Quest

KACE® Systemverwaltungs-Appliance 10.0

Versionshinweise

Inhaltsverzeichnis

Quest® KACE® Systemverwaltungs-Appliance 10.0 – Versionshinweise

Dieses Dokument enthält Informationen zur KACE Systems Management Appliance (SMA) Version 10.0.

Über die KACE Systemverwaltungs-Appliance 10.0

KACE Systems Management Appliance (SMA) ist eine virtuelle Appliance, die zur Automatisierung der Geräteverwaltung, der Anwendungsbereitstellung, des Patchings, des Asset Managements und der Service Desk-Ticketverwaltung entwickelt wurde. Weitere Informationen zu Appliances der KACE SMA Serie finden Sie unter https://www.quest.com/products/kace-systems-management-appliance/. Diese Version enthält eine Reihe neuer Funktionen, behobener Probleme und Sicherheitsverbesserungen.

Neue Funktionen und Erweiterungen

Diese Version der KACE Systemverwaltungs-Appliance (SMA) beinhaltet die folgenden Funktionen und Erweiterungen:

Service Desk-Funktionen

Diese Version der KACE Systemverwaltungs-Appliance (SMA) beinhaltet die folgenden Service Desk-Funktionen und -Erweiterungen:

- **Ticketvorlagen**: Mit dieser Funktion können Sie verschiedene Tickettypen innerhalb derselben Warteschlange erstellen. Mit dieser Funktion können Sie die Informationen, die Ihre Endbenutzer für verschiedene Anforderungsszenarien bereitstellen, besser kontrollieren, ohne mehrere Ticketwarteschlangen erstellen und verwalten 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.
- **Bedingte Felder in Ticketvorlagen**. Sie können in jeder Ticketvorlage eine bedingte Logik konfigurieren, um auf der Ticketseite bestimmte Felder basierend auf den zuvor ausgewählten Werten ein- oder auszublenden. Wenn Sie beispielsweise eine Ticketvorlage für Druckerprobleme haben, können Sie verschiedene Felder anzeigen, die für verschiedene Arten von Druckerproblemen relevant sind.

Asset Management-Funktionen

Diese Version von KACE Systems Management Appliance (SMA) beinhaltet folgende Asset Management-Funktionen.

- **Geplanter Asset-Import**: Ab dieser Version können Sie mithilfe des Assistenten *Assets importieren* einen geplanten Import von Assets aus einer CSV-Datei (durch Trennzeichen getrennte Datei) konfigurieren, die sich auf einer Netzwerkfreigabe befindet. Der Assistent enthält eine neue Seite, *Zeitplan für Asset-Importauswahl*, auf der Sie bei Bedarf aus verfügbaren Zeitplanmustern auswählen können.
- **Möglichkeit zur Zuordnung des Felds „Asset-Status“ während des Asset-Imports**: Auf der Seite *Zuordnung* im Assistenten *Assets importieren* können Sie das Feld *Asset-Status* einer Spalte in der CSV-Datei zuordnen. Dies ist nützlich, wenn Sie eine hohe Anzahl von Assets importieren müssen, wobei jedes Asset einen bestimmten Status aufweist (z. B. *Aktiv*). Wenn Sie diese Zuordnung nicht angeben, wird jedem importierten Asset-Eintrag der Standardstatus zugewiesen, der mit dem ausgewählten Asset-Typ verknüpft ist.
- **Administratoren können verhindern, dass Benutzer ohne Administratorrechte Assets löschen**: Die Seite *Details zum Asset-Typ* enthält nun die Option **Benutzern ohne Administratorberechtigungen das Löschen von Assets erlauben**, mit der Administratoren angeben können, ob Benutzer ohne Administratorrechte Assets löschen können. 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.
- **Appliance-Administratoren können Asset-Typen ohne die Felder „Standort“ und „Benutzer“ erstellen**. Es gibt bestimmte Asset-Typen (z. B. Käufe oder Verträge), bei denen diese Informationen nicht von Belang sind. Die Seite *Details zum Asset-Typ* enthält nun die Option **Speicherorteinstellungen anzeigen**, mit der das Feld *Standort* für den ausgewählten Asset-Typ ein- oder ausgeschlossen werden kann. Ebenso wird der Wert für den Asset-Bevollmächtigten nur für den Asset-Typ „Gerät“ angezeigt.

Endpunkt-Kommunikationsfunktionen

Diese Version der KACE Systemverwaltungs-Appliance (SMA) beinhaltet die folgenden Endpunkt-Kommunikations-Funktionen und -Erweiterungen:

- **Ermitteln von Microsoft Hyper-V- oder System Center Virtual Machine Manager (SCVMM)-Geräten**: Wenn Ihr Unternehmen eine virtuelle Hyper-V-basierte Umgebung verwendet, können Sie die Appliance verwenden, um Microsoft Hyper-V- oder SCVMM-Geräte durch Erkennungszeitplanung zu ermitteln. Um Ihr Netzwerk nach Hyper-V- oder SCVMM-Geräten zu durchsuchen und Informationen über diese Geräte zu erfassen, fügen Sie einen authentifizierten Erkennungszeitplan hinzu. Für jedes SCVMM-/Hyper-V-Gerät

ist eine Lizenz ohne Agent notwendig. Wenn das Gerät auch über einen KACE-Agenten verfügt, ist zudem eine Lizenz für den Agenten notwendig.

- **Akkuinformationen wurden zu den Gerätedetails hinzugefügt**: Die Seite *Gerätedetails* enthält nun eine neue Gruppe von Feldern, *Akkus*, die Akkuinformationen für Windows-, Linux- und MacOS-Geräte mit und ohne Agenten anzeigen. Diese Gruppe umfasst folgende Felder:
  - **Ladestand**: Die aktuelle Akkukapazität in Prozenten.
  - **Chemie**: **Nur Windows- und Linux-Geräte**. Der Akkutyp, z. B. Lithium-Ionen usw.
  - **Stromleistung (mWh)**: Die Akku-Stromleistung.
  - **Vorgesehene Kapazität (mWh)**: Die vorgegebene maximale Kapazität des Akkus.
  - **Vollständige Ladekapazität (mWh)**: Maximale Stromleistung des Akkus. Dieser Wert nimmt mit der Zeit ab.
  - **Integrität (%)**: Der Prozentsatz der Akku-Stromleistung im Vergleich zur vorgegebenen maximalen Kapazität.
  - **Hersteller**: Der Akkuhersteller.
  - **Name**: Der Name oder das Modell des Akkus.
  - **Angeschlossen**: Eine Anzeige dafür, ob der Akku derzeit an eine Stromquelle angeschlossen ist.
  - **Anzahl der Aufladungen**: **Nur MacOS-Geräte**. Die Anzahl der Ladevorgänge des Akkus.
  - **Seriennummer**: Die Seriennummer des Akkus.
  - **Verbleibende Zeit (Minuten)**: Die Anzahl der Minuten, nach deren Ablauf der Akku entladen ist. Wenn das Gerät an eine Stromquelle angeschlossen ist, ist dieses Feld leer.
- **Möglichkeit zum Hochladen und Verteilen von cURL-Zertifikatpaketen**: 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 wurden, auf die im Standard-Agentenpaket nicht verwiesen wird. Ab dieser Version können Sie die Einstellung *CA-Zertifikat-Paketdatei* auf der Seite *Agenten-Einstellungen* verwenden, um ein benutzerdefiniertes cURL-CA-Paket hochzuladen oder die Einstellung auf Standard zurückzusetzen.
- **Remote-Steuerung**: Integration in eine Lösung von Drittanbietern für die Remote-Steuerung von Windows-, Mac- und Linux-Systemen. *SimpleHelp* wird jetzt als Option unter *Geräteaktionen* auf der Seite *Allgemeine Einstellungen* angezeigt. Weitere Informationen zu diesem Tool finden Sie in der SimpleHelp-Dokumentation.
- **Kontinuierliche Integration mit KACE Cloud Mobile Device Manager (MDM)**:
  - **Anzeigen von Informationen zu Geräten, die bei KACE Cloud Mobile Device Manager (MDM) registriert sind**: Die Appliance zeigt Informationen zu Mac OS X-Geräten an, die bei einer integrierten KACE Cloud MDM-Instanz registriert sind. Die Art der für solche Geräte verfügbaren Informationen hängt davon ab, ob auf ihnen ein KACE-SMA-Agent installiert ist.
  - **Die Geräteverwaltungsmethode wird unter Gerätedetails angezeigt**: Das neue Feld *Geräteeintragstyp* auf der Seite *Gerätedetails* mit der Verwaltungsmethode des ausgewählten Geräts: *Gerät mit Agent*, *Gerät ohne Agent*, *Manuell eingegebener Datensatz* oder *Agent/ohne Agent* (KACE Cloud MDM-Hybridinventar).
  - **Trennen einer Geräteverbindung von KACE Cloud MDM**: Klicken Sie für Geräte ohne Agent, die bei KACE Cloud MDM registriert sind, zum Entfernen der Gerätezuordnung zu KACE Cloud MDM und

zum Zurücksetzen auf reine Agenteninventardatensätze auf der Seite *Gerätedetails* auf **Agentenlose Integration entfernen**.

- **KBRSL wurde von dem Gerät entfernt**: `KBRSL` ist nicht mehr im Bereitstellungscode enthalten. Vorhandene `KBRSL`-Bereitstellungszeitpläne werden zur Verwendung von WinRM konvertiert.
- **Integration mit KACE Systems Deployment Appliance (SDA)**: Die KACE SDA-Konfigurationsinformationen in der Inventaransicht KACE SMA *Gerätedetail* werden mit dem KACE-Agenten ausgefüllt.
- **Notfallwarnmodus**: Eine neue Option wird der Seite „Warnungsdetails“ für den Modus „Notfallwarnmodus“ hinzugefügt. Wenn diese Option ausgewählt ist, wird die Warnmeldung 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.
- **Hinzufügen der systemeigenen Skriptvariablen des Betriebssystems für den nativen Windows-Registrierungsspeicher**: Ab dieser Version können Sie `NAT` zu `HKLM` (`HKEY_LOCAL_MACHINE`) hinzufügen, um bei Bedarf auf 32- oder 64-Bit-Registrierungsspeicher in Skriptaufgaben zuzugreifen. Beispiel: `HKLMNAT\Software\ABC`.

Infrastrukturfunktionen

Diese Version der KACE Systemverwaltungs-Appliance (SMA) beinhaltet die folgenden Infrastruktur-Funktionen und -Erweiterungen:

- **KACE SMA-Patching-Lösung**: In dieser Version wurde eine vollständige KACE SMA-Patching-Lösung für MS Windows und Mac OS hinzugefügt. 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 heruntergeladen. Quest bietet sichere, zeitnahe und qualitativ hochwertige Patch-Signaturen für Windows- und Mac-Betriebssysteme sowie viele gängige Anwendungen.

  HINWEIS: Vor der Verwendung dieser Funktion müssen Sie nach der Aktualisierung auf 10.0 einen Patch-Download ausführen.

  - Smart Labels, die vor Version 6.0 erstellt wurden, müssen manuell aktualisiert werden, bevor 10.0 auf eine assistentenbasierte Version angewendet wird.
  - Ein Upgrade auf 10.0 mit einer großen Anzahl von Patch-Erkennungs- oder Patch-Bereitstellungsergebnissen kann zu längeren Upgrade-Zeiten führen.
  - Nach dem Upgrade auf diese Version wird auf der Seite *Zusammenfassung* eine Warnmeldung angezeigt, die alle veralteten Berichte, Ticket-Regeln oder benutzerdefinierten Filter auflistet.
  - Ein neuer integrierter Bericht, *Softwarekatalog-Anwendungen erkannt, aber im Anwendungs-Patching nicht verfügbar*, ist verfügbar, um im Softwarekatalog erkannte Software anzuzeigen, die nicht durch KACE-Patching gepatcht werden kann. Dies kann bei der Überprüfung von Third Party Software auf Sicherheitsupdates hilfreich sein.
  - In dieser Version ist ein neuer Bericht, *KACE-Patch-Diskrepanzen*, enthalten. Während des Upgrade-Prozesses werden vorhandene Patching-Daten nach Möglichkeit in das neue Format konvertiert. Dieser Bericht enthält Patches, die nicht konvertiert werden können.
- **Verwenden der Security Assertion Markup Language (SAML) für die einmalige Anmeldung**: Sie können die Appliance so konfigurieren, dass Benutzer ohne Angabe ihrer Anmeldeinformationen auf der Willkommensseite mit einem Authentifizierungstool eines Drittanbieters authentifiziert werden. 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. Verwenden Sie die Seite *SAML-Einstellungen*, um diese Funktion zu konfigurieren.
- **Möglichkeit zum Senden von Daten an einen Syslog-Server**: Jetzt können Sie die Appliance konfigurieren, um begrenzte Serverprotokolldaten an einen Remote-`Syslog`-Server zu senden. Wählen Sie hierzu auf der Seite *Sicherheitseinstellungen* die Option **Remote-Syslog aktivieren** aus und geben Sie

im Feld *Remote-Syslog-Server* den vollqualifizierten Domänennamen (FQDN) oder die IP-Adresse und die Port-Nummer des Remote-`Syslog`-Servers an.

- **Anzahl der betroffenen Geräte, die für das Software-Inventar verfügbar sind**: Die Seite mit der Liste der *Software* enthält nun das Feld *Betroffene Geräte* in der erweiterten Suche.
- **Verschieben des Fokus auf Listenseiten zur Unterstützung des Barcode-Scannens**. Beim Laden einer Listenseite wechselt der Fokus auf das Suchfeld auf der Seite. Dies wird durch den Cursor im Textfeld angezeigt. Dies wird implementiert, um das Scannen von Barcodes zu unterstützen.

Behobene Probleme

Im Anschluss finden Sie eine Liste mit Problemen, die in dieser Version behoben wurden:

Behobene Probleme

Behobenes Problem	ID des Problems
Die Installation über die KACE Cloud Mobile Device Manager (MDM)-Bereitstellung kann aufgrund eines abgelaufenen Zertifikats mit dem Installationsprogramm für den Mac OS-Agent 9.1.204 fehlschlagen.	K1-20620
Der Upload des Mac OS-Profils kann zu Fehlern führen.	K1-20563
Der Upload des Mac OS-Profils führte dazu, dass die `Klasse „NetworkSettingsUtil“ nicht gefunden` wurde.	K1-20561
Archivierte übergeordnete Tickets konnten nicht angezeigt werden.	K1-20557
Sonderzeichen in westeuropäisch (ISO) codierten E-Mails wurden nicht korrekt angezeigt.	K1-20549
Einige Modelle von Dell Chromebooks konnten evtl. nicht erkannt werden, wenn als Hersteller Dell aufgeführt war.	K1-20544
Sicherungsdateien konnten unnötig groß sein.	K1-20543
Die Daten zur Lizenz-Compliance werden möglicherweise nicht aktualisiert, wenn sie sich mit dem Backup-Fenster überschneiden.	K1-20542
Die Optionen *Timeout bei Erkennung* und *Timeout bei Bereitstellung* über zwei Stunden standen (fälschlicherweise) zur Auswahl.	K1-20533
Neue Zeilen des Kommentars wurden gemeinsam ausgeführt, wenn sie aus der Prozessvorlage kommen.	K1-20528
Die Arbeitsinformationen wurden manchmal nicht angezeigt, nachdem die Seite auf der Seite *Ticketdetails* neu geladen wurde.	K1-20522
Token für eingehende E-Mails funktionierten nicht, als sie von einer Ticketregel gesendet wurden.	K1-20458
Der Agent wurde aufgrund eines abgelaufenen Zertifikats manchmal als Virenschutzsoftware erkannt.	K1-20457

Behobenes Problem	ID des Problems
Die Aktualisierung von Compliance-Daten konnte unnötig lange dauern.	K1-20450
Der Asset-Bericht des Assistenten mit benutzerdefiniertem Benutzerfeld war leer, es sei denn, `OWNER_ID` wurde festgelegt.	K1-20446
Der Asset-Import hat `OWNER_ID` für Nicht-Gerätetypen nicht festgelegt.	K1-20445
Benutzer ohne E-Mail-Einstellung konnten Tickets, die nicht zu ihnen gehören, auf der Seite mit der Liste der *Tickets* sehen.	K1-20441
Ausstehend (Missing in action, MIA): Das Archiv funktionierte nicht wie erwartet für Geräte ohne entsprechende Assets.	K1-20438
Die Asset-Archivierung konnte nicht nach Zeitplan ausgeführt werden, wenn ein Backup durchgeführt wurde.	K1-20431
Das Laden einer Seite mit Software-*Asset-Details* konnte sich verlangsamen, wenn eine große Anzahl installierter Softwareelemente vorhanden war.	K1-20430
Patchen: Die Auswahl des Betriebssystem wurde beim Speichern ohne Benachrichtigung entfernt, wenn alle Geräte ausgewählt wurden.	K1-20417
Nicht standardmäßige Berechtigungen konnten verhindern, dass die mobile Kace GO-App Geräte korrekt auflistet.	K1-20405
Das Popup-Feld *Standort ändern* wurde nicht im französischen Gebietsschema angezeigt.	K1-20400
Beim Erstellen eines neuen Assets konnte der Standard-Untertyp auf *Keine* statt auf den Standard-Untertyp gesetzt werden.	K1-20398
Elemente, die vor der vollständigen Replikation entfernt wurden, konnten weiterhin in der *ToDo*-Liste angezeigt werden.	K1-20396
Bei der Bereitstellung von Zeitplanlisten wurden keine Stunden oder Minuten für den Zeitplan *Ausführen alle* oder *Ausführen um* angezeigt.	K1-20394
Eine Garantieprüfung von Dell Geräten, die zum Wert *Ungültig* führt, konnte zukünftige Garantieprüfungen desselben Geräts verhindern.	K1-20385
Ein Smart Label zur Entdeckung mit ungültiger SQL-Kennung konnte dazu führen, dass der gesamte Scan fehlschlägt.	K1-20374
Beim Senden eines Tickets per E-Mail mit einem archivierten Benutzer konnten mehrere Benutzer erstellt werden.	K1-20369
E-Mail-Benachrichtigungen über Ticket-Updates konnten nicht erstellt werden.	K1-20360
Verknüpfungen in geplanten HTML-Assistentenberichten sind fehlgeschlagen, wenn der Bericht per E-Mail geöffnet wurde.	K1-20351

Behobenes Problem	ID des Problems
Das Dropdown-Feld *Geräte* auf der Skriptseite *Jetzt ausführen* konnte bei der Verwendung von Bezeichnungen für den Geräteumfang viel Zeit in Anspruch nehmen.	K1-20347
Das Löschen eines großen Asset-Verlaufs konnte fehlschlagen.	K1-20344
Der Task-Zeitplan konnte manchmal nicht auf einer Appliance mit vielen Replikatoren geladen werden.	K1-20342
Die Option `Suchstruktur` im *LDAP-Browser* konnte möglicherweise nicht ausgeführt werden.	K1-20327
Die Bereitstellung von Mac-Profilen ist aufgrund eines falschen Agentenpfads fehlgeschlagen.	K1-20321
Das Ticket wurde in der Ansicht *Alle meine Tickets* angezeigt, wenn ein Benutzer mit ähnlicher E-Mail-Adresse zur CC-Liste hinzugefügt wurde.	K1-20304
Dunkler Designtext/-hintergrund im Prozessassistenten hatte zu wenig Kontrast.	K1-20290
Das Agent-Installationsprogramm konnte versehentlich `userinit`-Werte von Drittanbietern aktualisieren, wenn sie den Substring `userinit.exe` enthielten.	K1-20286
Einige bereitgestellte virtuelle Maschinengeräte haben die VMware-Geräteaktionen auf der Seite *Gerätedetails* nicht angezeigt.	K1-20285
Vordefinierter Bericht: Computer, die nach freien Kapazitätsbereichen aufgelistet sind, haben Ergebnisse falsch gruppiert.	K1-20275
Die Nachricht `Die Genehmigung des übergeordneten Elements ist erforderlich, bevor das Ticket abgeschlossen werden kann` konnte fälschlicherweise angezeigt werden.	K1-20267
Die erweiterte Suche im Feld *Status* funktionierte auf der Seite *Patch-Katalog* nicht.	K1-20091
Das Messungssymbol konnte fälschlicherweise für Windows-Geräte ohne Agent angezeigt werden, bei denen das Messungslabel hinzugefügt wurde.	K1-20061
Die Timeout-Einstellung in Ermittlungszeitplänen hat sich nicht wie erwartet verhalten.	K1-20012
Der Chip Count im Inventar konnte für Raspberry Pi falsch sein.	K1-20007
Leere oder doppelte BIOS-Seriennummer mit zugehöriger doppelter MAC-Adresse konnte dazu führen, dass Inventardatensätze fälschlicherweise überschrieben wurden.	K1-19988
Blacklisting-Prozesse haben nicht immer die gesamte Prozessstruktur beendet. Dies führte zu verwaisten untergeordneten Prozessen und konnte in extremen Fällen den Speicher auf dem Endpunkt erschöpfen.	K1-19905

Behobenes Problem	ID des Problems
Bei der Verwendung von Offline-Patching konnten die Offline-Quelle und das Offline-Ziel unterschiedliche aktive, inaktive und deaktivierte Zählwerte haben.	K1-19873
Patch-Feed-E-Mails konnten nicht gesendet werden, da die SMTP-Konfiguration in den Netzwerkeinstellungen nicht beachtet wurde.	K1-19816
Die erweiterte Suche *beginnt nicht mit* schlägt für Gruppen wie Labelnamen und Softwaretitel fehl.	K1-19814
Das Dell BIOS-Update startet den Client möglicherweise nicht neu, wenn er per Push übertragen wird, sodass er erst nach einem Neustart vollständig installiert werden kann.	K1-19770
Vordefinierter Bericht: *In den letzten 7 Kalendertagen hinzugefügte oder geänderte Benutzer* war ungenau.	K1-19703
Neue-Zeile-Zeichen in der Neustartmeldung von Dell Updates konnte dazu führen, dass der Neustart nicht abgeschlossen wurde.	K1-19569
Manuell hinzugefügte Geräte konnten durch den nächtlichen MIA-Bereinigungsprozess versehentlich gelöscht werden.	K1-19531
Die MI-Bereitstellungsreihenfolge wird zwischen von Software und Katalog-Software verwalteten Installationen (MIs) möglicherweise nicht korrekt durchgesetzt.	K1-19512
Wenn ein Software-Inventarelement nicht-englische Zeichen enthielt, konnten Smart Labels nicht korrekt ausgeführt werden.	K1-19507
Die Formatierung in einer vom Kunden definierten Meldung zum *Patch-Neustart* wurde nicht berücksichtigt.	K1-19492
Beim LDAP-Import konnten Attribute ausgeschlossen werden, die nicht in allen Datensätzen gefunden wurden.	K1-19406
Dell XPS-Modelle wurden von Dell Updates nicht unterstützt.	K1-19282
Ein benutzerdefiniertes Benutzerfeld für ein Asset, das den zugewiesenen Benutzern in Berichten falsch zugeordnet wurde.	K1-19226
Das Laden der Seite *Software*-Inventar konnte viel Zeit in Anspruch nehmen.	K1-18985
Fehler beim Patch-Download konnten inkorrekt gemeldet werden.	K1-18930
Wenn Sie im *Patch-Katalog* auf den Fehler-Link klicken, wird möglicherweise die Meldung *Keine Geräte gefunden* angezeigt.	K1-18721
Smart Labels, die auf Softwaretitel und -version abzielen, konnten falsche Ergebnisse liefern.	K1-18398
Die auf dem Clientcomputer angezeigte Meldung zum Neustart des Patches spiegelt möglicherweise nicht das wider, was im Patch-Zeitplan konfiguriert ist.	K1-18215

Behobenes Problem	ID des Problems
In der in Azure gehosteten KACE SMA-Konsole wurde ein fehlerhaftes Fragezeichen „?“ festgestellt.	ESMP-6820
Der Abschnitt Kommentare für Tickets wurde nicht gelöscht, wenn Kommentare und Anhänge gleichzeitig hinzugefügt wurden.	ESMP-6672
Das Ticket konnte zu einem abgeschlossenen Ticket zusammengeführt werden.	ESMP-6671
Die Suchfunktion wurde für Benutzer mit eingeschränktem Zugriff unterbrochen, wenn die Option „Anzeigen nach“ auf *Meine Elemente* eingestellt ist.	ESMP-6633
Leere Seite *Patch-Details* beim Klicken auf den Patch der Seite unter dem Abschnitt *Ersetzt* auf der Seite *Patch-Details*.	ESMP-6591
Die Verarbeitung von Agenteninventaren mit einer fehlenden Liste von Netzwerkschnittstellen schlägt möglicherweise fehl.	ESMP-6588
Der Abschnitt *SDA-Einstellungen* auf der Seite *Anzuzeigende Felder* des Systemberichtsassistenten fehlte.	ESMP-6468
Die Suche nach Geräten mit *SDA-Bereitstellungszeit* funktionierte auf der Seite mit der Liste der *Geräte* mit der erweiterten Suche nicht.	ESMP-6467
HTML-Tags wurden manchmal unter in der Spalte *Kommentare und Lösung* in Service Desk-Berichten angezeigt.	ESMAS-4552
Durch das Zusammenführen von zwei Tickets mit demselben Übermittler wurden diese der CC-Liste hinzugefügt.	ESMAS-4537
Übermittler konnten ihre Tickets nicht sehen, wenn sie in eine Warteschlange verschoben wurden, für die der Übermittler keine Berechtigungen hatte.	ESMAS-4516
Es war nicht möglich, auf der Seite *Standortdetails* im Abschnitt *Zugewiesene Assets* nach der Spalte *Typ* zu sortieren.	ESMAM-1897

Bekannte Probleme

Die folgenden Problem sind zum Zeitpunkt dieser Freigabe bekannt.

Allgemeine bekannte Probleme

Bekanntes Problem	ID des Problems
WinRM: Die Bereitstellung auf neueren Versionen von MS Windows-Geräten unter Verwendung eines alternativen Speicherorts wird nicht unterstützt.	K1-20616
`TICK:XXXX`-Links im Kommentarabschnitt funktionieren nicht mehr.	K1-20558
Umleitungsfehler können nach Abschluss des Upgrades auftreten.	ESMP-7010

Bekanntes Problem	ID des Problems
Problemumgehung: Löschen Sie den Cache und starten Sie den Browser neu.	
Bei Verwendung von *Alle Patches erkennen* können Timeout-Fehler auftreten.	ESMP-7005
Bei SAML-Attributzuordnungen wird derzeit zwischen Groß- und Kleinschreibung unterschieden.	ESMP-6887
Mac OS-Patches in manuellen Labels werden nach dem Upgrade auf 10.0 nicht mehr auf dem Label angezeigt.	ESMP-6536
OVAL-Scan schlägt auf Windows Server 2019 mit Timeout-Fehler fehl.	ESMP-6535
Patchen: Alte Regeln für benutzerdefinierte Tickets, die auf Patches verweisen, funktionieren nicht mehr.	ESMP-6176
`KUserAlert` kann unter MS Windows 7 falsch gerendert werden, wenn Schriftarten auf 125 % oder 150 % eingestellt sind.	ESMEC-3461
Die SNMP-Durchlaufdaten sind in den Ermittlungsergebnissen und Bestandsdaten nicht verfügbar, wenn SNMP-Version „SNMPv2c“ für einige Microsoft Windows-Geräte verwendet wird. Folgende Windows-Geräte sind betroffen: • Windows 10 (1709 und höher) • Windows Server 2016 (1709 und höher) • Windows Server 2019 (alle Versionen) **Problemumgehung**: Wählen Sie die SNMP-Version *SNMPv1* aus, um dieses Problem zu vermeiden.	ESMEC-3263
Der KACE-Agent wird auf Geräten mit SUSE Linux Enterprise Server Version 15 und openSUSE Leap Version 15 nicht unterstützt, wenn SELinux installiert und aktiviert ist.	ESMEC-3100
Agent kann auf SLES v.15 nicht mit Fehlern installieren. **Problemumgehung**: Stellen Sie vor der Installation des Agenten auf SLES v.15 sicher, dass auf dem System die folgenden Pakete installiert sind: • `cups-client` • `pciutils` • `psmisc`	ESMEC-2987
Der Import und Export von Ticket-Vorlagen in der Warteschlangenkonfiguration (als Ressource) wird derzeit nicht unterstützt.	ESMAS-4631
Einmalige SAML-Anmeldung wird derzeit in KACE GO nicht unterstützt.	ESMAS-4585

Systemanforderungen

Die mindestens erforderliche Version für die Installation von KACE SMA Version 10.0 ist 9.1. Wenn auf Ihrer Appliance eine frühere Version ausgeführt wird, müssen Sie eine Aktualisierung auf die angegebene Version durchführen, bevor Sie die Installation fortsetzen können.

Für ein Upgrade des KACE SMA Agenten ist mindestens Version 7.1 erforderlich. Wir empfehlen die Ausführung der neuesten Agentversion mit KACE SMA 10.0.

Um die Versionsnummer der Appliance zu überprüfen melden Sie sich bei der Administratorkonsole an und klicken Sie auf **Hilfe**. Klicken Sie auf der angezeigten Hilfefeld auf die umkreiste Schaltfläche „**i**“.

Vergewissern Sie sich vor der Aktualisierung auf Version 10.0 bzw. der Installation von Version 6.3, dass das System die Mindestanforderungen erfüllt. Diese Anforderungen werden in den technischen Daten der KACE SMA erläutert.

- Virtuelle Appliances: Weitere Informationen finden Sie unter https://support.quest.com/technical-documents/kace-systems-management-appliance/10.0-common-documents/technical-specifications-for-virtual-appliances/.
- KACE als Dienst: Weitere Informationen finden Sie unter https://support.quest.com/technical-documents/kace-systems-management-appliance/10.0-common-documents/technical-specifications-for-kace-as-a-service/.

Produktlizenzierung

Falls Sie derzeit eine KACE SMA Produktlizenz besitzen, ist keine zusätzliche Lizenz erforderlich.

Wenn Sie die KACE SMA zum ersten Mal verwenden, finden Sie ausführliche Informationen zur Produktlizenzierung im Handbuch zur Appliance-Einrichtung. Das entsprechende Handbuch finden Sie unter .

HINWEIS: Produktlizenzen für Version 10.0 können nur für KACE SMA Appliances mit Version 6.3 oder höher verwendet werden. Lizenzen für Version 10.0 können nicht auf Appliances verwendet werden, auf denen ältere KACE SMA-Versionen wie etwa Version 6.0 ausgeführt werden.

Installationsanweisungen

Sie können diese Version mit einer mitgeteilten Aktualisierung oder durch das manuelle Hochladen und Anwenden einer Aktualisierungsdatei anwenden. Anweisungen hierzu finden Sie in den Abschnitten zu den folgenden Themen:

- Aktualisierung vorbereiten
- Eine Aktualisierung manuell hochladen und anwenden
- Aufgaben nach der Aktualisierung

HINWEIS: Um die Genauigkeit der Softwareerkennung und Installationszahlen für Geräte mit einer bestimmten Software ab KACE SMA Version 7.0 sicherzustellen, wird der Softwarekatalog bei jedem Upgrade neu installiert.

Aktualisierung vorbereiten

Befolgen Sie vor der Aktualisierung Ihres KACE SMA Servers die folgenden Empfehlungen:

- **Überprüfen Sie die KACE SMA Serverversion**:

  Die mindestens erforderliche Version für die Installation von KACE SMA Version 10.0 ist 9.1. Wenn auf Ihrer Appliance eine frühere Version ausgeführt wird, müssen Sie eine Aktualisierung auf die angegebene Version durchführen, bevor Sie die Installation fortsetzen können.

  Um die Versionsnummer der Appliance zu überprüfen melden Sie sich bei der Administratorkonsole an und klicken Sie auf **Hilfe**. Klicken Sie auf der angezeigten Hilfefeld auf die umkreiste Schaltfläche „**i**“.

- **Überprüfen Sie die KACE SMA Agentenversion**.

  Für ein Upgrade des KACE SMA Agenten ist mindestens Version 7.1 erforderlich. Wir empfehlen die Ausführung der neuesten Agentversion mit KACE SMA 10.0.

- **Führen Sie eine Sicherung durch, bevor Sie beginnen**.

  Sichern Sie Ihre Datenbank und Ihre Dateien und legen Sie diese für spätere Zwecke an einem Speicherort außerhalb des KACE SMA Servers ab. Anweisungen zur Sicherung Ihrer Datenbank und Ihrer Dateien finden Sie im Administratorhandbuch, https://support.quest.com/technical-documents/kace-systems-management-appliance/10.0-common-documents/administrator-guide/.

- **Stellen Sie sicher, dass Port 52231 verfügbar ist**.

  Vor einem `.kbin`-Upgrade muss Port 52231 verfügbar sein, damit die Seite KACE Upgrade-Konsole zugänglich ist. Wenn das Upgrade initiiert wird, ohne diesen Port verfügbar zu machen, können Sie den Fortschritt des Upgrades nicht verfolgen. Quest KACE empfiehlt dringend, Datenverkehr von einem vertrauenswürdigen System zum SMA über Port 52231 zuzulassen und das Upgrade von der Upgrade-Konsole aus zu überwachen. Ohne Zugriff auf die Upgrade-Konsole wird das Upgrade zu einer Seite umgeleitet, auf die nicht zugegriffen werden kann, was im Browser als Timeout angezeigt wird. Dies kann den Anschein vermitteln, dass das Upgrade das System zum Absturz gebracht hat, woraufhin häufig der Kasten neu gestartet wird, obwohl das Upgrade noch ausgeführt wird. Wenn Sie sich nicht sicher sind, wie weit das Upgrade fortgeschritten ist, wenden Sie sich an den KACE-Support und **starten Sie die Appliance nicht neu**.

Aktualisieren des KACE SMA Servers mit einer beworbenen Aktualisierung

Sie können den KACE SMA Server mithilfe einer Aktualisierung aktualisieren, die auf der Seite *Dashboard* oder *Appliance-Aktualisierungen* der Administratorkonsole zur Verfügung gestellt wird.

VORSICHT: Während einer Aktualisierung dürfen Sie keinen manuellen Neustart des KACE SMA Servers durchführen.

1. Sichern Sie Ihre Datenbank und die entsprechenden Dateien. Anweisungen hierzu finden Sie im Administratorhandbuch (https://support.quest.com/technical-documents/kace-systems-management-appliance/10.0-common-documents/administrator-guide/).
2. Navigieren Sie zur *Systemsteuerung* der Appliance:
   - Wenn die Organisationskomponente auf der Appliance nicht aktiviert ist, klicken Sie auf **Einstellungen**.
   - Wenn die Organisationskomponente auf der Appliance aktiviert ist: Melden Sie sich an der Systemverwaltungskonsole der Appliance an: `http://`KACE_SMA_hostname`/system`. Oder

wählen Sie rechts oben auf der Seite aus der Dropdown-Liste die Option **System** aus und klicken Sie dann auf **Einstellungen**.

3. Klicken Sie auf der linken Navigationsleiste auf **Appliance-Aktualisierungen**, um die Seite *Appliance-Aktualisierungen* anzuzeigen.
4. Klicken Sie auf **Überprüfen**, ob aktuelle Versionen verfügbar sind.

   Die Ergebnisse der Überprüfung werden im Protokoll angezeigt.
5. Wenn eine Aktualisierung verfügbar ist, klicken Sie auf **Aktualisieren**.

   WICHTIG: Während der ersten 10 Minuten stürzen einige Browser scheinbar ab, während die Aktualisierung entpackt und überprüft wird. Verlassen oder aktualisieren Sie die Seite während dieses Zeitraums nicht und klicken Sie nicht auf Browserschaltflächen auf der Seite, da diese Aktionen den Vorgang unterbrechen würden. Nachdem die Aktualisierung entpackt und überprüft wurde, wird die Seite *Protokolle* angezeigt. Starten Sie die Appliance während des Aktualisierungsvorgangs nicht manuell neu.

   Die Version 10.0 wird angewandt und der KACE SMA Server wird neu gestartet. Der Bearbeitungsstatus wird im Browserfenster und in der Administratorkonsole angezeigt.
6. Wenn das Server-Upgrade abgeschlossen ist, aktualisieren Sie alle Agenten auf Version 10.0.

Eine Aktualisierung manuell hochladen und anwenden

Wenn Sie eine Aktualisierungsdatei von Quest erhalten haben, können Sie diese manuell hochladen, um den KACE SMA Server zu aktualisieren.

VORSICHT: Während einer Aktualisierung dürfen Sie keinen manuellen Neustart des KACE SMA Servers durchführen.

1. Sichern Sie Ihre Datenbank und die entsprechenden Dateien. Anweisungen hierzu finden Sie im Administratorhandbuch (https://support.quest.com/technical-documents/kace-systems-management-appliance/10.0-common-documents/administrator-guide/).
2. Melden Sie sich mit Ihren Kundenanmeldeinformationen auf der Quest Website an: https://support.quest.com/kace-systems-management-appliance/download-new-releases. Laden Sie die `KBIN`-Datei des KACE SMA Servers für die allgemein verfügbare Version 10.0 GA (general availability, Allgemeine Verfügbarkeit) herunter und speichern Sie sie lokal.
3. Klicken Sie auf der linken Navigationsleiste auf **Appliance-Aktualisierungen**, um die Seite *Appliance-Aktualisierungen* anzuzeigen.
4. 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 Version 10.0 wird angewandt und der KACE SMA Server wird neu gestartet. Der Bearbeitungsstatus wird im Browserfenster und in der Administratorkonsole angezeigt.
5. Wenn das Server-Upgrade abgeschlossen ist, aktualisieren Sie alle Agenten auf Version 10.0.

Aufgaben nach der Aktualisierung

Überprüfen Sie im Anschluss an die Aktualisierung, ob diese erfolgreich war und die richtigen Einstellungen festgelegt sind.

Erfolgreichen Abschluss überprüfen

Überprüfen Sie den erfolgreichen Abschluss, indem Sie die KACE SMA Versionsnummer kontrollieren.

1. Navigieren Sie zur *Systemsteuerung* der Appliance:
   - Wenn die Organisationskomponente auf der Appliance nicht aktiviert ist, klicken Sie auf **Einstellungen**.
   - Wenn die Organisationskomponente auf der Appliance aktiviert ist: Melden Sie sich an der Systemverwaltungskonsole der Appliance an: `http://`KACE_SMA_hostname`/system`. Oder wählen Sie rechts oben auf der Seite aus der Dropdown-Liste die Option **System** aus und klicken Sie dann auf **Einstellungen**.
2. Um die aktuelle Version zu überprüfen, klicken Sie oben rechts auf der Seite auf **Hilfe**, und klicken Sie anschließend im angezeigten Hilfefeld unten auf die umkreiste Schaltfläche **i**.

Sicherheitseinstellungen überprüfen

Zur Erhöhung der Sicherheit wird während der Aktualisierung der Datenbankzugriff per HTTP und FTP deaktiviert. Wenn Sie mithilfe dieser Methoden auf Datenbankdateien zugreifen, ändern Sie die Sicherheitseinstellungen nach der Aktualisierung entsprechend.

1. Navigieren Sie zur *Systemsteuerung* der Appliance:
   - Wenn die Organisationskomponente auf der Appliance nicht aktiviert ist, klicken Sie auf **Einstellungen**.
   - Wenn die Organisationskomponente auf der Appliance aktiviert ist: Melden Sie sich an der Systemverwaltungskonsole der Appliance an: `http://`KACE_SMA_hostname`/system`. Oder wählen Sie rechts oben auf der Seite aus der Dropdown-Liste die Option **System** aus und klicken Sie dann auf **Einstellungen**.
2. Klicken Sie auf der linken Navigationsleiste auf **Sicherheitseinstellungen**, um die Seite *Sicherheitseinstellungen* anzuzeigen.
3. Ändern Sie im oberen Bereich der Seite die folgenden Einstellungen:
   - **Aktivieren von "Sicherungsdateien sichern"**: Deaktivieren Sie dieses Kontrollkästchen, damit Benutzer per HTTP ohne Authentifizierung auf Datenbanksicherungsdateien zugreifen können.
   - **Datenbankzugriff aktivieren**: Aktivieren Sie dieses Kontrollkästchen, damit Benutzer über Port 3306 auf die Datenbank zugreifen können.
   - **Sicherung über FTP aktivieren**: Aktivieren Sie dieses Kontrollkästchen, damit Benutzer per FTP auf Datenbanksicherungsdateien zugreifen können.

   VORSICHT: Die Änderung dieser Einstellungen verringert die Sicherheit der Datenbank und wird aus diesem Grund nicht empfohlen.
4. Klicken Sie auf **Speichern**.
5. **Nur KBIN-Upgrades**. Erschweren Sie den Zugriff auf Root-Kennwort (2FA) für die Appliance.
   a. Klicken Sie in der Systemverwaltungskonsole auf **Einstellungen** > **Support**.
   b. Klicken Sie auf der Seite *Support* unter *Problembehebungstools* auf **Zweifaktor-Authentifizierung**.
   c. Klicken Sie auf der Seite *System unterstützt Zweifaktor-Authentifizierung* auf **Geheimen Schlüssel ersetzen**.
   d. Notieren Sie die Token und bewahren Sie diese Informationen an einem sicheren Ort auf.

Weitere Ressourcen

Zusätzliche Informationen erhalten Sie in den folgenden Ressourcen:

- Online-Produktdokumentation (https://support.quest.com/kace-systems-management-appliance/10.0/technical-documents)
  - **Technische Daten**: Informationen zu den Mindestanforderungen bei der Installation der bzw. Aktualisierung auf die aktuelle Version des Produkts.

    Virtuelle Appliances: Weitere Informationen finden Sie unter https://support.quest.com/technical-documents/kace-systems-management-appliance/10.0-common-documents/technical-specifications-for-virtual-appliances/.
    KACE als Dienst: Weitere Informationen finden Sie unter https://support.quest.com/technical-documents/kace-systems-management-appliance/10.0-common-documents/technical-specifications-for-kace-as-a-service/.
  - **Einrichtungshandbücher**: Anweisungen zum Einrichten virtueller Appliances. Die Dokumentation der neuesten Version finden Sie unter https://support.quest.com/kace-systems-management-appliance/10.0/technical-documents.
  - **Administratorhandbuch**: Anweisungen zur Verwendung der Appliance. Die Dokumentation der neuesten Version finden Sie unter https://support.quest.com/technical-documents/kace-systems-management-appliance/10.0-common-documents/administrator-guide/.

Globalisierung

Dieser Abschnitt enthält Informationen zum Installieren und Verwenden dieses Produkts in nicht englischsprachigen Konfigurationen (beispielsweise für Kunden außerhalb Nordamerikas). Dieser Abschnitt ersetzt nicht die anderen Angaben zu unterstützten Plattformen und Konfigurationen in der Produktdokumentation.

Diese Version ist für Unicode aktiviert und unterstützt alle Zeichensätze. In dieser Version sollten alle Produktkomponenten für die Verwendung derselben oder kompatibler Zeichenkodierungen konfiguriert und so installiert werden, dass sie dieselben Gebietsschema- und Regionsoptionen verwenden. Diese Version unterstützt die Verwendung in folgenden Regionen: Nordamerika, Westeuropa und Lateinamerika, Mittel- und Osteuropa, Fernost (Asien), Japan.

Diese Version wurde für die folgenden Sprachen lokalisiert: Französisch, Deutsch, Japanisch, Portugiesisch (Brasilien), Spanisch.

Über uns

Quest bietet Softwarelösungen für die sich schnell verändernde Welt der Unternehmens-IT. Wir unterstützen Sie dabei, die Herausforderungen zu vereinfachen, die durch Datenexplosion, Cloud-Erweiterung, hybride Rechenzentren, Sicherheitsbedrohungen und behördliche Auflagen entstehen. Wir sind ein globaler Anbieter für 130.000 Unternehmen in 100 Ländern, darunter 95 % der Fortune 500 und 90 % der Global 1000. Seit 1987 haben wir ein Lösungsportfolio aufgebaut, das nun Datenbankmanagement, Datenschutz, Identitäts- und Zugriffsmanagement, Microsoft-Plattformmanagement und einheitliches Endpoint-Management umfasst. Mit Quest verbringen Unternehmen weniger Zeit mit der IT-Administration und mehr Zeit mit geschäftlichen Innovationen. 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

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.

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 Systemverwaltungs-Appliance – Versionshinweise

Letzte Überarbeitung: August 2019

Software-Version: 10.0