbeiten von Skripten.

Smart Labels

Smart Labels sind Labels, die auf der Grundlage von von Ihnen festgelegten Kriterien automatisch zugewiesen und entfernt werden. Wenn Sie zum Beispiel Notebooks in einer bestimmten Niederlassung

nachverfolgen möchten, können Sie ein Label mit der Bezeichnung "Niederlassung in San Francisco" und dann ein Smart Label auf Basis des IP-Adressbereichs oder des Subnetzes für Geräte erstellen, die sich in der Niederlassung in San Francisco befinden. Bei jeder Inventarisierung eines Geräts aus dem IP-Adressbereich wird automatisch das Smart Label "San Francisco" zugewiesen. Wenn das Gerät den IP-Adressbereich verlässt und danach erneut inventarisiert wird, wird das Label automatisch entfernt.

Smart Labels werden auf verwaltete Geräte angewendet bzw. entfernt, wenn die Geräte eine Verbindung mit der Appliance herstellen. Wenn Sie also ein Smart Label erstellen, das die Erfassung der Nutzung auf Geräten ermöglicht, kann es einige Zeit dauern, bis das Smart Label auf die Geräte angewendet wird und die Geräte mit der Meldung von Erfassungsinformationen beginnen. Die Erfassung der Nutzung wird für Geräte, die den Smart Label-Kriterien entsprechen, erst nach der Inventarisierung der Geräte und der Anwendung des Smart Labels aktiviert.

Siehe Verwalten von Smart Labels.

Softwarekatalog

Der Softwarekatalog ist eine Datenbank mit standardisierten Informationen zu mehr als 57.000 Windows und Mac Anwendungen und Software-Suites. Die Informationen im Katalog umfassen den Namen, die Version, den Herausgeber sowie die Kategorie jeder Anwendung oder Suite sowie das Betriebssystem, auf dem die Anwendung oder Suite ausgeführt wird. Siehe Verwalten des Softwarekataloginventars.

Softwarekategorie

Softwarekategorien unterteilen Software in bestimmte Gruppen wie Softwaretreiber oder Sicherheitsanwendungen. Bei auf der Seite Software aufgelisteten Anwendungen werden die Kategorien manuell zugewiesen. Bei auf der Seite Softwarekatalog aufgelisteten Anwendungen werden die Softwarekategorien den Anwendungen automatisch zugewiesen. Siehe Verwenden von Bedrohungsstufen und Kategorien für Software.

Sperrung

Siehe Anwendungssteuerung.

T

Testen auf Sicherheitslücken

Das Testen auf Sicherheitslücken ist der Prozess des Scannens und das Einrichten von Scan-Zeitplänen, um Windows Geräte mithilfe von OVAL(Open Vulnerability Assessment Language)-Tests auf bekannte Sicherheitslücken zu überprüfen. Sicherheitslückentests sind eine nützliche Ergänzung zu Patches und anderen Formen der Sicherheitsverbesserung, mit denen überprüft werden kann, ob mit diesen Maßnahmen bekannte Probleme behoben werden. Siehe Informationen zu OVAL-Sicherheitsprüfungen.

Tether

Die Verbindung zum **Quest Support**. Mithilfe des Tether können Mitarbeiter von KACE sich zur Fehlerbehebung mit Ihrem System verbinden. Siehe Tether zum Support von Quest KACE aktivieren.

Ü

Überwachte Server

Die Produktlizenzvereinbarung berechtigt Sie zur Verwaltung einer bestimmten Anzahl von Geräten, die als verwaltete Server klassifiziert sind. Überwachte Server sind Server, 1) die die Anforderungen für verwaltete Computer erfüllen und 2) auf denen die Überwachung aktiviert ist. Sie können fünf Server mit Ihrer Appliance-Lizenz überwachen. Wenn Sie bis zu 200 Server überwachen möchten, benötigen Sie eine Lizenz für das Überwachungsmodul. Siehe Produktlizenzinformationen anzeigen und Verwalten der Geräteüberwachung.

V

Verknüpfen

Siehe Appliance-Verknüpfung.

Verwaltete Computer

Die Produktlizenzvereinbarung berechtigt Sie zur Verwaltung einer bestimmten Anzahl von Geräten, die als verwaltete Computer klassifiziert sind. Verwaltete Computer sind Geräte im Appliance-Inventar, auf denen Windows, Mac, Linux oder UNIX Betriebssysteme installiert sind, 2) die als PCs oder Server eingestuft werden und 3) die dem Inventar nicht manuell, über die WSAPI oder mithilfe der Verwaltung von Mobilgeräten hinzugefügt wurden. Siehe Produktlizenzinformationen anzeigen.

Verwaltete Installationen

Verwaltete Installationen (MI) sind die primäre Methode zum Bereitstellen oder Entfernen von Anwendungen von verwalteten Geräten der Appliance. Jede verwaltete Installation beschreibt einen bestimmten Anwendungstitel und eine bestimmte Version, der bzw. die installiert oder entfernt wird. Dies umfasst auch Installationsbefehle, Installationsdateien und Zielgeräte (nach Label). Verwaltete Installationen finden stets dann statt, wenn verwaltete Geräte Inventardaten in die Appliance hochladen. Auf diese Weise bestätigt die Appliance vor Durchführung der Installation, dass die Installation tatsächlich benötigt wird. Installationspakete können so konfiguriert werden, dass sie unbeaufsichtigt oder mit Benutzereingriffen ausgeführt werden. Verwaltete Installationen können Installations-, Deinstallations- und Befehlszeilenparameter enthalten. Siehe Verwenden verwalteter Installationen.

Verwaltung der Anmeldeinformationen

Die Verwaltung der Anmeldeinformationen ermöglicht es Ihnen, Benutzernamen und Kennwörter, die für die Protokollierung in anderen Systemen wie z. B. Computern und Servern erforderlich sind, sowie für die Google- oder SNMP-Authentifizierung erforderliche Informationen über eine zentrale Stelle zu organisieren. So wird der Prozess zur Eingabe und Verwaltung von Anmelde- und Authentifizierungsinformationen verbessert. Siehe Verwalten von Anmeldeinformationen.

Verwaltung ohne Agent

Die Geräteverwaltung ohne Agent ist ein Verfahren zur Verwaltung von Geräten, ohne dass dafür die KACE Agent-Software auf diesen Geräten bereitgestellt und gewartet werden muss. Die Verwaltung ohne Agent nutzt SSH, SNMP und andere Verfahren für die Verbindung mit Geräten, die keine Agenten unterstützen, wie Drucker, Netzwerkgeräte und Speichergeräte, und meldet die erfassten Inventarinformationen an die Appliance **Administratorkonsole**. Dies ist nützlich bei Betriebssystemversionen und Verteilungen, die vom KACE Agent nicht unterstützt werden und in Fällen, bei denen die Verwaltung ohne Agent der Installation des Agenten vorgezogen wird. Siehe Geräte ohne Agent verwalten.

Virtual Appliance

Siehe Appliance oder Virtual Appliance.

W

Wake on LAN

Mit Wake on LAN können Sie Geräte von einem Remote-Standort aus über die Appliance einschalten, unabhängig davon, ob der KACE Agent auf diesen Geräten installiert ist oder nicht. Siehe Verwenden von Wake on LAN.

Warnungen

Broadcast-Warnungen sind Meldungen wie Popups, die zur Anzeige auf vom Agenten verwalteten Geräten von der Appliance übertragen werden können. Die Anzeige von Warnungen ist nützlich, wenn Sie dringende Informationen kommunizieren bzw. Benutzer über das bevorstehende Ausführen von Aktionen oder Skripten auf ihren Geräten informieren möchten. Siehe Senden von Warnungen an verwaltete Geräte.

Überwachungswarnungen sind Meldungen, die auf unterstützten Servergeräten generiert und an die Appliance gesendet werden, um Mitarbeiter auf Fehler und Probleme hinzuweisen, die in den Ereignis- und Systemprotokollen der Geräte gemeldet wurden. Siehe Überwachen von Servern.

Über uns

Quest entwickelt Softwarelösungen, die sich die Vorteile neuer Technologien bei einer immer komplexer werdenden IT-Infrastruktur zu Nutze machen. Von der Datenbank- und Systemverwaltung über Active Directory- und Office 365-Verwaltung bis hin zur Erhöhung der Widerstandskraft gegen Cyberrisiken unterstützt Quest Kunden bereits jetzt bei der Bewältigung ihrer nächsten IT-Herausforderung. Weltweit verlassen sich mehr als 130.000 Unternehmen und 95 % der Fortune 500-Unternehmen auf Quest, um proaktive Verwaltung und Überwachung für die nächste Unternehmensinitiative bereitzustellen, die nächste Lösung für komplexe Microsoft-Herausforderungen zu finden, und der nächsten Bedrohung immer einen Schritt voraus zu sein. Quest Software. Wo die Zukunft auf die Gegenwart trifft. Weitere Informationen hierzu finden Sie unter www.quest.com.

Ressourcen für den technischen Support

Der technische Support steht Quest Kunden mit gültigem Servicevertrag sowie Kunden mit Testversionen zur Verfügung. Auf das Quest Support Portal können Sie unter https://support.quest.com/de-de/ zugreifen.

Im Support-Portal finden Sie Tools zur Selbsthilfe, mit denen Probleme rund um die Uhr schnell und selbständig gelöst werden können. Das Support-Portal bietet folgende Möglichkeiten:

- Einreichen und Verwalten einer Serviceanfrage
- Anzeigen von Knowledge Base-Artikeln
- Registrieren für Produktbenachrichtigungen
- Herunterladen von Software und technischer Dokumentation
- Anzeigen von Anleitungsvideos
- Teilnehmen an Community-Diskussionen
- Online Chatten mit Supporttechnikern
- Anzeigen von Services, die Sie bei Ihrem Produkt unterstützen können

Rechtliche Hinweise

© 2021 Quest Software Inc. ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Quest Software Inc.

The information in this document is provided in connection with Quest Software products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Quest Software products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, QUEST SOFTWARE ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL QUEST SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF QUEST SOFTWARE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Quest Software makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Quest Software does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

Quest Software Inc.

Attn: LEGAL Dept

4 Polaris Way

Aliso Viejo, CA 92656

Refer to our Web site (https://www.quest.com) for regional and international office information.

Patente

Quest Software ist stolz auf seine fortschrittliche Technologie. Für dieses Produkt können Patente bzw. Patentanmeldungen bestehen. Aktuelle Informationen zum bestehenden Patentschutz für dieses Produkt finden Sie auf unserer Website unter https://www.quest.com/legal.

Trademarks

Quest, the Quest logo, Join the Innovation, and KACE are trademarks and registered trademarks of Quest Software Inc. For a complete list of Quest marks, visit https://www.quest.com/legal/trademark-information.aspx. All other trademarks and registered trademarks are property of their respective owners.

Legende

VORSICHT: Das Symbol VORSICHT weist auf eine mögliche Beschädigung von Hardware oder den möglichen Verlust von Daten hin, wenn die Anweisungen nicht befolgt werden.

WICHTIG, HINWEIS, TIPP, MOBIL oder VIDEO: Ein Informationssymbol weist auf ergänzende Informationen hin.

KACE Systems Management Appliance Administratorhandbuch

Letzte Überarbeitung: August 2021

Software-Version: 12.0

Index

Zahlen

2FA für die Appliance aktivieren 111
2FA konfigurieren 101
2FA, für Organisationen konfigurieren 349
2FA, konfigurieren 101

A

Abhängigkeiten für Skripte 700
Abonnieren von Patches 785, 789
Active Directory
Einmalige Anmeldung mit 205
Einmalige Anmeldung, Konfiguration 120, 202
Einstellungen für Mac OS X 739
Administration
Aktualisieren der Appliance-Software 1114
Aktualisieren der OVAL-Definitionen 1117
Aktualisieren des Lizenzschlüssels 1116
Daily Run Output 1127
E-Mail-Benachrichtigungen für Administratoren 178
Fehlerbehebung 1122
Neustarten der Appliance 1116
Protokolle, anzeigen 1122
Protokolle, herunterladen 1127
Sichern der Daten 1105
Wiederherstellen der Appliance-Einstellungen 1111
Wiederherstellen der letzten Sicherung 1111
Wiederherstellen der Werkseinstellungen 1114
Administratorkonsole 30, 30
Gebietsschema-Einstellungen für 85, 91
Informationen 28
Komponenten
mit der Organisationskomponente 38
ohne Organisationskomponente 34
Agent
Aktivieren der Dateifreigabe 500
Aktivieren der Dateifreigabe auf Organisationsebene 501, 501
Aktualisierungen 521, 521
Hochladen, manuell 523
Konfigurieren, automatisch 522
Aufgabenstatus 519
Beziehen von Installationsdateien 525
Gruppenrichtlinienobjekt-Provisionierungstool für Windows 502
Hinzufügen von Windows Registrierungsschlüsseln für Zugriff auf DDP|E-Informationen 485
In Quarantäne
Genehmigen 497
löschen 497
Sperren 497
Überprüfen 497
Informationen 28, 210, 499
Installieren auf mehreren Geräten 506
Kommunikationseinstellungen für 513
Konea 520
Konfiguration 123
Manuelle Bereitstellung 210, 524
Nachrichten anzeigen 520
Nachrichten, löschen 521
Protokolleinstellungen für 513
Provisionierung 500, 501, 501, 502
Provisionierung mithilfe von Erkennungsergebnissen 410
Provisionierungsergebnisse 512
Provisionierungsmethoden 210, 499
Provisionierungszeitpläne
anzeigen 511
Bearbeiten 511
duplizieren 511
Löschen 512
wird ausgeführt 511
Registrierung bei der Appliance 495
Starten und Beenden unter Linux 531
Starten und Beenden von Mac OS X 534
Systemanforderungen für die Installation 504
Token
Bearbeiten 495
Hinzufügen 495
Verfügbare Funktionen für verwaltete Geräte 412
Verlauf 210, 499
Vorbereiten der Installation mit der integrierten Provisionierung 504
Agenten in Quarantäne
Genehmigen 497
löschen 497
Sperren 497
Überprüfen 497
Agenten-Bereitstellung
Linux Geräte 529
Aktualisierung wird durchgeführt 530
Anzeigen der Version auf Linux 531
Systemstart/Anmeldung 530
Überprüfen der Version 531
Linux Geräte entfernen 531
Mac OS X Geräte
Bereitstellen/Aktualisieren 532
Entfernen 534
Terminalfenster verwenden 532
Überprüfen 534
Überprüfen der Version 534
Verwenden Shellskripten 533
Windows Geräte 525
Agenten-Messaging-Protokoll 123

Aktivieren 1109
2FA für das Gerät 111
Appliance-Verknüpfung 139
Dateifreigabe
ohne Organisationskomponente 501
Organisationsebene 501, 501
Systemebene 500
Einmalige Anmeldung 201
File Sharing für Windows Geräte 505
LDAP-Labels 171
Mobilgerätezugriff
für Benutzer 136
für Benutzer aktivieren 136
für die Appliance 135
Nutzungsrichtlinie 134
Schneller Wechsel von Organisationen 138
Sichern von Anhängen für Tickets 992
SSH für die Appliance 111
Tether zu Quest 1121
Ticket-Erstellung per E-Mail 1016
Über- und untergeordnete Ticketbeziehungen 1095
Wechseln zwischen Organisationen 138
Aktualisierung wird durchgeführt
Appliance-Agenten automatisch 521
Appliance-Software 62
KACE Agenten auf Linux, manuell 530
KACE Agenten auf Mac OS X, manuell 532
KACE Agenten automatisch 522
Lizenzschlüssel der Appliance 1116
OVAL-Definitionen 1117
Softwarekatalog 626
Softwarelizenz-Compliance 309
Aktualisierungen
Dell Aktualisierungen und Patchen 849
im Vergleich zu Bereitstellungen 849
KACE Agent-Updates anzeigen 521
Überprüfen, ob Appliance-Aktualisierungen verfügbar sind 1114
Allgemeine Einstellungen 78
Alternative Download-Quellen
für Skripte 700
Informationen 664
Verteilen von Paketen über 664
Ändern benutzerdefinierter Ticketfelder per E-Mail 1019
Ändern von Ticketfeldern per E-Mail 1017
Ändern von Ticketgenehmigungsfeldern per E-Mail 1018
Änderungsverlauf
Anzeigen, Suchen und Exportieren 146, 147, 147
für Assets 144
für Einstellungen 142
für Objekte 145
in den SQL-Berichten 899
Löschen 147
Organisationsebene, Einstellungsverlauf 143
Systemebene 143
Android 134
Anfordern der lokalen Katalogisierung für Anwendungen 598
Anfordern von Ticketgenehmigungen 1098
Angaben zur Hardware der Appliance 74
Anhänge an Tickets 992, 1027
Ankündigungen
Auf der Startseite der Benutzerkonsole hinzufügen und bearbeiten 985
Priorität auf der Startseite der Benutzerkonsole 987
Anmeldeinformationen
Ermittlung der Verwendung der 228
Erstellen von Berichten über 229
Exportieren 229
Hinzufügen eines geheimen Schlüssels 216
Hinzufügen von Benutzern/Kennwörtern 218
Hinzufügen von Google OAuth 221
Hinzufügen von LDAP-Benutzern/Kennwörtern 219
Hinzufügen von SNMP 223
Löschen 230
Office 365 hinzufügen 225
Verwalten 216
Anmeldeinformationen für Chrom 388
Anmeldeinformationen verwalten 216
Anmelden 71
Anmeldungsanforderungen für Organisationen 78
Anpassen
Asset-Typen 241
Begrüßungsmeldung der Benutzerkonsole 978, 980
Benutzerkonsole, interaktive Schaltflächen und Widgets 983
Benutzerkonsolenlogo 978, 980
Details zum Ticket 976
Käufe 281
Lizenzen 274
Standorte 265
Verträge 270
Antwortvorlagen
Konfigurieren 974
Anwendungen
Anzeigen erkannter 589
Anzeigen nicht erkannter 589
Anzeigen nicht katalogisierter Anwendungen 590
Anzeigen von lokal katalogisierten Anwendungen 591
Katalogisiert 585
Lokal katalogisiert 585
Nicht zulässig 585
Suchen mithilfe der erweiterten Suche 579
Anwendungen werden blockiert
Anforderungen 622
Angezeigte Meldungen 622
Anzeigen nicht zulässiger Apps 624
Berichterstellung zu 624
Einschränkungen von 622
Entfernen der Kennzeichnung von Apps 625
Informationen 621
Kennzeichnen als 'Nicht zulässig' 623
Zuweisen von Anwendungssteuerungslabels 623
Anwendungsklassifizierungen 584
Anwendungspatches anzeigen 796

Anwendungssteuerung
Anforderungen 622
Angezeigte Meldungen 622
Anzeigen nicht zulässiger Anwendungen 624
Berichterstellung zu 624
Editionen mit gemeinsamen ausführbaren Dateien 622
Einschränkungen von 622
Entfernen der Kennzeichnung 625
Kennzeichnen als 'Nicht zulässig' 623
Verwendung 621
Zuweisen von Labels für 623
Anzeigen von Mac Profil-Listen 763
Anzeigen von Patch-Zeitplänen 816
Anzeigen von Zeitplänen für Linux-Paket-Upgrades 864
Anzeigen von Zeitplänen für Windows-Funktionsaktualisierungen 842, 858
Apache
Grafiken 1122
Protokollpfade 923
Webserverdiagnose-Diagramme 111
API
Zugriff auf die Appliance 111
AppDeploy Live (siehe ITNinja) 581
Apple iOS 134
Appliance
Angaben zur Hardware 74
Aufgabenpläne 59
Bestandsaufnahme-Dashboard-Widgets 231
Domänenzugriff 104
Download-Einstellungen für Patches 792
Download-Einstellungen für Windows-Funktionsaktualisierungen 792
Konfiguration
automatische Aktualisierung, Eigenschaften 126
Sitzungs-Timeout 125
SSL-Zertifikat 122
Konfigurieren der Netzwerkeinstellungen 74
Labels 62
Lizenzinformationen 912
lokale Routing-Tabellen 109
NTP-Dienst, Status überprüfen von 104
Port-Einstellungen 102
Sicherheitseinstellungen 111
Softwareaktualisierungen 62
Softwareversion 59
Appliance herunterfahren 1116
Appliance-Einstellungen
Aktualisierungen überprüfen 1116
Allgemein 78
beworbene Aktualisierungen 1114
Hochladen von Sicherungsdateien 1112
Lizenzschlüsselaktualisierungen 1116
manuelle Aktualisierungen 1115
Sicherheit 111
Wiederherstellen 1111
Wiederherstellen der Werkseinstellungen 1114
Wiederherstellen von Sicherungskopien 1111, 1113
Appliance-Ressourcen
Exportieren aus Organisationen 360
Exportieren von der Appliance 358
Importieren in Appliances 359
in Organisationen importieren 360
Informationen zum Importieren und Exportieren 357
Appliance-Sicherungen 1109, 1109
FTP-Zugriff auf 1108
Herunterladen von Dateien 1107
Informationen 1105
Löschen 1108
Manuell 1107
Status von 1120
Zeitplan der täglichen Sicherung 1106
Appliance-Verknüpfung
Aktivieren 139, 139
Deaktivieren 141, 141
Hinzufügen von Namen und Schlüsseln 140
Informationen 139
Zugriff auf Federation-API-Einstellungen aktivieren 141, 141
Appliance-Version 59
APPROVAL_INFO (Feld) 1099
Arbeitsinformationen für Service Desk Tickets 1020
Archivierung
Aktivieren für Tickets 1054
Löschen von Tickets aus 1058
Ticket-Warteschlangeneinstellungen für 1056
Wiederherstellen von Tickets 1058
Arten
Service Desk-Prozesse 1042
Asset Management
Aktualisieren von Assets, manuell 256
Anzeigen verfügbarer Asset-Untertypen 254
Anzeigen von Assets 236, 238
Anzeigen von Asset-Untertypen auf der Seite "Assets" 254
Asset-Administratorrolle 263
Asset-Lebenszyklus-Einstellungen anzeigen 238
Asset-Typen
Anpassen 241
Beziehungen mit einem übergeordneten Element für Standorte 247
Hinzufügen 241
Hinzufügen von benutzerdefinierten Feldern für Geräte 245
Hinzufügen von Feldern für Standorte 246
Informationen 240
Löschen 247
umbenennen 240
Asset-Untertypen 248, 249
Bearbeiten 253
Festlegen als Standardeinstellung 253
Hinzufügen 249
Löschen 256
Barcodes hinzufügen 237
Berichterstellung zu Assets 263
Beziehungen zwischen Asset-Feldern 246
Datenformat 301
Erfassung der Softwarenutzung
Aktivieren für Anwendungen 614
Aktivieren für Geräte mit Smart Labels 612
Aktivieren mit manuellen Geräte-Labels 610

Anzeigen von Gerätedetails 618
Anzeigen von Nutzungserfassungsdetails 616, 617
Deaktivieren 619
Deaktivieren für Geräte mit manuellen Labels 619
Deaktivieren für Geräte mit Smart Labels 619
Erfasste Informationen 609
Geräteauswahl für 610
Informationen 608
Informationen zum Aktivieren 610
Konfigurieren von Optionen 614
Planen der Inventarerfassungsintervalle 620
Skripte, die Informationen erfassen 609
Software-Suites 609
Festlegen der nachzuverfolgenden Assets 236
Gerätebeständen
Archivierung 262
Hinzufügen und Löschen von Asset-Feldern 241
Hinzufügen von Software-Assets 575
Importieren von Lizenzdaten 301
Informationen 300
Vorbereitung 300
Informationen 230, 248
Käufe
Anpassen 281
Bearbeiten 280
Hinzufügen 280, 281
Informationen 280
Klassische Erfassung 609
Lizenz-Asset-Typ, anpassen 285
Lizenz-Compliance 306
Anpassen des Warnungsschwellenwerts 310
Einrichten 284
Konfigurationsinformationen anzeigen 311
Lizenzen
Anpassen 274
Bearbeiten 273
Hinzufügen 273, 274
Informationen 273
Physische Assets
Hinzufügen 260
Informationen 260
Software-Assets 257, 257
Anpassen von Asset-Typen 257
Hinzufügen vom Abschnitt "Inventar" aus 258
Von Abschnitt Assets hinzufügen 258
Standorte
Anpassen 265
Bearbeiten 264
Hinzufügen 264, 265
Informationen 264
Suchen nach Assets 236, 238
Vergleichen der Assets mit dem Inventar 235
Verträge
Anpassen 270
Bearbeiten 269
Hinzufügen 269, 270
Informationen 269
Verwalten 306
Verwalten von Assets, manuell 263
Workflow für SNMP-Geräte 249
Zuweisen von Assets zu Untertypen 254, 255

Asset Management-Dashboard
Anpassen 234
Informationen 231
Asset Management-Dashboard, Administratorkonsole 231
Assistent für die Agenten-Provisionierung
Verwenden, um den Agenten auf Geräten bereitzustellen 506
Windows Geräte mit dem Tool für die Gruppenrichtlinienobjekt-Agenten-Provisionierung provisionieren 503
Assistenten
für Agenten-Provisionierung 506
für Berichterstellung 892
für Konfigurationsrichtlinien 721
für Smart Labels 155
zum Generieren von SSL-Zertifikaten 122
Aufgabenabfolge
bearbeiten 770
Hinzufügen 770
Informationen 770
Aufgabenpläne
Informationen 59
Ausführungsreihenfolge
von Organisationsfiltern 351
von Smart Labels 165
Auspacken der Appliance 74
Ausstehende Geräte
Informationen 566
Konfigurieren von Einstellungen 566
Authentifizierung
Anzeigen der Nutzung der Anmeldeinformationen 228
Google OAuth-Anmeldeinformationen 221
Office 365-Anmeldeinformationen 225
SNMP-Anmeldeinformationen 223
Verwalten von Anmeldeinformationen 216
Authentifizierung und Benutzerkonten 174

B

Bandbreite für Replikationsfreigaben 212
Bearbeiten
Käufe 280
Lizenzen 273
Standorte 264
Verträge 269
Bearbeiten von Agenten-Token 495
Bedingungsregeln
Erstellen in benutzerdefinierter Inventarisierung 639
Bedrohungsstufen 578
Befehle, die als Root ausgeführt werden müssen 532
Befehlszeilenbereitstellung
Mac OS X Agent 532
Windows Agent 526, 526
Befehlszeilenkonsole
Informationen 28
Zugriff 77
Begrüßungsmeldung, Benutzerkonsole 978

Beispiele
Importieren von Asset-Lizenzdaten 301
Mac Profil entfernen 768
Perl-Skript für Inventar-Uploads 557
Verwaltete Installation, EXE 674
Verwaltete Installation, MSI 673
Verwaltete Installation, TAR.GZ 682
XML-Schema für Windows Geräte 560
Benachrichtigungen
für Administratoren 178
Informationen 891
Serverüberwachungswarnungen 940
Benachrichtigungszeitpläne
Bearbeiten 908
Hinzufügen vom Abschnitt "Berichterstellung" aus 905
Hinzufügen von Listenseiten 907
Löschen 909
Benchmarks für SCAP 884
Benutzer-/Kennwort-Anmeldeinformationen
Hinzufügen und bearbeiten 218
Benutzer-/Kennwort-Anmeldeinformationen für LDAP
Hinzufügen und bearbeiten 219
Benutzerauthentifizierung 187
Einmalige Anmeldung mit LDAP 201
LDAP 187
LDAP-Konfiguration 188
Lokale Konten auf dem Server 174
Benutzerdefinierte Ansichten
Erstellen von Kriterien für die erweiterte Suche 67
für Service-Desk-Tickets 1023
Benutzerdefinierte Datenfelder
Hinzufügen 430
Benutzerdefinierte Felder
für Asset-Untertypen 248
benutzerdefinierte Ticketfelder
Ändern per E-Mail 1019
Definieren 1084
Benutzerdefinierte Ticketlayouts 1081, 1087, 1087, 1088
Benutzerdefinierte Ticketregeln
duplizieren 1052
Erstellen 1049
Löschen 1052
Benutzerdownloads
Entfernen von Paketen 1070
Erstellen von Paketen für 1066
Informationen 1066
Labels entfernen von 1070
Zuweisen von Labels 1070
Benutzerkonsole
Ankündigungen auf der Startseite hinzufügen 985
Anpassen 978, 980
Begrüßungsmeldung 980
Benutzerdefinierte Links auf der Startseite 988
Einstellungen 78
Erstellen von Tickets in 996
Gebietsschema-Einstellungen für 85, 91
Hinzufügen von Ticket-Links zur Startseite 989
Informationen 28
Interaktive Schaltflächen und Widgets 983
Links zu KB-Artikeln auf der Startseite 984
Logo 980
Priorität von Ankündigungen auf der Startseite 987
Schnellaktions-Ticket-Links auf der Startseite 990
Verteilungspakete 663
Benutzerkonten 187
Authentifizierung mit LDAP 187
DefaultTicketOwners 317
Frist für Sitzungen 78, 91, 125
Labels für 156
LDAP-Authentifizierung 187
LDAP-Import, geplant 195
LDAP-Import, manuell 191
Organisationsebene 174
Archivierung 184, 184
Bearbeiten 181, 183
Hinzufügen 181, 183
Verwalten 179, 350
Profile anzeigen 185
Profile bearbeiten 185
Service Desk, alle Ticketbesitzer Label für 157
Systemebene 174
Bearbeiten 175
Hinzufügen 175
Löschen 179
Verwalten 175
Zuweisen von Rollen zu 315
Benutzerprofile für Mac hinzufügen 745
Benutzerrollen
Bearbeiten 179
Hinzufügen 179
Löschen 180
Zuweisen 315
Berechtigungen für die Rolle „Service Desk-Mitarbeiter“ 314
Bereitstellen von Mac Profilen per Zeitplan 760
Bereitstellungen
im Vergleich zu Aktualisierungen 849
Bereitstellungsstatus von Geräte-Patches 832
Berichte ausführen 891
Beschleunigen des Patching mit Replikationsfreigaben 782
Best Practices für das Patchen 782
Bestandsaufnahme-Dashboard
Anpassen 366
Informationen 363
Bestandsaufnahme-Dashboard, Administratorkonsole 363
Betriebssysteme
Von der Verwaltung ohne Betriebssystem unterstützt 536
Betriebszeit und Lastdurchschnitt der Appliance 1119

C

Chrome
Anmeldeinformationen für die Authentifizierung 388
Erkennungszeitplan für Gerät 392
Client-Drop-Speicherort
Filtereinstellungen für Organisationen 341
Kopieren von Dateien auf 577
Client-ID
in Anmeldeinformationen für die Chrome-Authentifizierung verwendet 388
Code von Drittanbietern 59
Code-Zuschreibungen 59
Common Vulnerabilities and Exposures 873
Compliance
DIACAP 133
für Softwarelizenzierung 284
Computer
in Inventar suchen 491
Statistik 57
Computeraktionen (Siehe Geräteaktionen) 85
Computerbericht 879
Computerfremde Geräte
Anzeigen verfügbarer Asset-Untertypen für 254
Hinzufügen von Asset-Untertypen für 249
Zuweisen von Geräten zu Asset-Untertypen 254, 255
CSV-Format für Lizenzdaten 301
CustomerResponded-Ticketregel 1048
CVE 873

D

Daily run output 1117
Dashboard
Anpassen 43
Informationen 41
Systemebene 42
Verwaltungsebene 42
Dateien an Tickets anhängen 1027
Dateien, unterstützt durch verwaltete Installationen 665
Dateifreigabe
Aktivieren auf Systemebene 500
mit der Organisationskomponente 501
Dateigrößenfilter für Client Drop 91
Dateisynchronisierungen
Anzeigen von ITNinja-Informationen 583
Erstellen 689
Informationen 663
Datenaufbewahrung 85
Datenaufbewahrungseinstellungen 85, 91
Datenbanktabellen der
Organisationsebene 1133
Systemebene 1133
Datenbankzugriff auf Berichte 111
Datenfreigabeeinstellungen 132
Datenträgerstatus 1118
Datums- und Uhrzeiteinstellungen 100
Deaktivieren 1109
Appliance-Verknüpfung 141
Einmalige Anmeldung 202, 206
Mobilgerätezugriff
für Benutzer 137
für die Appliance 137
Nutzungsrichtlinie 134
Service Desk Zufriedenheitsumfrage 991
Sichern von Anhängen für Tickets 992
SSH für die Appliance 111
Debugging der Agenten-Software 1128
Debugging des Agenten 1128
DefaultTicketOwners
E-Mail-Benachrichtigungen für 317
Deinstallationsskripte für Windows 738
Dell
Abrufen von Garantieinformationen 570
Berichte zum Service von Dell 571
Geräteservice, Informationen 570
Services erneuern 571
Dell Aktualisierungen
Aktualisierungsdetails anzeigen 863
Anzeigen verfügbarer Aktualisierungen 862
Anzeigen von Zeitplänen 858
Konfigurieren von Dell Aktualisierungen 850
Konfigurieren von Zeitplänen 858
Patchen, im Vergleich 849
Dell Aktualisierungen, Anzeigen 862
Dell Command | Monitor
Hinzufügen
Dell Command | Monitor-Skripte 728
Informationen auf Seite „Gerätedetails“ 435
Installieren mit verwalteter Installation 728
Unterstützte Betriebssysteme 724
Unterstützte Hardware 724
Dell Data Protection | Encryption
Aktivieren der Inventarerfassung auf Windows-Geräten mit Agentenverwaltung 485
Informationen, in Gerätedetails angezeigte 479
Inventarerfassung auf ohne Agent verwalteten Windows-Geräten ermöglichen 489
Inventarerfassung von Windows Clients 485
Designeinstellungen
Standardmäßiges Appliance-Design 131
Standardmäßiges Benutzer-Design 131
Desktop-Einstellungen
Desktop-Verknüpfungen Konfigurationsskripte 730
Hintergrundbild-Konfigurationsskript 729
DIACAP-Compliance 133, 134
Diagnosedienstprogramme 1120, 1121
Dialogfeld für Konfliktwarnungen
aktivieren und deaktivieren 973
Dienstinventar verwalten 632
Digitale Assets an Anwendungen anhängen 576
Digitale Assets für die Verteilung 663
DMM
Gerätedetails 435
DNS Service Discovery (DNS-SD)-Anforderungen 111
Dokumentation
Durchsuchen des Hilfesystems 68
für MySQL 897
Domains
Beitritt des Appliance-Servers zu 120, 202
Trennen des Appliance-Servers von 206
Domains, die für das Patching zugänglich sein müssen 785
Domänenbeitritt rückgängig machen 206

Download wird durchgeführt
Appliance, Sicherungsdateien 1107
KACE GO 136
Patches 792
SCAP-Benchmarks 889
Windows-Funktionsaktualisierungen 792
Download-Quellen, alternativ 664, 664
Drucker
Anwenden der SNMP-Konfiguration auf 550
duplizieren
Agenten-Provisionierung, Zeitpläne 511
in den SQL-Berichten 898
Mac Profile 759
Organisationsrollen 339
Service Desk-Ticketwarteschlangen 1061
Skripte 718
Smart Labels 155

E

Einmalige Anmeldung
Active Directory Methode 120, 202
Aktivieren 201
Deaktivieren 202, 206
Informationen 200
SAML-Methode 206
AD in Azure als IdP verwenden 208
Verwenden von Active Directory für 202
Webbrowsereinstellungen
Firefox 205
Microsoft Edge 205
Zugriff mit Active Directory 205
Einrichten der Lizenz-Compliance 287, 601
Einrichten des Appliance-Servers 74
Einstellungen
Benutzerkonsole 78
Lokale 85, 91
POP-Server 105
Verlauf 142, 142
Einstellungen der automatischen Aktualisierung 125, 126
E-Mail
Ändern benutzerdefinierter Ticketfelder 1019
Ändern von Genehmigungsfeldern mithilfe von 1018
Ändern von Ticketattributen per 1017
Ändern von Ticketfeldern mithilfe von 1017, 1017
Anpassen der E-Mail-Vorlagen 324
Authentifizierung mit POP3 319
Automatisches Hinzufügen von Adressen zu Tickets 332
Benachrichtigung über offenes Ticket 322
Benachrichtigungen für Service Desk 318, 318, 966
Benachrichtigungen, empfohlen 322
Ereignisauslöser 321
Festlegen eines Genehmigungsfeldwerts 1019
Genehmigen von Tickets 1100
Konfigurieren des internen SMTP-E-Mail-Servers 1101
Konfigurieren eines externen SMTP-E-Mail-Servers 1102
Konfigurieren eines sicheren SMTP-E-Mail-Servers 1102
Löschen von Ticketfeldern mithilfe von 1017
POP3-Server, verwenden 319
Service Desk-Ausschlüsse 333
Testen ausgehender E-Mail-Nachrichten 1129
Testen eingehender E-Mails 1129
Testen und Fehlerbehebung 1128
Ticketabschluss, Benachrichtigung über 322
Unverschlüsselter Text mit POP3 319
Voreinstellungen 320
E-Mail bei Ereignissen konfigurieren 322
E-Mail-Benachrichtigungen für Administratoren 178
EmailOnClose-Ticketregel 1048
Energieverwaltung für Mac OS X 740
Energieverwaltung für Windows 734
Entfernen
Agenten von Linux Geräten 531
Agenten von Mac OS X Geräten 534
Anwendungssteuerungskennzeichnung 625
Labels aus Labelgruppen 168
Mac Profile aus der Appliance 769
Mac Profile von Geräten 765
Ereignisprotokoll-Reporter 731
Erfassung der Nutzung
Aktivieren für Anwendungen 614
Aktivieren für Geräte mit manuellen Labels 610
Aktivieren für Geräte mit Smart Labels 612
Datenaufbewahrungseinstellungen für 85
Informationen zum Aktivieren 610
Planen der Inventarerfassung 620
Erfassung der Softwarenutzung
Aktivieren für Anwendungen 614
Aktivieren für Geräte mit Smart Labels 612
Aktivieren mit manuellen Geräte-Labels 610
Anzeigen von Gerätedetails 618
Anzeigen von Nutzungserfassungsdetails 616, 617
Deaktivieren für Geräte mit manuellen Labels 619
Deaktivieren für Geräte mit Smart Labels 619
Deaktivieren für Softwarekatalog-Apps 619
Informationen 608
Konfigurieren von Optionen 614
Erforderliche Felder auf Service-Desk-Tickets setzen 1081
Erhöhen der Lizenzkapazität 61
Erkennen, Patch-Zeitpläne nur zum
Fehlercodes 814

Erkennung 366
Anhalten eines laufenden Zeitplans 410
Anzeigen und Suchen von Ergebnissen 409
Ergebnisse 409
Ergebnisse und Agenten-Provisionierung 410
Hinzufügen von Zeitplänen für ESXi-Hosts oder vCenter-Server 398
Hinzufügen von Zeitplänen für Hyper-V- oder SCVMM-Geräte 401
Hinzufügen von Zeitplänen für KACE Cloud Mobile Device Manager-Geräte 389
Informationen 367
Nmap 381
SCVMM-Anmeldeinformationen 404
Statistik 57
Verwaltung ohne Agent
Aktivieren 537
Verwenden von Smart Labels mit 160
Zeitpläne für Chrome-Geräte hinzufügen 392
Zeitpläne für computerfremde Geräte hinzufügen 404
Zeitpläne für schnelle Scans hinzufügen 368
Zeitpläne für umfassende Scans hinzufügen 382
Zeitpläne für Workspace ONE-Geräte hinzufügen 395
Zeitpläne löschen 411
Erkennung, stattdessen verwendeter Inventarbegriff 849
Ermittlung der Verwendung der Anmeldeinformationen 228
Erneutes Installieren des Softwarekatalogs 626
Erstellen
POP3-E-Mail-Konten 319
Tickets per E-Mail 1016
Erstellen einer Ticketvorlage 1087, 1088
Erstellen eines benutzerdefinierten Ticketlayouts 1087
Erweiterte Suche
für Inventar der Softwareseite 579
für Organisationen 356
und benutzerdefinierte Ansichten 67
und Smart Labels 67
Eskalieren von Tickets 1031, 1032, 1033
Zeitlimit 1032
Exportieren
Anmeldeinformationen 229
Mac Profile 764
Ressourcen von Appliances 358
Ressourcen von Organisationen 360
Verwaltete Installationen 696

F

Fehlende Patches 833
Fehlerbehebung 1121, 1122
Agenten-Provisionierung auf Windows-Geräten 889, 1128
Agenten-Software 1128
Appliance-Probleme 1122
E-Mail-Kommunikation 1128
Wake on LAN-Anforderungen 696
Fehlercodes
Patches 814
Skripte 814
Fehlerprotokolle
für E-Mail 1130, 1131
Feiertage für Service Desk 959
Feste Ticket-Felder 1081
Filter
Daten und LDAP, für Organisationen 351
Geräte getrennt nach Organisation 491
Hinzufügen von Datenfiltern 352
Informationen zu Datenfiltern 149
Umleiten von Geräten an Organisationen 356
Firefox Einstellungen für die einmalige Anmeldung 205
Format des Protokolldatums
nicht standardmäßig, Überwachung 924
Freigeben von Daten 132
Frist für offene, inaktive Benutzersitzungen 78, 91, 125
FTP
Sicherheitseinstellungen für 111
Zugriff auf Appliance-Sicherungen 1108

G

Gebietsschema-Einstellungen 85, 91, 128
für Benutzer 130
für Organisationen 129
Informationen 127
Konfigurieren der Administratorkonsole 127
Konfigurieren der Befehlszeilenkonsole 127
Konfigurieren der Benutzerkonsole 128
Geheimer Client-Schlüssel
in Anmeldeinformationen für die Chrome-Authentifizierung verwendet 388
Geheimschlüssel-Anmeldeinformationen
Hinzufügen und bearbeiten 216
Genehmigen von Tickets per E-Mail 1100
Genehmigungen, Tickets erforderlich 1098
Geplante Aufgabe - Status 832
Gerät
Aktivieren der Überwachung 912, 913, 914
Anwenden der SNMP-Konfiguration auf 550
Anzeigen des Status 1120
Anzeigen von DDP|E-Informationen 479, 485
Anzeigen von Statistiken für 57
Detailseite für Organisationen 356
Erkennungszeitplan für Chrome 392
Erkennungszeitplan für ESXi-Hosts oder vCenter-Server 398
Erkennungszeitplan für Hyper-V- oder SCVMM-Geräte 401
Erkennungszeitplan für KACE Cloud Mobile Device Manager 389
Erkennungszeitplan für SNMP-fähige 404
Erkennungszeitplan für Workspace ONE 395
Geräteaktionen ausführen 493
Hinzufügen von Überwachungsprofilen 924
Manuelles Hinzufügen mithilfe der API 556
Mit der Administratorkonsole manuell hinzufügen 552
Organisation erneut zuweisen 356
Patch-Status für einzelnes 826
SCVMM-Anmeldeinformationen 404
SCVMM-Geräte 404
Suchen im Inventar 491
Warnung bei Konfigurationsänderung 934
Geräte umleiten 356
Geräteaktionen 85, 91
Ausführen von der Seite "Details zum Ticket" 1029
wird ausgeführt 493
Geräteaktionen ausführen 1029

Geräteprobleme
Identifizieren von 1121
Geräteverwaltung 411, 429, 551
Geschäftszeiten für Service Desk 959, 959
Google OAuth-Anmeldeinformationen hinzufügen und bearbeiten 221
Google Play 134
Größenbeschränkungen für Ticketanhänge 1016

H

Helpdesk 953
Hilfesystem im PDF-Format 68
Hilfesystem und PDF-Datei 68
Hintergrundbild, Steuerung für Windows 729
Hinzufügen 608
Ankündigungen in der Benutzerkonsole 985
Asset-Typen 241
Benachrichtigungszeitpläne 907
Benutzerdefinierte Ansichten 67
Dateisynchronisierungen 689
Käufe 280, 281
LDAP-Labels 169
Lizenz-Assets für das Inventar der Seite "Software" 293
Lizenz-Assets für Softwarekataloginventar 287, 601
Lizenzen 273, 274
Manuelle Labels 150
Service Desk-Ticketwarteschlangen 1060
Skripte 703
Smart Labels 153
Software-Assets im Abschnitt "Assets" 575
Software-Assets im Abschnitt "Inventar" 575
Standorte 264, 265
Verträge 269, 270
Verwaltete Installationen 666
von Anwendungen zum Inventar der Softwareseite 572, 665
von Anwendungen zum Softwarekatalog 597
von Geräten zum Inventar (manuell) 551
Hinzufügen von Agent-Token 495
Hochladen
Appliance, Sicherungsdateien 1112
Mac Profile in die Appliance 759
SSL-Zertifikate für die Appliance 111
Hochladen von Dateien auf den Appliance-Server 577

I

Identifizieren von Geräten mit installierten Mac Profilen 763
Identifizieren von Geräteproblemen 1121
Importieren
Appliance-Ressourcen, Info 357
Benutzer von LDAP-Servern 191
Importieren von Lizenz-Asset-Daten 300
Mac Profile 759
Ressourcen für Appliances 359
Ressourcen für Organisationen 360
SCAP-Benchmarks 884
in den SQL-Berichten
Aktivieren des Datenbankzugriffs auf 111
Bearbeiten 899
Benachrichtigungszeitpläne 905
Benachrichtigungszeitpläne löschen 909
Benutzerdefinierte Berichte löschen 900
Benutzerdefinierte Logos für 78, 900
Duplizieren vorhandener 898
Erstellen durch SQL-Eingabe 895
Erstellen mit Berichtsassistent 892
Erstellen und bearbeiten 892
Erstellen von Listenseiten 897
für blockierte Anwendungen 624
für eine einzige Organisation 901
für mehrere Organisationen 901
Hinzufügen von Zeitplänen 902
in Zusammenhang mit Patches 827
Informationen 891
Layout 900
OVAL 879
Service von Dell 571
Sicherheitsrisikoberichte 878
SQL-Anweisungen bearbeiten 898
über Anmeldeinformationen 229
wird ausgeführt 891, 901
Zeitpläne löschen 905
zum Service Desk 1053
Inaktive Patches 834
Installationsdateien für Agent 525
Installationsprogrammdateien
Unterstützte Parameter identifizieren 667
Installieren des Agenten mit Provisionierungszeitplan 506
Installieren von Mac Profilen auf Geräten 762
Intel AMT
in Gerätedetails angezeigte Informationen 490
Interaktive Schaltflächen der Benutzerkonsole 983
Inventar
Aktualisierung erzwingen 564
Appliance 565
Linux Geräte 566
Mac OS X Geräte 566
Windows Geräte 565
Änderungsverlauf 429, 551
Ausstehende Geräte
Konfigurieren 566
Löschen 568
Zuweisen von Labels 567
Benutzerdefinierte Felder, hinzufügen 430
Datenerfassungszeitplan 431
Dell Serviceinformationen 570
Dienste
Anzeigen und Bearbeiten 632
Hinzufügen von Labels für 633
Informationen 632
Kategorisieren 634
Löschen 634
Zuweisen und Entfernen von Labels 633

Zuweisen von Bedrohungsstufen zu 634
Geräte anzeigen 494
Geräte löschen 495
Geräte suchen 491
Geräteaktionen ausführen 493
Gerätebenachrichtigungen 491
Gerätedetails 433, 434, 435, 479
Hinzufügen
Geräte manuell, Administratorkonsole 552
Software manuell 572
Software-Assets 575
von Geräten (manuell), Informationen 551
von Geräten mithilfe der API (manuell) 556
Labels für Geräte 492
Manuelle Inventarinformationen 564
Prozesse
Anzeigen und Bearbeiten 627
Hinzufügen von Labels für 628
Informationen 627
Kategorisieren 629
Löschen 629
Zuweisen und Entfernen von Labels für 628
Zuweisen von Bedrohungsstufen zu 629
Seite "Software"
Anzeigen der Elemente 572
Informationen 571
Senden von Informationen über API 556
Smart Labels für 493
Software
Bedrohungsstufe 578
digitale Assets 576
Hinzufügen von Labels für 579
ITNinja-Informationen für 582
Kategorien 579
Löschen 574
Smart Labels 580
Zuweisen und Entfernen von Labels 580
Softwarekatalog
Hinzufügen von Labels für 579
Zuweisen und Entfernen von Labels 580
Startprogramme
Anzeigen und Bearbeiten 630
Hinzufügen von Labels für 630
Informationen 630
Kategorisieren 631
Löschen 632
Zuweisen und Entfernen von Labels 631
Zuweisen von Bedrohungsstufen für 631
Störungsbehebung bei ausstehenden Geräten 568
Suchen nach Geräten 491
Übersicht 429
Verwalten von Geräten 411, 551
XML hochladen 564
Zeitplänen für 620
Inventar, stattdessen verwendeter Erkennungsbegriff 849
iOS 134
IP-Scan
Informationen 367
Übersicht 366
ITNinja
Aktivieren 582
Anzeigen von Informationen 582
Dateisynchronisierungen 583
Deaktivieren 583
Informationen 581
Verwaltete Installationen 582

J

Jetzt ausführen (Befehl)
Informationen 718
Überwachungsstatus von 720
zur Ausführung von Skripten verwenden 719

K

KACE Agent
Automatisches Aktualisieren 522
Konfigurieren 123
Manuelles Aktualisieren 523
Provisionierung mit dem Gruppenrichtlinienobjekt-Tool 502, 503
Systemanforderungen für die Installation 504
Zugriff über die Mac-Menüleiste 535
Zugriff über Windows-Taskleiste 528
KACE Cloud Mobile Device Manager
Erkennungszeitplan für Gerät 389
KACE GO 134
Aktivieren des Mobilgerätezugriffs 135
Download wird durchgeführt 136
Informationen 28
Katalogisierte Anwendungen 585
Katalogisierungsanforderungen
Auflösen benutzerdefinierter Namen 598
Senden 598
Stornieren 600
Kaufen von Lizenzen 61
KBSYS-Datenbanktabelle 1133
Kennwörter verwalten 216, 218, 219
Klassische Erfassung 609
Knowledge Base
Informationen 1071
Links zu Artikeln in der Benutzerkonsole 984
Kommentare 1026
Kommentare, zu Tickets hinzufügen 1024
Kommentar-Feldoptionen 1084
Komponenten
Aktiviert auf der Appliance 61
Übersicht 28
Konea
Informationen 123
Konfiguration
Allgemeine Einstellungen, Verwaltungsebene 85
automatische Aktualisierung, Eigenschaften 126
Datum und Uhrzeit 100
Designeinstellungen 130
Standardmäßiges Appliance-Design 131

Standardmäßiges Benutzer-Design 131
Einstellungen für Service Desk Tickets 975
Gebietsschema-Einstellungen 127
KACE Agent 123
lokale Routing-Tabellen 109
lokaler Webserver 109
mit der Organisationskomponente 78
Mobilgerätezugriff 134
Deaktivieren für Benutzer 137
Deaktivieren für die Appliance 137
für Benutzer aktivieren 136
für die Appliance aktivieren 135
Netzwerkeinstellungen 105
ohne Organisationskomponente 91
POP3-E-Mail-Konten 319
Service Desk
Importieren von Tickets aus einem anderen System 955
Service Desk-Setup-Aufgaben 954
Sicherheitseinstellungen 111
Sitzungs-Timeout 125, 125
SSL-Zertifikat 122
Zugriff durch Hosts zulassen 109
Konfigurationsrichtlinien 721
Automatische Updates unter Windows 722, 723
Deinstallationsprogramm 738
Dell Command | Monitor 728
Desktop-Verknüpfungen 730
Energieverwaltung für Mac OS X 740
Energieverwaltung für Windows Geräte 734
Ereignisprotokoll-Reporter 731
Informationen 721
MSI-Installationsprogramm 732
Registrierungseinstellungsskripte 735
Remote-Desktop-Steuerung 735
UltraVNC 736
Konfigurieren 1109
KScripts
Beziehen von Abhängigkeiten 700
Informationen 699
Standard 701
Token-Ersetzungsvariablen für 703

L

Labelgruppen
Hinzufügen und bearbeiten 166
Informationen 149
Labels entfernen von 168
Löschen 168
Zuweisen von Labels für 168
Labels
Aktivieren von LDAP-Labels 171
Anzeigen von Details zu manuellen Labels 152
Bearbeiten von Smart Labels 155
für Anwendungssteuerung 623
für Service Desk-Mitarbeiter 316
Hinzufügen und Bearbeiten von Labelgruppen 166
Hinzufügen und Bearbeiten von LDAP-Labels 169
Hinzufügen und Bearbeiten von manuellen Labels 150
Hinzufügen von Smart Labels 153
Informationen 62, 148
Labelgruppen, Informationen 149
LDAP-Labels, Informationen 149
Löschen 152
Löschen von LDAP 172
Manuell 492
Organisationsfilter 149
Service Desk, alle Ticketbesitzer 157
Smart Labels, Informationen 148
Suchen mit dem LDAP-Browser 172
Zuweisen zu Labelgruppen 168
LDAP-Browser 172
LDAP-Labels 149
Aktivieren 171
Hinzufügen und bearbeiten 169
Informationen 62
Löschen 172
Suchen mit dem LDAP-Browser 172
Variablen, die verwendet werden in 1167
LDAP-Serverauthentifizierung 187
LDAP-Serverbenutzerimport 191
Links auf der Startseite der Benutzerkonsole 988
Linux
SELinux und Serverüberwachung 910
Starten und Beenden des Agenten 531
Linux-Paket-Upgrades
Anzeigen von Zeitplänen 864
Informationen 863
Konfigurieren von Zeitplänen 864, 869
Verlauf anzeigen 871
Lizenzablauf 59
Lizenz-Assets
Hinzufügen für das Inventar der Seite "Software" 293
Hinzufügen zum Softwarekatalog 287, 601
verwalten für den Softwarekatalog 600
Lizenz-Compliance
Aktualisierung wird durchgeführt 309
Anzeigen von Compliance-Informationen 306
Einrichten 287, 601
Informationen 284
Rückgewinnen ungenutzter Softwarelizenzen 309
Lizenzinformationen 61
Lizenznutzung Warnungsschwellenwert 310
Lizenzschlüssel
Abrufen für erweiterte Serverüberwachung 914
Aktualisieren der Appliance mit erweiterter Überwachung 915
Überwachung, angerechnet auf das Lizenzlimit 912

Log Enablement Package (LEP)
Bearbeiten von Geräten mit Windows Server 2003 930
Bearbeiten von Geräten mit Windows Server 2008 oder höher 928
für die Anwendungs- und Schwellenwertüberwachung 925
Installieren 926
optional über ITNinja verfügbar 925
Protokoll für LEP-Installation 926
Logos 78, 85, 91, 350, 978, 980
Lokal katalogisierte Anwendungen
Ändern zu katalogisiert 597
anzeigen 591
Informationen 585
Lokale Authentifizierung für die Appliance 175
lokaler Webserver 109
Löschen
Agenten-Nachrichten aus Befehlswarteschlange 521
Anmeldeinformationen 230
Asset-Typen 247
Asset-Untertypen 256
Ausstehende Geräte 568
Benachrichtigungszeitpläne 909
Benutzer-Downloads 1070
Erkennungszeitpläne 411
Inventar der Seite "Software" 574
Labelgruppen 168
LDAP-Labels 172
Mac Profile aus der Appliance 769
Mac Profile von Geräten 765
Manuelle Labels 152
Organisationen 350
Organisationsfilter 355
Provisionierungszeitpläne 512
Service Desk-Ticketwarteschlangen 1061
Sicherungsdateien der Appliance 1108
Smart Labels 166
Warnungen 952
Warnungen, automatisch 933
Löschen von Ticketfeldern per E-Mail 1017

M

Mac OS X
Manuelle Bereitstellung von Agenten 532
Patchen 834
Starten und Beenden des Agenten 534
Verteilung 664
Verwaltete Installationen für 683
Mac OS X Konfigurationsrichtlinien
Energieverwaltung 740
Erzwingen von Active Directory-Einstellungen 739
für VNC 741
Mac Profile
Anzeigen von Profillisten 763
Beispiel für das Löschen von Geräten 768
Bereitstellen per Zeitplan 760
duplizieren 759
Exportieren von Mac Profil-Listen 764
Hinzufügen von Benutzerprofilen 745
Hinzufügen von Systemprofilen 753
Identifizierung von Geräten mit Profilen 763
Importieren in die Appliance 759
Installieren von Mac Profilen auf Geräten 762
Löschen aus der Appliance 769
Löschen von Geräten 765
Mac Profile verwalten 745
Mac-Geräte
KACE Agent verwalten 535
Manuelle Appliance-Sicherungen 1107
Manuelle Bereitstellung von Agenten
Anzeigen der Version 531
Befehlszeile für Windows 526
Installationsassistent für Windows 526
Installationsprogramm für Mac OS X 532
Linux Geräte 529, 530
Entfernen 531
Logon-Skript 210, 524
Mac OS X Terminalfenster 532
Per E-Mail 210, 524
Windows Geräte 525
Manuelle Labels 150
Microsoft Edge
Einmalige Anmeldung, Einstellungen für 205
Migrieren von Softwarelizenz-Assets 607
Mitarbeiterrolle erstellen 314
Mitre 873
Mobilgerätezugriff
Deaktivieren für Benutzer 137
Deaktivieren für die Appliance 137
für Benutzer aktivieren 136
für die Appliance aktivieren 135
Herunterladen von KACE GO 136
Informationen 134
Modellnummer der Appliance 59
MSI-Installationsprogramm 732
Multicast Domain Name System (mDNS)-Anforderungen 111
MySQL
Berichterstellungskennwort für 78
Dokumentationslink 895, 897
Protokollpfade 923

N

Nachverfolgen von Änderungen der Einstellungen 143
National Vulnerability Database 879
Netzwerkdienstprogramme 1120
Netzwerkeinstellungen 74
Netzwerk-Scans, Übersicht 57
Netzwerkschnittstellen-Status der Appliance 1118
Neue Patches
Verwenden von Smart Labels zur Anzeige 157
Neues Ticket
anpassen 1093

Neustarten der Appliance 1116
Nicht zulässige Anwendungen
Anwendungssteuerung 623
anzeigen 624
Entfernen der Kennzeichnung von Apps 625
Informationen 585
Nmap-Erkennung
Überlegungen 381
Notebooks, kritische Patches für 800
NTLMv2 501
NTP-Dienst
Anforderung für Patching 785
Status überprüfen von 104
Nur Besitzer, Kommentare für Tickets 1026
Nutzungsdatenfreigabe 132
Nutzungsrichtlinie 134
NVD 879

O

Objektbezeichner (OID)
Mit der Appliance abgerufen 548
Verwendet im Inventar 547, 548
Objekte, Verlaufsabonnements konfigurieren für 145
Offboard-Sicherungsübertragung 1109, 1109
Office 365-Anmeldeinformationen, Hinzufügen und bearbeiten 225
Offline-KScripts
Beziehen von Abhängigkeiten 700
Informationen 699
OID
Mit der Appliance abgerufen 548
Verwendet im Inventar 547, 548
Online-KScripts
Beziehen von Abhängigkeiten 700
Informationen 699
Standard 701
Token-Ersetzungsvariablen für 703
Online-Shellskripts
Informationen 699, 705
Organisationen
2FA konfigurieren 349
Anpassen von Logos für 350
Auswahl bei Anmeldung erforderlich 78
Benutzerkonten 350
Erweiterte Suche für Geräte 356
Filter löschen 355
Filtern von Geräten 356
Gebietsschema-Einstellungen für 129
Geräte umleiten 356
Gerätedetail-Seite 356
Hinzufügen und bearbeiten 341
Hinzufügen von Datenfiltern 352
Hinzufügen von LDAP-Filtern 353
Informationen 336
Informationen zum Filtern von Geräten 351
Löschen 350
Rollen hinzufügen und bearbeiten 338
Rollen, duplizieren 339
Rollen, Informationen über 336
Rollen, löschen 340
Standardorganisation 336
Testen von Filtern 355
Verwalten 335
Wechseln zwischen 138
Organisationsfilter
Datenfilter 149
Informationen 149
LDAP-Filter 149
Organisationskomponente 30, 336
Allgemeine Appliance-Einstellungen für 78
schnelles Wechseln zwischen Organisationen 78
Organisationsmodus 30
ORG-Datenbanktabellen 1133
OVAL
Aktualisieren der Definitionen 1117
Aktualisierungen 875
Betroffene Geräte, Label 879
Computerbericht 879
Definitionen 874
Einstellungen 875
in den SQL-Berichten 879
Labels für 875
Sicherheitsprüfungen 873
Sicherheitsrisikobericht 878
Statistik 57
Tests anzeigen 874
Tests ausführen 874
Tests und Definitionen 873
Zeitstempel 886
OVAL-Tests ausführen 874
OverdueClose-Ticketregel 1048

P

Pakete, für Patch-Verwaltung 780
Parameter für verwaltete Installationen 666
Patch-Details für ein Gerät prüfen 832
Patches 780
Fehlercodes 814

Patch-Verwaltung 780
Abonnieren von Patches 789
Anzeigen des Patch-Status 826
Anzeigen des Patch-Status von Geräten 826
Anzeigen fehlender Patches 833
Anzeigen heruntergeladener Patches 829
Anzeigen verfügbarer Patches 796
Anzeigen von Dateien in Patches 826
Anzeigen von Patch-Details 831
Anzeigen von Protokollen 834
Anzeigen von Statistiken 833
Anzeigen von Zeitplänen 816
Bereitstellungstests 781
Berichte für 827
Beschleunigen mit Replikationsfreigaben 782
Best Practices 782
Bewertungstests 781
Dell Aktualisierungen, im Vergleich 849
Dell Aktualisierungen, Zeitplanung 850, 852
Details nach Gerät 832
Downloadeinstellungen für 792
Downloadoptionen 780
Download-Status 796
Erkennen, Zeitpläne nur zum Fehlercodes 814
für Mac OS X Geräte 834
Informationen 778
Informationen zu Abonnements 785
Informationen zu kritischen Patches für Notebooks 800
Informationen zu Paketen 780
Informationen zu Signaturdateien 780
Informationen zu verwalteten Geräten erfassen 788
Konfigurieren von Zeitplänen 801, 812, 818, 824
Patches als inaktiv markieren 834
Patch-Katalog 829
Planen nicht kritischer Patches 800
Quest Software, Inc. 781
Rollback 828
Rollback-Optionen für Patches 827
Rückgängigmachen der letzten Patch-Bereitstellung 828
Smart Labels für Desktops 161
Smart Labels für kritische Betriebssystem-Patches 158
Smart Labels für Laptops 164
Smart Labels für neue Patches 159
Smart Labels für Server 163
Testumgebung 781
Verwenden von Replikationsfreigaben für 212
Verwenden von Smart Labels mit 157
Warnen der Benutzer vorab, Bedeutung 782
Websites, die zugänglich sein müssen 785
Workflow für Desktops und Server 799
Workflow für erstes Patching 788
Workflow für kritische Betriebssystem-Patches 799
Workflow für Patching 778
Zeitplanfeld-Beschreibungen 801
Zurücksetzen von Patch-Bereitstellungsversuchen 832, 832
Perl-Skript
Beispiel 557
Ping-Test
Deaktivieren 933
POP3-E-Mail-Konten
DefaultTicketOwners@meinedomain.com 319
supprt@meinedomain.com 319
POP3-E-Mail-Server 319
POP-Servereinstellungen 105
Port 443 111
Port 80 111
Port Einstellungen für die Appliance
Firewall Ausnahmen für die Appliance 102
Primäre Schlüssel für importierte Lizenzdaten 301
Profile
bearbeiten 947, 948, 949
Informationen 915
Mac Profile
Anzeigen von Profillisten 763
Bereitstellen per Zeitplan 760
duplizieren 759
Exportieren der Liste 764
Hinzufügen von Benutzerprofilen 745
Hinzufügen von Systemprofilen 753
Identifizierung von Geräten mit Profilen 763
Importieren in die Appliance 759
Informationen 744
Installieren auf Geräten 762
Löschen aus der Appliance 769
Löschen von Geräten 765
standardmäßige Überwachung 915
Überwachung
bearbeiten 916, 918
Bearbeiten von Windows Log Enablement Packages (LEP) 928, 930
Herunterladen 923
Hinzufügen zu einem Gerät 924
Hochladen 923
Informationen 915
Log Enablement Package (LEP) für Windows Server 2003 926
Neu erstellen 921, 923
SNMP-Traps 918
Protokoll für LEP-Installation
anzeigen 926
Protokolle
Anzeigen für die Appliance 1122
Daily run output 1127
E-Mail-Fehler 1131
für Patching 834
Für Skripte 742
Herunterladen für die Appliance 1127
Protokollpfade
Apache 923
MySQL 923
Provisionierung
Anzeigen der Ergebnisse 512
Zeitpläne für den Agenten 511
Proxy-Servereinstellungen 105

Prozesse
Anzeigen von Details 627
Hinzufügen von Labels für 628
Inventar, Informationen zu 627
Kategorisieren 629
Löschen 629
Zuweisen und Entfernen von Labels für 628
Zuweisen von Bedrohungsstufen zu 629

Q

Quest Software, Inc. 781

R

RAID-Laufwerkstatus 1120
Regeln
Benutzerdefinierte Inventarisierung 635, 635, 648
für Service-Desk-Tickets 1047
Regeln für benutzerdefinierte Inventarisierung
Abrufen von Werten von einem Gerät 648
Arten 635
Definieren von Regelargumenten 655
Erstellen 636
Implementierung 637
Informationen 635
Reguläre Ausdrücke zum Abgleichen von Dateinamen 654
Reguläre Ausdrücke zum Abgleichen vonDateinamen 652
Syntax 638
Testen 660
Überprüfen von Bedingungen 639
Registrierungseinstellungsskripte für Windows 735
Remote-Desktop-Steuerung 735
ReopenTicket-Ticketregel 1048
Replikationsfreigaben
Anzeigen von Details 215
für Gebietsschemata-Patches 212
Hinzufügen 212
Informationen 211, 664
Wöchentliche Zeitpläne für 212
Ressourcen
Anzeigen des Status der Exporte 361
Anzeigen von exportierten oder importierten 361
Exportieren aus Organisationen 360
Exportieren von der Appliance 358
Importieren in Appliances 359
in Organisationen importieren 360
Informationen zum Übertragen 357
Löschen des Status der Reporte 361
Verschieben von lokalen auf Netzwerkstandorte 361
Richtlinien
Konfiguration 721
Windows basierte, verwenden 722
Rollen
für Organisationen 336
für Service Desk-Mitarbeiter 314
Hinzufügen und Bearbeiten für Organisationen 338
Hinzufügen und bearbeiten, Benutzer 179
Informationen 312
Standard 337
überwachungsspezifisch 935
Zuweisen von Benutzerrollen 315
Root-Befehle 532

S

Samba Freigabe
Appliance-Einstellungen 111
Übertragen von Ressourcen zwischen Appliances 357
und Client-Drop-Speicherort für Organisationen 341
Verwaltungsebene, Einstellungen für Organisationen 85
Verwaltungsebene, Einstellungen ohne Organisationen 91
SAML
Einmalige Anmeldung, Konfiguration 206
AD in Azure als IdP verwenden 208
SCAP 879
Benchmarks anzeigen 884
Benchmarks herunterladen 889
CCE 880
CPE 880
Importieren von Benchmarks 884
Informationen zu Benchmarks 882
Informationen zu Scans 883
Konfigurieren von SCAP-Zeitplänen 885
National Vulnerability Database 879
NVD 879
OVAL 880
Protokoll 880
Scannen
Auflösungsdateien 886
Bearbeiten von Zeitplänen 886
Durchführen von Scans 880
Ergebnisse 887
Zugriff auf Scaninformationen 883
Unterstützte Plattformen 879
XCCDF 880
Schnelle Scans, für die Erkennung 368
Schnellen Wechsel von Organisationen aktivieren 138
Schritte für Aufgabenbereiche von Skripten 1150
Screenshots an Tickets anhängen 1027
Secure Content Automation Protocol 879
Seite "Software"
Funktionsvergleich mit Softwarekatalog 586
Lizenzinformationen 293
SELinux
Serverüberwachung mit 910
Senden von Katalogisierungsanforderungen 597, 598
Senden von Warnungen 696, 696
Seriennummer der Appliance 59
Server-Enhanced Linux
Auswirkung auf Serverüberwachung 910

Serverüberwachung
Aktivieren 939
Aktualisieren des Lizenzschlüssels zum Erhöhen des Limits 915
Anhalten der Überwachung 932, 932
Anwendung 925
Anzahl von Servern, die überwacht werden können 910
Arbeiten mit Warnungen 939
beim Gerät aktivieren 912, 913, 914
Deaktivieren 938
Erwerben eines Lizenzschlüssels für erweiterte 914
Fortsetzen der Überwachung 932
Informationen 910
nicht standardmäßiges Protokolldatumsformat 924
Schwellenwert 925
Suchen nach Warnungen 947
Verwenden von Profilen 915
Verwerfen von Warnungen 952
Warnungen filtern 947, 948, 948, 949
Service Desk 1027
Anpassen
Ticketauswirkungen 976, 1080
Ticketeinstellungen 1074
Ticketfelder 1084
Ticketkategorien 976
Ticketlayout 1087
Ticketlayouts 976, 1081
Ticketprioritäten 976, 1078
Ticketstatus 976, 1077
Bearbeiten 1034
Berichte ausführen 1053
E-Mail
Benachrichtigungsstrategie 318
Ereignisauslöser 321
Fehler 1131
Fehlerbehebung 1128
Fehlerbehebung ausgehender E-Mail-Nachrichten 1129
Fehlerbehebung eingehender E-Mail-Nachrichten 1129
Fehlerprotokolle 1130
Konfigurieren von Einstellungen 318, 966
Testen ausgehender E-Mail-Nachrichten 1129
Testen eingehender E-Mails 1129
Verbinden von Servern mit der Appliance 1100
Voreinstellungen 320
Importieren von Tickets aus einem anderen System 955
Knowledge Base
Anhänge, Hinzufügen 1071
Benutzerbewertungen und -ansichten 1073
Externe Links für 1071
Hinzufügen von Artikeln 1071
Löschen von Artikeln 1073
Markdown verwenden 1071
Konfigurieren
E-Mail-Ausschlüsse 333
E-Mail-Einstellungen 332
Externe SMTP-E-Mail-Server 1102
Geltende Bedingungen für Tickets 972
Interne SMTP-E-Mail-Server 1101
Titel des Service Desk 972
Widget-Datenspeicher 335
Labels und Rollen für Mitarbeiter 316
Mitarbeiterrolle 314
Organisieren von doppelten Tickets 1098
Prozesse
Arten 1042
Hinzufügen 1034
Löschen 1046
Umwandeln in reguläre Tickets 1046
Verwendung 1034, 1043, 1043, 1044, 1045
Setup-Aufgaben für 954
Sichern von Anhängen 111, 992
Standardbenutzerrollen für 312
Systemanforderungen für 953
Testen von E-Mails
Verwenden von Telnet 1130
Ticketgenehmiger konfigurieren 1099
Ticketgenehmiger verwenden 1098
Tickets
anzeigen in Warteschlangen 1062
Kategorien und Unterkategorien, erstellen 1074
Kommentare nur für Besitzer 1026
Lebenszyklus von 996
Links in der Benutzerkonsole 989
Schnellaktions-Links auf der Benutzerkonsole 990
Umwandeln in Prozesstickets 1047
über-/untergeordnete Tickets 1094, 1095
Übergeordnete Tickets als Aufgabenliste 1097
Übergeordnete Tickets, aktivieren 1095
Übersicht 953
Untergeordnete Tickets 1094, 1095
Untergeordnete Tickets erstellen 1096
verhindern
unnötigen E-Mail-Verkehr 334
Verwalten
Ticketvorlagen 1087, 1088
Warteschlangen
Aktivieren von Konfliktwarnungen 973
Antwortvorlagen konfigurieren 974
Anzeigen von Tickets in allen Warteschlangen 1062
duplizieren 1061
Festlegen als Benutzerstandardeinstellung 1063
Festlegen als Standardeinstellung 1062
Hinzufügen 1060
Informationen 1059
Konfigurieren 961
Löschen 1061
Standardfelder für alle Warteschlangen 1064
Verschieben von Tickets zwischen 1065
Zufriedenheitsumfrage 990
Zuweisen von übergeordneten Tickets 1097
Service Desk-Dashboard
Anpassen 995
Informationen 993
Service Desk-Dashboard, Administratorkonsole 993
Service für Dell Geräte, Informationen 570
Shellskripts 705
Shell-Unterstützung
SSH 546

Sicherheit 873
Einstellungen für die Appliance 111
für Service Desk-Anhänge 992
Informationen zu OVAL 873
Konfigurationsprobleme 873
Sicherheitslücken 873
SSL-Zertifikate 122
Überwachung mittels Security Run Output 890
Sicherheits-Dashboard
Anpassen 777
Informationen 774
Sicherheits-Dashboard, Administratorkonsole 774
Sicherheits-Dashboard-Widgets
Ansichten 774
Bereitgestellte Patches 774
Berichte 774
Dell Aktualisierungen 774
Fehlerhafte Patches 774
Freigegebene Patches 774
Gesamt-Compliance nach Computer 774
Gesamt-Compliance nach Patch 774
Patch-Aufgaben abgeschlossen 774
Patch-Installationsfortschritt 774
SCAP-Zusammenfassung 774
Windows 10 Versionen 774
Sicherungen
Aktivieren 1109
Deaktivieren 1109
Einstellungen für Sicherungen 111
Informationen 1105
Löschen von Sicherungsdaten 1108
Manuell 1107
Offboard-Übertragung konfigurieren 1109, 1109
Zeitplanung und Aufbewahrung 1106
Sicherungsdateien
Download wird durchgeführt 1107
Hochladen 1112
Wiederherstellen 1113
Signaturdateien, für Patching 780
Sitzungs-Timeout
Informationen 78, 91, 125
Verlängern 990
Verlieren nicht gespeicherter Änderungen 990
Zurücksetzen 78, 91, 125
Skripte
Aufgaben, die automatisiert werden können 699
ausführen über die Seite mit den Skriptdetails 720
ausführen über die Skript-Seite 720
Bearbeiten 715
Beziehen von Abhängigkeiten 700
Dateien protokollieren für 742
duplizieren 718
Exportieren 744
Fehlercodes 814
Hinzufügen 705
Importieren 716, 717
Jetzt ausführen 718, 719
KScripts 705
Löschen 716, 716
Online-Shellskripts 705
Schritte hinzufügen 1150
Standard 701
Token-Ersetzungsvariablen für 703
wiederverwenden 718
Windows basierte Richtlinienassistenten 722
Windows Registrierungseinstellungen 735
Workflow 703
Skripterstellung
Anzeigen von Skript-Aufgaben 887
Durchsuchen von Protokollen 742
'Jetzt ausführen'-Status 720
Mac Profile
Anzeigen von Profillisten 763
Bereitstellen per Zeitplan 760
Duplizieren von Mac Profilen 759
Exportieren von Mac Profil-Listen 764
Hinzufügen oder Bearbeiten von Benutzerprofilen 745
Hinzufügen oder Bearbeiten von Systemprofilen 753
Identifizierung von Geräten mit Profilen 763
Importieren von Profilen in die Appliance 759
Informationen 744
Installieren von Mac Profilen auf Geräten 762
Löschen aus der Appliance 769
Löschen von Geräten 765
Richtlinien und Skripte bearbeiten 742
SLA
Aktivieren 960
Feiertage für Service Desk 959
Geschäftszeiten konfigurieren 959
Konfigurieren 960
Smart Labels 148
Bearbeiten 155
für Desktops 161
für Erkennungsergebnisse 160
für Geräteinventar 493
für kritische Betriebssystem-Patches 158
für Laptops 164
für neue Patches 159
für Patching 157
für Server 163
Hinzufügen 153
kombinieren 154
Löschen 166
Verwalten 153
zum Service Desk 156
Zuweisen der Ausführungsreihenfolge von 165

SMTP-Server
Überprüfen der Einstellungen 1119
Verbinden mit der Appliance 1100
verwenden anstelle von POP3 319
SNMP
Druckervorlagen 550
Erkennungszeitplan für Gerät 404
für die Appliance aktivieren 111
Hinzufügen und Bearbeiten von Anmeldeinformationen 223
Inventarkonfigurationen 547, 548, 548, 550
Vollständiger Durchlauf 404
Software
Bereitstellung über die Benutzerkonsole 1066
Deinstallationsprogramm 738
Entfernen von Benutzer-Downloads 1070
Smart Labels 580
Statistik 57
Software-Assets 257, 575
Anpassen 257
für Lizenz-Compliance 575
Hinzufügen aus dem Inventar 258
Von Abschnitt Assets hinzufügen 258, 575
Softwarekatalog
Aktualisieren der Lizenz-Compliance für 309
Aktualisierung und Neuinstallation 626
Anwendungskategorien 585
Anzeigen der Lizenz-Compliance für 306
Anzeigen erkannter Anwendungen 589
Anzeigen nicht erkannter Anwendungen 589
Anzeigen nicht katalogisierter 590
Anzeigen nicht zulässiger Anwendungen 624
Anzeigen von Softwaredetails 592
Benutzerdefinierte Namen 598
Datenfreigabe 586
Entfernen der lokalen Katalogisierung 600
Funktionsvergleich mit Seite "Software" 586
für Organisationen 586
Hinzufügen von Anwendungen 597
Informationen 584
Informationen zu katalogisierten Anwendungen 585
Informationen zu nicht zulässigen Anwendungen 585
Informationen zur Datenerfassung 585
ITNinja 586
Klassifizierungen 584
Konfigurieren von Erfassungsoptionen für 614
Lizenz-Assets migrieren 607
Lizenz-Compliance für 284
Lizenzinformationen 287, 601
Lokal katalogisiert in katalogisiert ändern 597
Lokal katalogisierte Anwendungen 585, 591
Lokalisierung 586
Planen der Erfassung 620
Planen der Inventarerfassung 620
Rückgewinnen ungenutzter Softwarelizenzen 309
Senden von Katalogisierungsanforderungen 597, 598
Smart Label-Einschränkungen 153
Softwarelizenzen 600
Stornieren von Katalogisierungsanforderungen 600
und Anwendungssteuerung 623
Verwaltete Installationen 608
Softwarelizenz-Compliance
Aktualisierung wird durchgeführt 309
anzeigen 306
Informationen 284
Rückgewinnen ungenutzter Softwarelizenzen 309
Software-Version der Appliance 59
Softwareverteilung
Hinzufügen von Anwendungen für 665
Informationen 661
Testen 662
Übersicht 57
Sonderzeichen
Escape-Sequenzen in Überwachungsprofilen 949
SQL-Abfragen
Datenbank-Tabellennamen für 1133
Dokumentation 897
für Berichte 895
und Smart Labels 155
SSH für die Appliance aktivieren 111
SSLv3 (ältere Version von SSL) 111
SSL-Zertifikate hochladen 111
SSL-Zertifikate, Assistent 122
SSO 200
Standard-Designeinstellungen 130
Standardeinstellung für Tickets
Ansichten verwenden 1021
Festlegen einer Ansicht als Standardeinstellung 1024
Kategorien, Status und Prioritäten 976
Standardorganisation, Informationen 336
Standardrollen 312
Standardwarteschlange 1062
Starten und Beenden des Agenten auf dem Mac 534
Starten und Beenden des Agenten unter Linux 531
Startprogramm-Inventar
Anzeigen und Bearbeiten 630
Hinzufügen von Labels für 630
Kategorisieren 631
Löschen 632
Verwalten 630
Zuweisen und Entfernen von Labels 631
Zuweisen von Bedrohungsstufen für 631
Startseite, Administratorkonsole 41
Statistik
Computer 57
Geräte 57
OVAL 57
Software 57
Status der RAID-Laufwerke 1120
Status von Patch-Downloads 796
Suche
Dokumentation 68
erweitert
Benachrichtigungen 65
Smart Labels 65
Online-Hilfe 68
Seitenebene 64, 64
Verwaltungsebene 63
Suchen nach Geräten im Inventar 491
Support-Informationen
ITNinja 581
Synchronisieren von Dateien 689

Syntax
für Aufgabenbereiche von Skripten 1150
Regeln für benutzerdefinierte Inventarisierung 638
zum Ändern benutzerdefinierter Ticketfelder per E-Mail 1019
zum Löschen von Ticketfeldern per E-Mail 1017
Systemanforderungen
für die Agenteninstallation 504
für die Appliance 74
zum Service Desk 953
Systemebene 30, 78
Benutzerkonten 175
Dashboard 42
mit der Organisationskomponente 40
Systemprofile für Mac 753
Systemverwaltungskonsole 30

T

Technische Daten der Appliance 74
Technische Daten, Appliance 28
Technischer Support Tether 1121
Telnet zum Testen eingehender E-Mails 1130
Terminalfenster 77
Testen
Bereitstellung, für Patch-Verwaltung 781
Bewertung, für Patch-Verwaltung 781
eingehende E-Mails 1129
LDAP-Labels 169
LDAP-Serverkonfiguration 188
Organisationsfilter 355
Regeln für benutzerdefinierte Inventarisierung 660
Tether zu Quest 1121
Ticketdetail
anpassen 1084, 1093
Ticketdetails anpassen 1084, 1093
Ticket-Layoutfelder 1081
Ticketlayoutvorschau 1093
Ticketregeln 1047
Anpassen von Systemregeln 1047
duplizieren 1052
Erstellen 1049
Löschen 1052
Standardwerte für Systemregeln 1048
Verschieben zwischen Warteschlangen 1053, 1053
Verwenden von Systemregeln 1047
Tickets
Ändern benutzerdefinierter Felder per E-Mail 1019
Ändern der Feldreihenfolge 1087
Ändern per E-Mail 1017
Ändern von Feldern per E-Mail 1017
Ändern von Genehmigungsfeldern per E-Mail 1018
Anhänge an 1027
Anhänge, Hinzufügen 1027
Anmerkung anzeigen 1026
Anpassen
Auswirkungswerte 1080
Prioritätswerte 1078
Statuswerte 1077
Ticketeinstellungen 1074
Arbeitsinformationen für 1020
Archivierung
Aktivieren 1054
Informationen 1054
Löschen von Tickets aus 1058
von ausgewählten Tickets 1057
Warteschlangeneinstellungen für 1056
Wiederherstellen von Tickets 1058
aus einem anderen System importieren 955
Benachrichtigung über Abschluss 322
Benachrichtigung über Eskalation 322
Benachrichtigung über Öffnung 322
Benutzerdefinierte Ansichten für 1023
Benutzerdefinierte Felder, definieren 1084
benutzerdefinierte Felder, die Sie per E-Mail ändern können 1019
Benutzerdefinierte Layouts für 1087
Duplikate, organisieren 1098
Erstellen
auf der Seite Asset-Detail 1009
auf der Seite Gerätedetail 1008
aus Serverüberwachungswarnungen 941, 1010
in der Administratorkonsole 999
in der Benutzerkonsole 996
Erstellen von Status 976
Erstellung per E-Mail aktivieren 1016
Eskalation 1031
E-Mail-Empfänger 1032
E-Mail-Nachricht für 1033
Frist ändern 1033
Frist, Informationen 1032

Informationen 1032
Fälligkeitsdaten und SLAs 959, 959, 960
Felder auf Formular auf „Erforderlich“ setzen 1081
Felder, die per E-Mail geändert werden können 1017
Festlegen der Standardansicht 1024
Genehmigen per E-Mail 1100
Genehmigungen konfigurieren 1099
Genehmigungen, anfordern 1098
Genehmigungsfelder, die per E-Mail geändert werden können 1018
Größenbeschränkungen für Anhänge 1016
Informationen zu benutzerdefinierten Layouts 1081
Kategorien und Unterkategorien, erstellen 1074
Kategorien, Werte CC-Liste für 332
Kommentare nur für Besitzer, Hinzufügen 1026
Kommentare, hinzufügen 1024
Konfigurieren von Einstellungen für 975
Lebenszyklus von 996
Links auf der Startseite der Benutzerkonsole 989
Löscheinstellungen für 1058
Löschen aus Warteschlangen 1059
Löschen von Feldern per E-Mail 1017
Navigieren zwischen verwandten Elementen 1019
Per E-Mail erstellen 1016
Schnellaktions-Links auf der Benutzerkonsole 990
Screenshots hinzufügen 1027
Senden von Informationen per e-Mail 1029
SLA-Einstellungen für 960
Standardansichten verwenden 1021
Standardstatus von 976
Status 1032
Über-/untergeordnete Beziehungen aktivieren 1095
über-/untergeordnete Beziehungen verwenden 1094
Übergeordnet
Verwendung als Aufgabenliste 1097
Verwendung zur Organisation von Duplikaten 1098
Verlauf anzeigen 1028
Vorlagen für 1087, 1088
Zusammenführen 1030
über die Seite „Ticketdetail“ 1030
über die Seite „Ticketliste“ 1030

Timeout für Benutzersitzungen 990

Timing von E-Mails vom Service Desk 321

Token-Ersetzung
für Service Desk-E-Mail 324
Variablen für Skripte 703

Tool für die Gruppenrichtlinienobjekt-Agenten-Provisionierung
Agenten bereitstellen mit 502, 503
Vorbereiten des Systems für die Verwendung 503

U

Übergeordnete Tickets
Aktivieren zum Abschließen untergeordneter Tickets 1095
Hinzufügen vorhandener Tickets 1097
Verwendung als Aufgabenliste 1097

Überprüfen auf Ausführung des Agenten auf Linux Geräten 531

Überprüfen auf Ausführung des Agenten auf Mac Geräten 534

Übertragen von Ressourcen zwischen Appliances 357

Überwachung
Anhalten für ein Gerät 932
Anhalten für mehrere Geräte 932
auf einem Gerät aktivieren 939
Bearbeiten eines Profils 916, 947, 948, 949
SNMP-Traps 918
Bearbeiten von Windows Log Enablement Packages (LEP) 928, 930
bei in Frage kommenden Geräten aktivieren 912, 913, 914
Deaktivieren für ein Gerät 938
Erstellen eines neuen Profils 921
Erstellen von Benutzerrollen 935
Erstellen von Service-Desk-Tickets aus Warnungen 941, 1010
Filtern unerwünschter Warnungen 947, 948, 949
Fortsetzen für mehrere Geräte 932
Hinzufügen eines Profils zu einem Gerät 924
Profil herunterladen 923
Profile hochladen 923
Server 910
Verwenden von Profilen 915
Zurücksetzen eines Standardprofils auf die Werkseinstellungen 916

Uhrzeit- und Datumseinstellungen 100

UltraVNC-Skript für Windows 736

Umbenennen des Service Desk 972

Untergeordnete Tickets für ein beliebiges Ticket erstellen 1096

Untertypen für Assets
Anzeigen auf der Seite "Assets" 254
Anzeigen verfügbarer Untertypen 254
Bearbeiten 253
Festlegen als Standardeinstellung 253
Hinzufügen 249
Informationen 248
Löschen 256
Workflow für SNMP-Geräte 249
Zuweisen oder ändern 254, 255

V

Variablen
, die in Skripten verwendet werden 703
für Service Desk-E-Mail 324
verwendet in LDAP-Labels 1167

Verknüpfung von KACE SMAs
Aktivieren 139
Deaktivieren 141
Hinzufügen von Namen und Schlüsseln 140
Informationen 139
Zugriff auf Federation-API-Einstellungen aktivieren 141

Verlauf anzeigen
Linux-Paket-Upgrade 871

Verlaufseinstellungen
Abonnements für Organisationen 143
anzeigen 144
Asset-Abonnements 144
Assets anzeigen 145
Informationen 142
Objektabonnements 145
Objekte anzeigen 146
Systemebene 143
und die Organisationskomponente 142
Verschieben von Ressourcen auf Netzwerkstandorte 361
Verschlüsselung
Gerätedetails 435
Version der Appliance-Software 59
Version des Agenten auf Linux Geräten 531
Version des Agenten auf Mac Geräten 534
Verteilung
Mac Profile 760
Software 661
Verteilungspakete
für Mac OS X 664
Informationen 663
Informationen zum Anhängen digitaler Assets 663
Inventaranforderung für 663
Verwenden alternativer Download-Quellen 664, 664
Verwalten des Dienstinventars 632
Verwalten des Prozessinventars 627
Verwalten des Startprogramm-Inventars 630
Verwalten von Anmeldeinformationen 216
Verwalten von Geräten 411, 429, 551
Verwaltete Installationen
Beispiel für eine RPM-Datei 675
Erstellen für Windows 667
EXE, Beispiel 674
Exportieren 696
Hinzufügen zum Softwarekatalog 608
Informationen 663, 665
Informationen zum Erstellen 666
Installationsprogramm Dateiparameter 667
ITNinja 582
Mac OS X Plattform 683
MSI-Beispiel 673
Parameter für 666
TAR.GZ-Beispiel 682
ZIP-Beispiel 674
Verwaltung ohne Agent 536
Gerätedetails 547
Gerätedetails löschen 547
Hinzufügen von Windows Registrierungsschlüsseln für Zugriff auf DDP|E-Informationen 489
Manuell aktivieren 538
Unter Verwendung von Erkennungsinformationen aktivieren 537
Unterstützte Betriebssysteme 536
Verfügbare Funktionen für verwaltete Geräte 412
Verwaltungsebene 30
Allgemeine Einstellungen 78
Dashboard 42
Verwerfen von Warnungen, automatisch 933
VNC-Einstellungen, Mac OS X Richtlinien für 741
Voreinstellungen für Datenfreigabe 132
Vorlagen
für Konfigurationsrichtlinien 721
für Service Desk-E-Mail 324

W

WaitingOverdue-Ticketregel 1048
Wake on LAN
Ausgeben von Anforderungen 692
Fehlerbehebung 696
Informationen 692
Planen von Anforderungen 693
Warnungen 696
automatisches Löschen 933
automatisches Verwerfen 933
Beenden für Wartungsaufgaben 934
Erstellen für Broadcast 696
Erstellen von Service-Desk-Tickets aus 941, 1010
für geänderte Gerätekonfigurationen 934
Konea-Verbindung erforderlich für 696
Löschen 952
Suchen nach 947
Übersicht 57
Unerwünschte herausfiltern 947, 948, 948, 949
Verwerfen 952
verworfene abrufen 952
Warnungsschwellenwert für die Lizenznutzung 310
Warteschlangen
Aktivieren von Konfliktwarnungen 973
Anpassen von Ticketdetails für 976
Antwortvorlagen konfigurieren 974
Festlegen als Benutzerstandardeinstellung 1063
Festlegen als Standardeinstellung 1062
Hinzufügen 1060
Informationen 1059
Konfigurieren 961
Löschen 1061
Standardfelder für alle Warteschlangenlisten 1064
Verschieben von Ticketregeln zwischen 1053
Verschieben von Tickets zwischen 1065
Wartungsfenster
Planen zum Beenden der Warnungsgenerierung 934
Websites, die für die Appliance zugänglich sein müssen 104
Werkseinstellungen, wiederherstellen 1114
Widget-Datenspeicher
Service Desk-Konfiguration von 335
Widgets
Abgelaufene Verträge 231
Ablaufende Verträge 231
Assets nach Standort 231
Assets nach Status 231
Assets nach Typ 231
Bestandsaufnahme-Dashboard-Widgets 363
Anzahl der Agent-Versionen 363
Anzahl der VMware ESXi-Versionen 363
Bestandszählungen 363
Geräte nach Datenträgerkapazität 363
Geräte nach Hersteller 363
Geräte nach Modell 363
Geräte nach Prozessor 363
Geräte nach Speicher 363

Geräte nach Untertyp 363
Geräteanmelderate 363
Geräteberichte 363
Provisionierte Plattformen 363
Provisionierung 363
Verbindungen 363
Verknüpfungen 363
Verwaltete Betriebssysteme 363
VMware ESXi-Gerät nach Status 363
VMware-Geräteanzahl 363
VMware-Geräteberichte 363
Dashboard-Widgets auf der Startseite 44
Abgelaufene Verträge 44
Abgeschlossene Tickets 44
Ablaufende Dell Services 44
Ablaufende Verträge 44
Aktive Tickets 44
Aktive Tickets nach Benutzer 44
Aktive Tickets nach Kategorie 44
Aktive Tickets nach Priorität 44
Aktuelle Skripte 44
Am häufigsten aufgerufene Knowledge Base-Artikel 44
Ansichten 44
Anzahl der VMware ESXi-Versionen 44
Assets nach Standort 44
Assets nach Status 44
Assets nach Typ 44
Aufgaben werden durchgeführt 44
Bereitgestellte Patches 44
Berichte 44
Compliance der kritischen Patches 44
Dateisynchronisierungen 44
Datenträgerkapazität 44
Dell Aktualisierungen 44
Durchschnittliche Ticket-Auflösungszeit 44
Erneut geöffnete Tickets 44
Fehlerhafte Patches 44
Freigegebene Patches 44
Geräte nach Datenträgerkapazität 44
Geräte nach Hersteller 44, 44
Geräte nach Modell 44, 44
Geräte nach Prozessor 44
Geräte nach Speicher 44
Geräte nach Untertyp 44
Geräteanmelderate 44
Gesamt-Compliance nach Computer 44
Gesamt-Compliance nach Patch 44
Heute fällige Tickets 44, 44
Heute geöffnete Tickets 44
Heute überfällige Tickets 44
Installierte, aber in 60 Tagen nicht verwendete Software 44
Kosten der ungenutzten Lizenzen nach Produkt 44
Letzte Nachrichtenartikel 44
Lizenz-Compliance 44
Patch-Aufgaben abgeschlossen 44
Patch-Installationsfortschritt 44
Provisionierte Plattformen 44
Provisionierung 44
SCAP-Zusammenfassung 44
Softwareherausgeber 44
Softwarelizenz-Konfiguration 44
Softwaretitel 44
Überfällige Tickets 44, 44
Überfällige Tickets nach Benutzer 44
Übersicht über Überwachungswarnungen 44
Überwachte Geräte 44
Überwachungswarnungen 44
Verbindungen 44
Verknüpfungen 44
Verwaltete Betriebssysteme 44, 44
Verwaltete Installationen 44
VMware ESXi-Gerät nach Status 44
VMware-Geräteanzahl 44
VMware-Geräteberichte 44
Wartung abgelaufener Software-Lizenzen 44
Wartung ablaufender Software-Lizenzen 44
Windows 10 Versionen 44
für die Benutzerkonsole 983
Installierte, aber in 60 Tagen nicht verwendete Software 231
Kosten ($) von ungenutzten Lizenzen nach Produkt 231
Lizenz-Compliance 231
Service Desk-Dashboard-Widgets 993
Abgeschlossene Tickets 993
Aktive Tickets 993
Aktive Tickets nach Benutzer 993
Aktive Tickets nach Kategorie 993
Aktive Tickets nach Priorität 993
Ansichten 993
Berichte 993
Durchschnittliche Ticket-Auflösungszeit 993
Erneut geöffnete Tickets 993
Heute fällige Tickets 993, 993
Heute geöffnete Tickets 993
Heute überfällige Tickets 993
Überfällige Tickets 993, 993
Überfällige Tickets nach Benutzer 993
Verknüpfungen 993
Sicherheits-Dashboard-Widgets 774
Compliance der kritischen Patches 774
Softwareherausgeber 231
Softwarelizenz-Konfiguration 231
Softwaretitel 231
Wartung abgelaufener Software-Lizenzen 231
Wartung ablaufender Software-Lizenzen 231
Wiederherstellen der Appliance-Einstellungen 1111
Windows
Dell Command | Monitor 728
Einstellungen für automatische Updates 723
KACE Agent verwalten 528
Manuelle Bereitstellung des KACE Agent 526, 526
Windows Gruppenrichtlinie
Verwenden, um den Agenten mit dem Tool für die Provisionierung bereitzustellen 502, 503
Windows Konfigurationsrichtlinien
See Konfigurationsrichtlinien
Windows Richtlinien 722
Windows Server 2003
Überwachung des Log Enablement Package (LEP) von ITNinja 926

Windows-Funktionsaktualisierungen
Aktualisierungen abonnieren 835
Aktualisierungsdetails anzeigen 848
Anzeigen verfügbarer Aktualisierungen 847
Anzeigen von Zeitplänen 842
Downloadeinstellungen für 792
Informationen 835
Konfigurieren von Zeitplänen 836, 842
Windows-Funktionsaktualisierungen abonnieren 835
Windows-Funktionsaktualisierungen, anzeigen 847
Workflow
für Asset-Untertypen und SNMP 249
für die Verwendung von Ticketgenehmigern 1098
für Patch-Abonnements 788
für Patching 778
Workspace ONE
Erkennungszeitplan für Gerät 395
Workstations, Patching-Workflow für 799

X

XML-Editor, für Skripte 715
XML-Schema
Linux und Mac 563
Windows 559

Z

zahlreiche E-Mails
Service Desk verhindert 334
Zeitplanung
Bereitstellung von Windows-Funktionsaktualisierungen 836, 842
Dell Aktualisierung bereitstellen 858
Dell Aktualisierungen 852
Erfassung von Anwendungen im Softwarekatalog 620
Erkennungsscans 368
in den SQL-Berichten 902
Inventarerfassung für den Softwarekatalog 620
Inventarerfassung, Geräte 431
LDAP-Benutzerimporte 191
Linux-Paket-Upgrades 864, 869
Mac Profile für die Bereitstellung 760
Patch-Bereitstellung 801, 812, 818, 824
SCAP-Scans 885
täglichen Sicherungen 1106
Wake on LAN-Anforderungen 693
Zertifikat für SSL 111
Zertifizierung, DIACAP 134
Zufriedenheitsumfrage
Ändern von Labels für 991
Verhinderung der Verteilung von 991
Verwendung 990
Zugehörige Ticketfelder 1081
Zugriff auf Anwendungen wird verweigert
Editionen mit gemeinsamen ausführbaren Dateien 622
Zugriff auf Federation-API-Einstellungen aktivieren
Appliance-Verknüpfung 141
Zugriff durch Hosts zulassen 109
Zurücksetzen von Patch-Bereitstellungsversuchen
über die Patch-Katalog-Seite 832
über die Seite "Patch-Detail" 832
Zustand der E-Mail-Systeme 1119
Zuweisen von Benutzerrollen 315