KACE Systems Management Appliance 15.0
Administrator Guide

Administrator Guide

Table of Contents

About the KACE Systems Management Appliance....27
About the appliance components....27
About the Administrator Console....28
Components available in Admin mode without the Organization component....32
Components available in Admin mode with the Organization component enabled....36
Components available in System mode with the Organization component enabled....38
Using the Home component....40
About Dashboards....40
View the Dashboard in Admin mode....40
View the Dashboard in System mode....41
About Dashboard widgets....42
Customize Dashboard pages....51
Work with Dashboard Settings....51
Bookmark a page as Favorite....55
View task schedules....56
View the appliance version, model, and license information....56
View product licensing information....58
About appliance software updates....59
About labels....59
Searching for information and filtering lists....60
Search at the Admin level....60
Search at the page level....60
Searching at the page level with advanced options....61
Create Custom Views using Filter criteria....63
Access product documentation....64
Log in to the Administrator Console: First login following initial network configuration....67
Getting started....69
Configuring the appliance....69
Requirements and specifications....69
Power-on the appliance and log in to the Administrator Console....69
Access the Command Line Console....71
Tracking configuration changes....72
Configuring System-level and Admin-level General Settings....72
Configure appliance General Settings with the Organization component enabled....72
Configure Admin-level or organization-specific General Settings....78
Configure appliance General Settings without the Organization component....83

Configure appliance date and time settings....89
Managing user notifications....90
Review user notification alerts....90
Configure user notifications....91
Enable Two-Factor Authentication for all users....92
Verifying port settings, NTP service, and website access....93
Verify port settings....93
Verifying the status of the NTP service....94
Make necessary websites accessible to the appliance....95
Configuring network and security settings....95
Change appliance network settings....95
Configure local routing tables....98
Configure local web server settings and allow access to hosts....99
Configure security settings for the appliance....100
Configure Encrypted Remote Logging to an External Server....108
Configure Active Directory as the single sign on method....110
Generate an SSL certificate....113
Configuring session timeout settings....114
Set session timeout....114
Configuring locale settings....115
How locale settings are applied....115
Configure locale settings for the Administrator Console and the Command Line Console....115
Configure locale settings for the User Console....116
Configure locale settings for organizations....117
Configure locale settings for users....117
Configuring the default theme....118
Configure the default theme for the appliance....118
Configure the default theme for a user....118
Configure data sharing preferences....119
About DIACAP compliance requirements....120
Enable or disable the Acceptable Use Policy....120
Enable API Access for the appliance....121
Disable API Access for the appliance....121
Configuring Mobile Device Access....121
Enable Mobile Device Access for the appliance....122
Enable Mobile Device Access for users....122
Download and use KACE GO....123
Disable Mobile Device Access on the appliance....124

Disable Mobile Device Access for users..... 124
Enable fast switching for organizations and linked appliances..... 124
Linking Quest KACE appliances.....125
Enable appliance linking..... 126
Add Names and Keys to appliances.....126
Enable access to Federation API settings.....127
Disable appliance linking.....128
Configuring history settings.....128
About history settings.....128
Managing settings history..... 129
Managing asset history..... 130
Managing object history..... 131
Using change history information.....132
Configuring Content Security Policy..... 133
Enable Content Security Policy.....133
Setting up and using labels to manage groups of items.....134
About labels..... 135
About Smart Labels.....135
About LDAP Labels.....135
About label groups..... 136
About organization filters.....136
Tracking changes to label settings..... 136
Managing manual labels.....136
Add or edit manual labels..... 136
View manual label details..... 138
Delete manual labels.....138
Managing Smart Labels.....139
Add Smart Labels.....139
Example: Combine Smart Labels to identify devices.....140
Edit Smart Labels.....141
Setting up labels for user accounts..... 142
Using Smart Labels for patching.....143
Using Smart Labels with Discovery Results..... 145
Adding Smart Labels for devices.....146
Assign the Smart Label run order.....150
Delete Smart Labels.....150
Managing label groups..... 151
Add, view, or edit label groups..... 151

Assign labels to or remove labels from label groups....152
Delete label groups....152
Managing LDAP Labels....153
Add or edit LDAP Labels....153
Enable LDAP Labels....155
Delete LDAP Labels....155
Use the LDAP Browser....155
Configuring user accounts, LDAP authentication, and SSO....156
About user accounts and user authentication....157
About locale settings....157
Managing System-level user accounts....157
Add or edit System-level user accounts....157
Manage appliance administrator email notifications....159
Delete System-level user accounts....160
Managing organization user accounts....160
Add or edit User Roles....160
Delete User Roles....161
Add or edit organization user accounts....161
Customize user details....164
Archive user accounts....164
View or edit user profiles....165
Using an LDAP server for user authentication....167
About the login account on your LDAP server....167
Configure and test LDAP user authentication....167
Importing users from an LDAP server....170
Import user information manually....170
Import user information according to a schedule....172
About single sign on (SSO)....176
Using external LDAP or Active Directory servers for single sign on....176
Enabling and disabling single sign on....177
Enable single sign on....177
Disable single sign on....177
Using Active Directory for single sign on....177
Configure Active Directory as the single sign on method....178
Configuring browser settings for single sign on....179
Unjoin the domain and disable Active Directory single sign on....180
Configure SAML for single sign on....181
Example: Using Microsoft Active Directory in Azure as a SAML Identity Provider....182

Reviewing user sessions..... 184
Install and configure the location database..... 184
View a list of user sessions..... 185
Deploying the KACE Agent to managed devices.....186
Using Replication Shares..... 186
Create Replication Shares.....187
View Replication Share details..... 190
Managing credentials.....190
Tracking changes to Credentials Management settings.....191
Add and edit Secret Key credentials..... 191
Add and edit User/Password credentials.....192
Add and edit LDAP User/Password credentials..... 193
Add and edit Google Workspace credentials..... 194
Add and edit SNMP credentials..... 197
Add and edit Microsoft Office 365 OAuth credentials.....199
View credential usage.....200
Create reports from the Credentials Management list.....201
Export credentials information..... 201
Delete credentials..... 202
Configuring assets..... 202
About the Asset Management component..... 202
Using the Asset Management Dashboard.....203
About the Asset Management Dashboard widgets.....203
Customize the Asset Management Dashboard..... 205
Work with Asset Management Dashboard.....205
About managing assets..... 207
How asset information differs from inventory information.....207
Identifying the assets to track..... 208
View assets and search for asset information..... 208
Add barcodes to assets..... 209
Change device owners.....210
View and configure asset lifecycle settings..... 211
Adding and customizing Asset Types and maintaining asset information..... 212
About Asset Types..... 212
Customizing Asset Types.....212
About Asset Subtypes, custom fields, and device detail preferences.....218
Managing Software assets.....225
Customize the Software Asset Type.....225

Adding Software assets.... 226
Managing physical and logical assets.... 228
Add physical Asset Types.... 228
Archive device Assets.... 230
Maintaining and using manual asset information.... 231
Managing locations.... 231
Manage locations.... 231
Add or edit locations.... 232
Customize location fields.... 233
Managing contracts.... 235
Manage contracts.... 235
Add or edit contracts.... 236
Managing licenses.... 238
Manage licenses.... 238
Add or edit licenses.... 239
Managing purchase records.... 242
Manage purchase records.... 242
Add or edit purchase records.... 243
Setting up License Compliance.... 245
About License Compliance for Software Catalog applications.... 246
About license upgrades.... 246
About license downgrades.... 246
Customize the License Asset Type.... 247
Add License assets for Software Catalog inventory.... 248
Add License assets for Software page inventory.... 252
Importing license data in CSV files.... 256
How asset information is handled during import.... 256
Importing asset data using CSV files.... 257
Managing License Compliance.... 261
View License Compliance information for Software Catalog applications.... 261
Reclaim unused software licenses.... 263
Update software License Compliance information manually.... 264
Customize license usage warning thresholds.... 264
View License Compliance and Configuration information.... 265
Setting up Service Desk.... 266
Setting up roles for user accounts.... 266
About default roles.... 266
Create a Service Desk staff role.... 267

Assign user roles....269
Apply labels and roles to Service Desk staff....270
Create the DefaultTicketOwners account....270
Configuring email settings....271
About email notifications....271
About Ticket Rules....272
About POP3 email accounts....272
Create and configure POP3 email accounts....272
Configure email preferences....273
Configuring email triggers and email templates....274
Configure CC lists for ticket categories....283
Automatically add email addresses to ticket CC List fields....283
Exclude addresses from ticket CC List fields....284
Prevent email loops....284
Configure the Cache Lifetime for Service Desk widgets....285
Creating and managing organizations....286
About organizations....286
About the Default organization....286
Tracking changes to organization settings....286
Managing Organization Roles and User Roles....286
Available default roles....287
Add or edit Organization Roles....287
Duplicate Organization Roles....288
Delete roles....289
Adding, editing, and deleting organizations....289
Add or edit organizations....289
Configure Two-Factor Authentication for organizations....295
Delete organizations....296
Customizing the logos used for the User Console and organization reports....296
Managing user accounts for organizations....296
Managing organization filters....296
How organization filters work....297
Add or edit organization Data Filters....297
Add or edit organization LDAP Filters....298
Test organization filters....299
Delete organization filters....300
Managing devices within organizations....300
Using Filter for Advanced Search....300

Filter devices..... 300
Redirect devices.....301
Understanding device details.....301
Running single organization and consolidated reports.....301
Importing and exporting appliance resources..... 301
About importing and exporting resources.....302
Transferring resources among appliances using Samba share directories..... 302
Export resources from an appliance..... 302
Import resources to an appliance..... 303
Transferring resources among organizations..... 304
Export resources from organizations..... 304
Import resources to organizations.....304
Managing exported resources at the System level..... 305
View or delete shared resources..... 305
Move shared resources from the local appliance to network locations.....305
View or delete the status of resource exports..... 305
Managing inventory.....306
Using the Inventory Dashboard.....306
About the Inventory Dashboard widgets.....306
Customize the Inventory Dashboard..... 308
Work with Inventory Dashboard..... 308
Setting an Inventory Dashboard..... 309
Adding a Widget to Inventory Dashboard.....309
Emailing Inventory Dashboard.....310
Refreshing Inventory Dashboard Data Manually.....310
Using Device Discovery.....310
About Device Discovery and device management.....311
Tracking changes to Discovery settings..... 311
Discovering devices on your network.....311
Add a Discovery Schedule to perform a quick "what and where" scan of your network.....312
Add a Discovery Schedule for a thorough scan of managed Windows, Mac, Linux, and UNIX computers..... 320
Obtain a Client ID and Client Secret for use in discovering Chrome devices..... 324
Add a Discovery Schedule for a KACE Cloud Mobile Device Manager device..... 325
Add a Discovery Schedule for a Google Workspace device..... 327
Add a Discovery Schedule for an Workspace ONE device..... 330
Add a Discovery Schedule for a VMware ESXi host or a vCenter Server..... 332

Add a Discovery Schedule for a Microsoft Hyper-V or System Center Virtual Machine Manager....334
System Center Virtual Machine Manager Credential Requirements....336
Add a Discovery Schedule for SNMP-enabled non-computer devices....336
About Discovery Results....340
View and search Discovery Results....340
Provision the Agent using the discovered IP address or hostname....340
Stop a running discovery scan....341
Delete Discovery Schedules....342
Managing device inventory....342
About managing devices....342
Features available for each device management method....342
About inventory information....348
Tracking changes to inventory settings....349
Managing inventory information....349
Add custom data fields....349
Schedule inventory data collection for managed devices....350
View device inventory and details....352
Viewing information about devices enrolled in KACE Cloud MDM....353
Groups and sections of items in device details....353
About Dell Data Protection | Encryption (DDP|E) and encryption information in device details....382
Add a Dump Inventory registry key to permit inventory collection on Windows DDP|E client devices....388
About Intel AMT information in device details....391
Finding and managing devices....392
Finding devices in inventory....392
Labeling devices to group them....393
Run actions on devices....394
View devices that have been added manually....395
Delete devices from inventory....395
Registering KACE Agent with the appliance....395
Manage KACE Agent tokens....396
Review quarantined KACE Agents....397
Provisioning the KACE Agent....398
Enabling file sharing....399
Provisioning the KACE Agent using the GPO Provisioning Tool for Windows devices....401
Provisioning the KACE Agent using onboard provisioning....402
Managing provisioning schedules....407

Managing Agent communications....410
Updating the KACE Agent on managed devices....416
Manually deploying the KACE Agent....418
Obtaining Agent installation files....419
Manually deploying the KACE Agent on Windows devices....419
Manually deploying and upgrading the KACE Agent on Linux devices....422
Performing Agent operations on Linux devices....424
Manually deploying and upgrading the KACE Agent on Mac devices....425
Performing other Agent operations on Mac devices....427
Viewing information collected by the Agent....429
Using Agentless management....429
About Agentless device management....429
Managing Agentless devices....430
Using SNMP Inventory Configurations to identify specific SNMP objects and non-computer devices to add to inventory....437
Adding devices manually in the Administrator Console or by using the API....439
About managing devices....440
Tracking changes to inventory settings....440
Add devices manually with the Administrator Console....440
Adding devices manually using the API....444
Forcing inventory updates....452
Force inventory updates from the appliance....453
Force inventory updates from Windows devices....453
Force inventory updates from Mac OS X devices....453
Force inventory updates from Linux devices....454
About Remote Control....454
Privacy and Data Safety in Remote Connections....454
Install Remote Control Applications....454
Configure Remote Control Settings....457
Start a Remote Control Session....459
Statuses of Remote Control Session....460
End a Remote Control Session....460
Track Remote Session History....460
Upload and View Streamer Logs....461
Customize the Blank Screen Logo....461
Troubleshoot Remote Control....462
Managing MIA devices....463
Configure MIA settings....463
Apply labels to MIA devices....464

Delete MIA devices manually....464
Troubleshoot devices that fail to appear in inventory....464
Obtaining Dell warranty information....466
Obtain Dell warranty information on a single Dell device instantly....466
Renew a Dell warranty....467
Run Dell warranty reports....467
Managing applications on the Software page....467
About the Software page....467
View items in Software page inventory....468
Tracking changes to inventory settings....468
Adding and deleting applications in Software page inventory....468
Add applications to Software page inventory manually....468
Delete applications....470
Creating Software assets....470
Add Software assets in the Inventory section....470
Add Software assets in the Assets section....470
Attach digital assets to applications and select supported operating systems....471
Copy files to the appliance Client Drop location....472
Using software threat levels and categories....473
Assign threat levels to applications....473
Assign categories to applications....473
Finding and labeling applications....473
About finding applications using Filter....474
Add manual software labels....474
Apply manual labels to or remove labels from software....474
Add software Smart Labels....474
Managing Software Catalog inventory....475
About the Software Catalog....475
Application classifications....476
About cataloged applications....476
About Locally Cataloged applications....477
About Not Allowed applications....477
Application categories....477
How Software Catalog information is collected....477
How the Software Catalog is used with the Organization component....477
How Software Catalog information is localized....477
How you can help improve the Software Catalog....478
Differences between the Software page and the Software Catalog page....478

Viewing Software Catalog information....479
View lists of Discovered and Not Discovered applications....480
View the list of Uncataloged applications....481
View the list of Locally Cataloged applications....482
View details of Software Catalog applications....483
Adding applications to the Software Catalog....486
Submitting cataloging requests automatically adds applications to the local Software Catalog....486
How Locally Cataloged applications change to Cataloged applications....486
How custom names are resolved when Locally Cataloged applications are added to the Software Catalog....487
Submit cataloging requests....487
Cancel cataloging requests and remove local cataloging....488
Managing License assets for Software Catalog applications....489
Add License assets for Software Catalog inventory....489
Migrate License assets to applications in the Software Catalog....493
Associate Managed Installations with Cataloged Software....494
Using software metering....494
About software metering....494
About metering information....494
Enabling and configuring metering for devices and applications....495
Viewing Software Catalog metering information....500
Disabling metering for Software Catalog applications and managed devices....502
Managing metering and scheduling inventory collection....503
Using Application Control....504
Requirements for blocking applications....504
How applications are blocked....505
About denying access to application editions that share executable files....505
Applications that cannot be blocked....505
Apply the Application Control label to devices....505
Mark applications and suites as Not Allowed....505
View applications and suites that are marked as Not Allowed....506
Create reports showing applications marked as Not Allowed....506
Remove the Not Allowed designation from applications....507
Update or reinstall the Software Catalog....508
Managing process, startup program, and service inventory....508
Managing process inventory....509
View and edit process details....509
Add labels for processes....509

Apply labels to or remove labels from processes....510
Categorize processes....510
Assign threat levels to processes....510
Delete processes....511
Managing startup program inventory....511
View and edit startup program details....511
Add labels for startup programs....512
Apply labels to or remove labels from startup programs....512
Categorize startup programs....512
Assign threat levels to startup programs....513
Delete startup programs....513
Managing service inventory....513
View and edit service details....513
Add labels for services....514
Apply labels to and remove labels from services....514
Categorize services....515
Assign threat levels to services....515
Delete services....515
Writing custom inventory rules....515
About Custom Inventory rules....516
Types of Custom Inventory rules....516
Create Custom Inventory rules....516
How Custom Inventory rules are implemented....517
Syntax for Custom Inventory rules....518
Checking for conditions (conditional rules)....519
Getting values from a device (Custom Inventory Field)....525
Matching filenames to regular expressions....528
Understanding regular expressions....528
Regular Expression Rule Reference....530
Defining rule arguments....530
Test Custom Inventory rules....534
Deploying packages to managed devices....535
Distributing software and using Wake-on-LAN....535
About software distribution....535
About testing software distribution....536
Tracking changes to distribution settings....536
Types of distribution packages....537
Attaching digital assets to applications and selecting supported operating systems...537

Distributing packages from the appliance....537
Distributing packages from alternate download locations and Replication Shares....538
About alternate download locations....538
About Replication Shares....538
Distributing applications to Mac OS X devices....538
Using Managed Installations....539
Adding applications to inventory....539
About creating Managed Installations....539
About installation parameters....540
Identify parameters that are supported by installer files....540
Create Managed Installations for Windows devices....540
Examples of common deployments on Windows....544
Create Managed Installations for ZIP files....545
Create Managed Installations for RPM files....545
Create Managed Installations for TAR.GZ files....550
Create Managed Installations for macOS X devices....551
Create and use File Synchronization....554
Using Wake-on-LAN....557
Issue Wake-on-LAN requests....557
Schedule Wake-on-LAN requests....558
Troubleshooting Wake-on-LAN....559
Exporting Managed Installations....560
Broadcasting alerts to managed devices....560
Create alerts to be broadcast....560
Running scripts on managed devices....562
About scripts....562
Obtaining script dependencies....563
Tracking changes to scripting settings....563
About default scripts....564
Adding and editing scripts....565
Token replacement variables....566
Add offline KScripts, online KScripts, or online shell scripts....567
Edit scripts....574
Delete scripts from the Scripts page....574
Delete scripts from the Script Detail page....575
Structure of importable scripts....575
Import scripts....576
Duplicate scripts....576

Using the Run and Run Now commands....576
Run scripts from the Run Now page....577
Run scripts from the Script Detail page....577
Run scripts from the Scripts page....577
Monitor Run Now status and view script details....578
Edit policies and scripts....579
Search the scripting logs....579
Exporting scripts....580
Using Task Chains....580
Add and edit Task Chains....581
Patching devices and maintaining security....584
Using the Security Dashboard....584
About the Security Dashboard widgets....584
Customize the Security Dashboard....586
Work with the Security Dashboard Settings....587
Setting a Security Dashboard....587
Adding Widget to Security Dashboard....588
Emailing a Security Dashboard....588
Refreshing Security Dashboard Data Manually....589
About patch management....589
Patching workflow....589
About patch signature files....591
About patch packages....591
About patch testing and security....591
About the patch testing environment....591
About the patch quality assurance process....592
Best practices for patching....593
Subscribing to and downloading patches....595
About patch subscription and downloads....595
Websites that must be accessible to the appliance....596
Overview of first-time patch-subscription workflow....596
View details about operating systems and applications....596
Subscribing to patches and configuring download settings....597
Subscribe to patches....597
Select patch and feature update download settings....599
Viewing available patches and download status....601
View available patches....602
View patch download status....602

Best practices for resolving patch subscription issues....602
Creating and managing patch schedules....604
About scheduling critical OS patches for desktops and servers....604
Workflow for critical OS patches for desktops and servers....605
About scheduling critical patches for laptops....605
Workflow for critical patches for laptops....605
About scheduling non-critical patches....605
Configuring patch schedules....606
Fields in the Patch Schedule Detail pages....606
Configure patch schedules....614
Error codes caused by patching and scripting....615
Viewing patch schedules, status, and reports....616
View a list of patch schedules....616
Review patch schedule details....619
Patching status definitions....622
View patch status....624
View patch status by device....624
View files within patches....624
View patch reports....624
Managing patch rollbacks....625
Determine whether a patch can be rolled back....625
Undo the last patching job....625
Managing patch inventory....626
Prerequisites for managing patch inventory....626
Viewing patch information....626
View downloaded patches....626
View patch details....628
Resetting the number of patch deploy attempts....628
View patch information for devices in inventory....629
View devices missing patches....630
Leveraging CVSS and EPSS for effective Patching....630
Viewing patch statistics and logs....631
View patch statistics....631
View the patch log....631
Mark patches as inactive....631
Patch Mac OS X devices....632
Managing Windows Feature Updates....632
Subscribe to Windows Feature Updates....632

Configure Windows Feature Update schedules.....633
View Windows Feature Update schedules.....637
Review Windows Feature Update schedule details.....637
View available Windows Feature Updates.....640
View Windows Feature Update status.....641
Managing Dell devices and updates.....641
Differences between patching and Dell Updates.....641
Select Dell Update download settings.....642
Configure Dell Update schedules.....644
View Dell Update schedules.....648
Review Dell Update schedule details.....649
View available Dell Updates.....651
View Dell Update status.....652
Managing Linux package upgrades.....652
View Linux package upgrade schedules.....652
Configure Linux package upgrade schedules.....653
Review Linux package upgrade schedule details.....656
Review Linux package upgrades.....658
Manage quarantined file attachments.....659
Using reports and scheduling notifications.....660
About reports and notifications.....660
About reports.....660
About notifications.....660
Tracking changes to report settings.....660
Creating and modifying reports.....661
Creating reports.....661
Create reports using the report wizard.....661
Create dashboard report using report wizard.....663
Create reports using SQL queries.....665
Create dashboard report using SQL queries.....667
Create reports from list pages.....668
Configuring Chart Types for a Report.....669
Duplicate reports.....711
Edit SQL statements on reports created with the report wizard.....712
Modifying reports.....712
Edit reports.....712
Delete reports.....713
Customizing logos used for reports.....713

Scheduling reports and notifications ... 713
Running single-organization and consolidated reports ... 713
Run single-organization reports ... 714
Run consolidated organization reports ... 714
Scheduling reports ... 714
Add report schedules ... 715
Delete report schedules ... 717
Scheduling notifications ... 717
Add notification schedules from the Reporting section ... 717
Add notification schedules from list pages ... 719
Edit notification schedules ... 719
Delete notification schedules ... 720
Monitoring devices ... 721
Getting started with monitoring ... 722
Enable monitoring for a device ... 723
Enable monitoring for one or more devices from the Devices inventory list ... 723
Enable monitoring for a server from its Device Detail page ... 724
Obtaining a new license key to increase server monitoring capacity ... 724
Apply a new license key to increase server monitoring capacity ... 725
Working with monitoring profiles ... 725
Edit a profile ... 726
Configure SNMP trap messages and alerting criteria ... 728
Create a new profile using a default profile as a template ... 730
Profile log paths for MySQL and Apache ... 732
Upload a profile that was created by another user ... 732
Download a profile so that it can be used by others ... 732
Bind an additional profile to a device ... 733
Define nonstandard log date format ... 733
Configuring application and threshold monitoring with Log Enablement Packages ... 733
Install one or more LEPs on monitored devices ... 734
Edit the monitoring Log Enablement Package (LEP) for a Windows Server 2008 or higher device ... 734
Managing monitoring for devices ... 736
Pause monitoring for a device ... 736
Pause or resume monitoring for multiple devices ... 736
Set the polling interval and any automatic dismissal or deletion of alerts ... 737
Disable ping probe ... 737
Receive alerts when device configurations change ... 738

Schedule a Maintenance Window during which time alerts are not collected from a device....738
Create and assign monitoring-specific roles....739
Disable monitoring for one or more devices....742
Enable monitoring for one or more devices....742
Working with alerts....743
Add notification schedules from the Monitoring Alerts list page....743
Create a Service Desk ticket from an alert....744
Search for alerts using Filter criteria....748
Filtering alerts using the Include Text and Exclude Text capability....748
Filter alerts using the Include Text and Exclude Text capability from the Profile Details page....748
Filter alerts using the Exclude Text capability from the Monitoring Alerts list page....749
Examples of Include Text and Exclude Text for monitoring profiles....750
Dismiss an alert....752
Retrieve and review alerts that have been dismissed from the alerts list....753
Delete alerts....753
Using the Service Desk....754
Configuring Service Desk....754
System requirements....754
About Service Desk....754
Overview of setup tasks....755
Import tickets from another system....755
Configuring Service Desk business hours and holidays....758
Configure Service Desk business hours....758
Configure Service Desk holidays....759
Configuring Service Level Agreements....759
Enable Service Level Agreements....759
Configuring Service Desk ticket queues....761
Configure ticket queues....761
Configure queue-specific email settings....765
Rename Service Desk titles and labels....769
Enable or disable the conflict warning....770
View and edit response templates....771
Configuring ticket settings....772
Customize the Ticket Detail page....772
Customizing the User Console home page....775
Change the User Console logo and text at the System level....775
Change the User Console logo and login text at the Admin-level....777

Show or hide action buttons and widgets on the User Console home page....779
Show or hide links to Knowledge Base articles on the User Console home page....780
Add, edit, hide, or delete User Console announcements....781
Prioritize User Console announcements or mark an announcement as urgent....782
Add, edit, or delete custom links on the User Console home page....783
Add ticket links to the User Console home page....784
Add a quick-action link for reporting problems on the User Console home page....785
About the session timeout period....785
Using the Satisfaction Survey....785
Changing the Satisfaction Survey default behavior....786
Enable or disable security for Service Desk attachments....787
Using the Service Desk Dashboard....787
About the Service Desk Dashboard widgets....787
Customize the Service Desk Dashboard....789
Work with Service Desk Dashboard....790
Setting a Service Desk Dashboard....790
Adding Widget to Service Desk Dashboard....790
Emailing a Service Desk Dashboard....791
Refreshing Service Desk Dashboard Data Manually....792
Managing Service Desk tickets, processes, and reports....792
Overview of Service Desk ticket lifecycle....792
Creating tickets from the Administrator Console and User Console....792
Create tickets from the User Console....793
Create tickets from the Administrator Console Ticket page....794
Create tickets from the Device Detail page....800
Create tickets from the Asset Detail page....801
Create a Service Desk ticket from an alert....802
Creating and managing tickets by email....805
About attachments to tickets created through email....805
Enable email ticket creation....806
Create a ticket by email....806
Modifying ticket attributes using email....807
Clearing a ticket field using email....807
Changing ticket fields using email....807
Changing ticket approval fields using email....808
Viewing tickets and managing comments, work, and attachments....809
Navigate among tickets, related devices, and assets....809
Add work information for tickets....809

Use default views for tickets....810
Create Filter views for tickets....812
Set a view as the default view for tickets....813
Add comments to tickets....813
Add owner-only comments to tickets....814
View ticket comments....815
Add or delete screen shots and attachments from Service Desk tickets....815
View ticket activity history....817
Send ticket information through email....817
Run Device Actions from tickets....817
Start a Remote Control Session from Ticket Details page....818
Merging tickets....818
Enable ticket merge....818
Merge tickets from the Tickets list page....819
Merge tickets from the Ticket Detail page....819
Using the ticket escalation process....819
Understanding ticket states....820
Understanding the escalation time limit....820
Understanding escalation....820
Changing ticket escalation settings....821
Change the list of escalation email recipients....821
Change the Response and Resolution time limits....821
Change the default escalation email message....821
Using Service Desk processes....822
Add, edit, and enable process templates....822
Define process types....828
Create process tickets to manage related tasks....829
Create process tickets by email....829
View process information....830
Cancel or complete process tickets....830
Delete process templates....831
Convert process tickets to regular tickets....831
Convert regular tickets to process tickets....832
Using Ticket Rules....832
Using and configuring system Ticket Rules....833
Understanding and customizing system Ticket Rules....833
Create custom Ticket Rules....833
Duplicate a custom Ticket Rule....835

Delete a custom Ticket Rule....836
Move a Ticket Rule from one queue to another....836
Run Service Desk reports....837
Archiving, restoring, and deleting tickets....837
Enable ticket archival....837
Configure queue archive settings....839
Archive selected tickets....840
Restore archived tickets....840
Delete archived tickets....840
Managing ticket deletion....840
Configure ticket deletion settings....841
Delete tickets....841
Managing Service Desk ticket queues....841
About Service Desk ticket queues....841
Adding and deleting queues....842
Add a queue....842
Add a queue by duplicating an existing queue....843
Delete a queue or queues....843
Viewing tickets in queues....843
View tickets across all queues....844
Setting the default queue....844
Set the default queue at the system level....844
Set the default queue at the user level....845
Set the default fields for the All Queues ticket list....845
Move tickets between queues....847
Bulk edit tickets in a queue....847
About User Downloads and Knowledge Base articles....848
Managing User Downloads....848
Add User Downloads....848
Apply labels to User Downloads....851
Remove labels from User Downloads....851
Delete User Downloads....851
Managing Knowledge Base articles....851
Add, edit, or duplicate Knowledge Base articles....852
Delete Knowledge Base articles....853
View user ratings and the number of views for Knowledge Base articles....854
Customizing Service Desk ticket settings....854
About customizing Service Desk ticket settings....854

Create ticket categories and subcategories 855
Customizing ticket values 857
Customize ticket status values 857
Customize ticket priority values 858
Customize ticket impact values 859
Customizing ticket layout 859
Customize Layout and Related Ticket Fields 860
Configure Comment Field Options 862
Define custom ticket fields 862
Customize the ticket list layout 864
Manage ticket templates 865
Configure a ticket template 866
Preview ticket layout 869
Using parent-child ticket relationships 870
Enable parent-child ticket relationships for a queue 870
Enable parent tickets to close child tickets 871
Create child tickets for any ticket 871
Designate tickets as parents and add existing tickets as their children 872
Use a parent ticket as a to-do list 872
Use parent tickets to organize duplicate tickets 873
Using ticket approvers 873
Configure ticket approvers 874
Approving tickets by email 874
Configuring SMTP email servers 874
Connect your email server to the appliance 874
Using internal and external SMTP servers 875
Use the internal SMTP server 876
Use an external SMTP server or Secure SMTP server 876
Maintenance and troubleshooting 878
Maintaining the appliance 878
Tracking changes to settings 878
About appliance backups 878
Set the daily backup schedule and the number of backups to retain 879
Back up the appliance manually 880
Download backup files from the Administrator Console 880
Access backup files through FTP 881
About deleting appliance backup data 881
Configure offboard backup transfer 882

Restoring the appliance....883
Restore the appliance using the most recent backup....883
Upload backup files to the appliance....884
Restore the appliance from backups....885
Restore the appliance to factory settings....886
Updating appliance software....886
Check for and apply advertised appliance updates....886
Upload an update file to the appliance manually....887
Verify updates....888
Update the appliance license key....888
Reboot or shut down the appliance....888
Understanding the daily run output....889
Disk status....889
Appliance network interface status....890
Appliance up-time and load averages....890
Email system health....890
Appliance backup status....891
Status of RAID drives....891
Troubleshooting the appliance....891
Using Troubleshooting Tools....891
Verify the status of devices on the network....892
Identify device issues....892
Enable a tether to Quest KACE Support....892
Troubleshooting appliance issues....893
View appliance logs....893
Download appliance activity logs....896
Viewing the daily run output....897
Troubleshooting and debugging the KACE Agent....897
Resolve Windows security issues that prevent Agent provisioning....897
Testing and troubleshooting email communication....897
Test outgoing email....898
Test incoming email....898
Use Telnet to test incoming email....898
Access appliance logs to view Microsoft Exchange Server errors....899
Troubleshooting email errors....900
About Diagnostic Console Two-Factor Authentication....900
Appendixes....901
Database table names....901

Adding steps to task sections of scripts....917
LDAP variables....926
List of Countries....928
Glossary....934
A....934
B....936
C....937
D....938
E....939
F....940
I....941
K....942
L....943
M....944
N....945
O....946
P....947
R....948
S....949
T....951
U....952
V....953
W....954
About us....955
Technical support resources....955
Legal notices....956
Index....957

About the KACE Systems Management Appliance

Quest® KACE® **Systems Management Appliance** is a virtual appliance designed to automate device management, application deployment, patching, asset management, reporting, and Service Desk ticket management.

For more information about **KACE** series appliances, go to the Quest website, https://www.quest.com/products/kace-systems-management-appliance/.

About the appliance components

Appliance components include software, hardware, web-based interfaces, and a mobile app interface.

Table 1. Appliance components

Component	Description
Virtual appliance	The appliance runs in a virtual environment that uses a VMware® or Microsoft® Hyper-V® infrastructure. For the latest information about requirements for managed devices, and browser requirements for accessing the **Administrator Console**, see the *Technical Specifications* available on the product documentation page: https://support.quest.com/kace-systems-management-appliance/technical-documents.
Command Line Console	The **Command Line Console** is a terminal window interface to the appliance. The interface is designed primarily to configure the appliance and enforce policies. See Power-on the appliance and log in to the Administrator Console.
Administrator Console	The **Administrator Console** is the web-based interface used to control the appliance. To access the **Administrator Console**, go to `http://`**appliance_hostname**`/admin` where **appliance_hostname** is the hostname of your appliance. If the Organization component is enabled, you can access the System-level settings of the **Administrator Console** at `http://`**appliance_hostname**`/system`. To view the full path of URLs in the **Administrator Console**, which can be useful when searching the database or sharing links, add `ui` to the URL you use to log in. For example: `http://`**appliance_hostname**`/admin`.
User Console	The **User Console** is the web-based interface that makes applications available to users on a self-service basis. It also enables users to file Service Desk support tickets to request help or report issues. To access the **User Console**, go to `http://`**appliance_hostname**`/user` where **appliance_hostname** is the hostname of your appliance.

Component	Description
	The **User Console** provides: • A repository of applications that users can download as needed. • A way for users to submit and track tickets requesting help. • Assistance for routine tasks, such as software installation, and access to the **Quest Support Knowledge Base**, https://support.quest.com/kace-systems-management-appliance/kb. To customize the **User Console**, see: • Configure appliance General Settings with the Organization component enabled. • Configure appliance General Settings without the Organization component.
KACE Agent	The KACE Agent is an application that can be installed on devices to enable device management through the appliance. Agents that are installed on managed devices communicate with the appliance through the agent messaging protocol. Agents perform scheduled tasks, such as collecting inventory information from, and distributing software to, managed devices. Agentless management is available for devices that cannot have Agent software installed, such as printers and devices with operating systems that are not supported by the Agent. See Provisioning the KACE Agent.
KACE GO	KACE GO is an app that enables administrators to access Service Desk tickets, inventory information, and application deployment features from their smart phones or tablets. The app also allows non-admin users to submit Service Desk tickets, view the status of submitted tickets, and read Knowledge Base articles from their mobile devices. You can download KACE GO from the Apple® App Store℠ for iOS devices, or from the Google Play™ store for Android™ devices. See Configuring Mobile Device Access.

About the Administrator Console

The components available in the **Administrator Console** might differ, depending on the license key, organization settings, appliance settings, and user role.

In addition, if the Organization component is enabled, the Administrator Console has two levels: The Admin level, which shows organization-related features, and the System level, which shows appliance-related features.

If the Organization component is not enabled, Admin- and System-level features are available at the Admin level.

NOTE: Your license key determines whether the Organization component is enabled or disabled. See View product licensing information and About organizations.

There are three login modes:

- **Admin mode without the Organization component enabled**: If the Organization component is not enabled on your appliance, go to `http://`**appliance_hostname**`/admin`, where **appliance_hostname** is the host name of

your appliance, to log in to this mode. For components available in this mode, see Components available in Admin mode without the Organization component.

- **Admin mode with the Organization component enabled**: If the Organization component is enabled on your appliance, go to `http://`**appliance_hostname**`/admin` to log in to the Default organization. **appliance_hostname** is the host name of your appliance. Admin mode enables you to manage the components available to the selected organization. For components available in this mode, see Components available in Admin mode with the Organization component enabled.

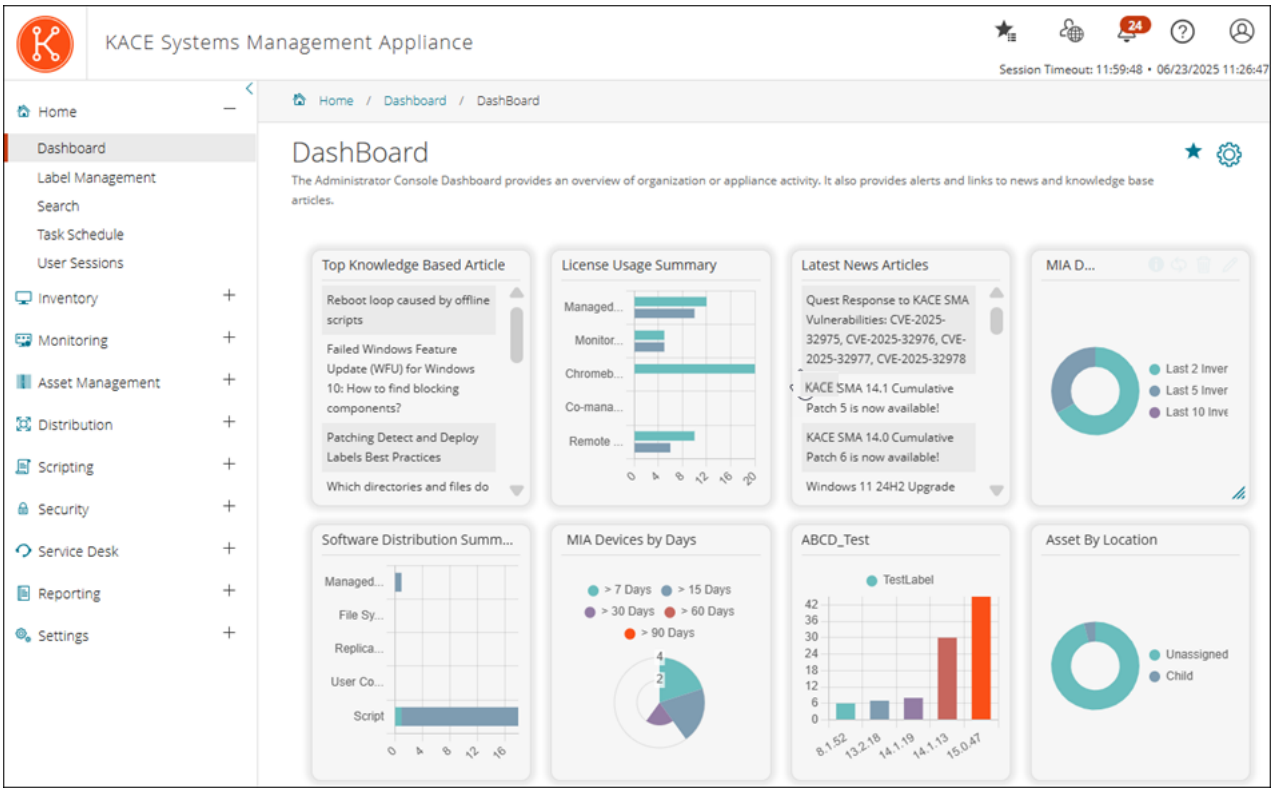
  If the *Login Organization* option is enabled in the appliance settings, the *Organization* box appears. You can type the name of an organization in the *Organization* box to log in to that organization directly.
  If you have multiple organizations and the *fast switching* option is enabled, you can switch between organizations and the System level using the drop-down list in the top-right corner of the page next to the login information. See Enable fast switching for organizations and linked appliances.

- **System mode with the Organization component enabled**: If the Organization component is enabled on your appliance, go to `http://`**appliance_hostname**`/system`, to log in to System mode. **appliance_hostname** is the hostname of your appliance. In this mode you can manage the components available at the System level. For components available in this mode, see Components available in System mode with the Organization component enabled.

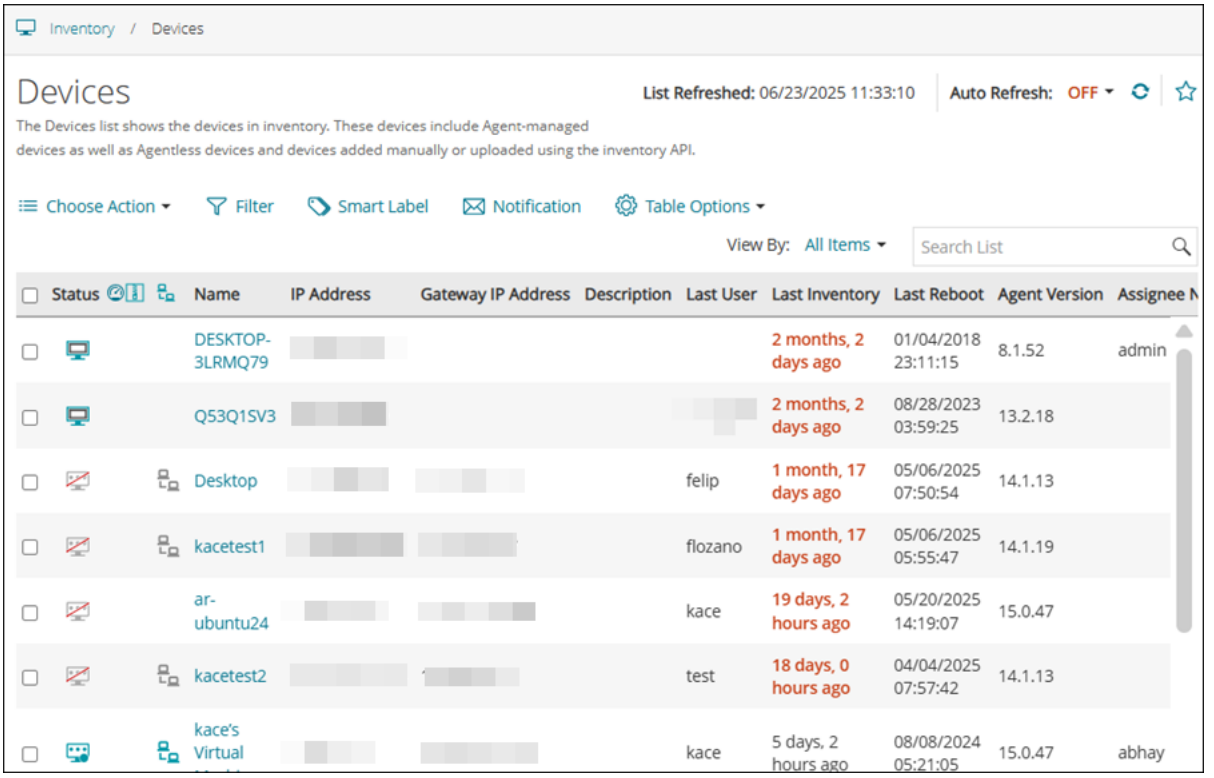
  In addition, if the *fast switching* option is enabled, and the passwords for the default admin accounts of the organizations are the same, you can switch between organizations using the drop-down list in the top-right corner of the page. See Enable fast switching for organizations and linked appliances.

Each mode has the following types of pages:

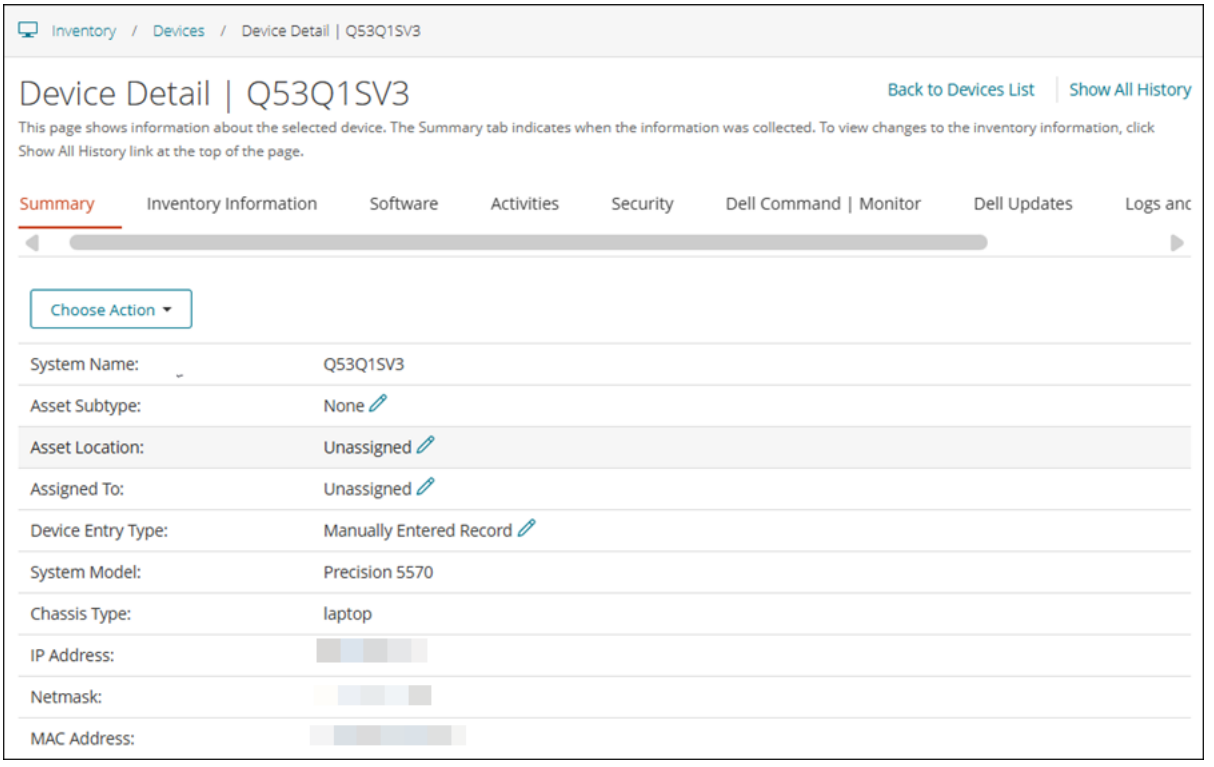
- **Dashboards**. These pages show status information for the appliance. If the Organization component is enabled, Dashboards are available at the organization and appliance level.



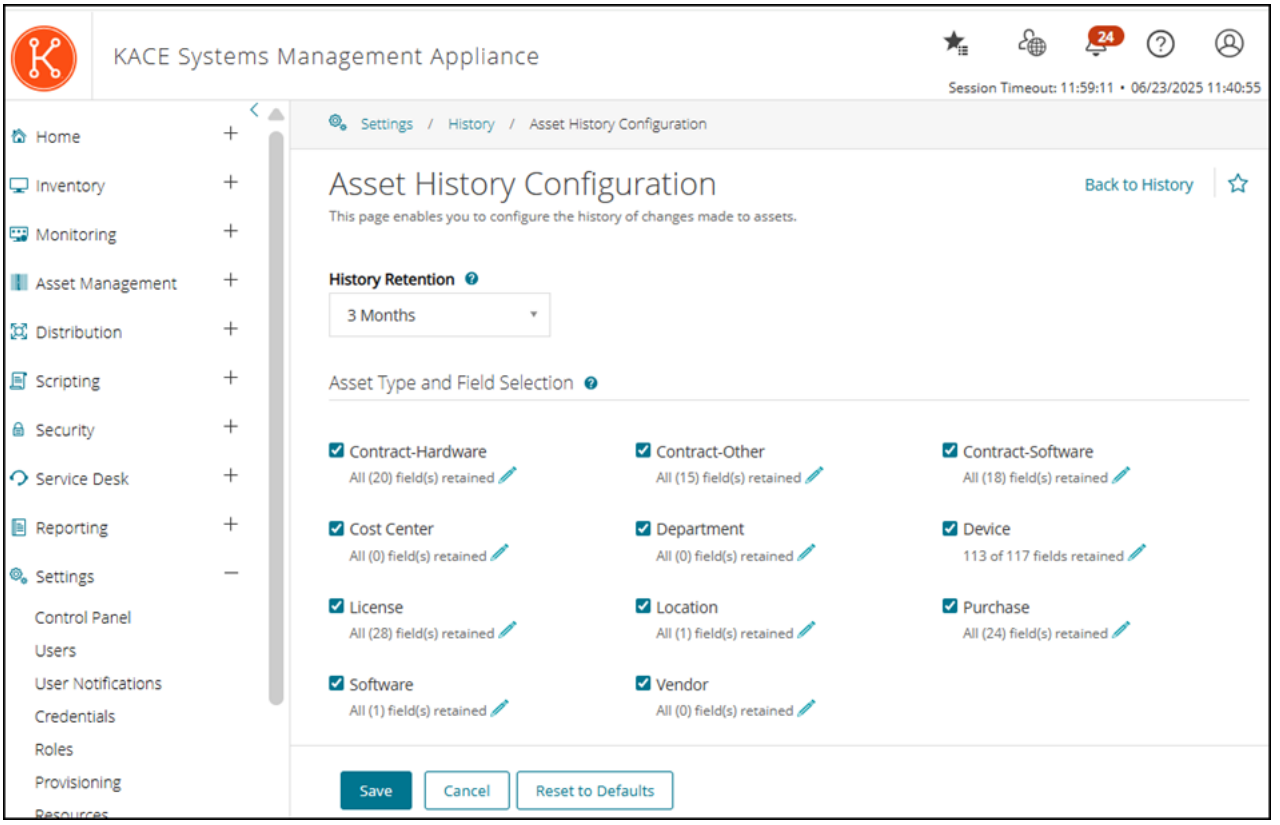
- **List pages**. These pages enable you to view items available on the appliance or, if the Organization component is enabled, in the selected organization.



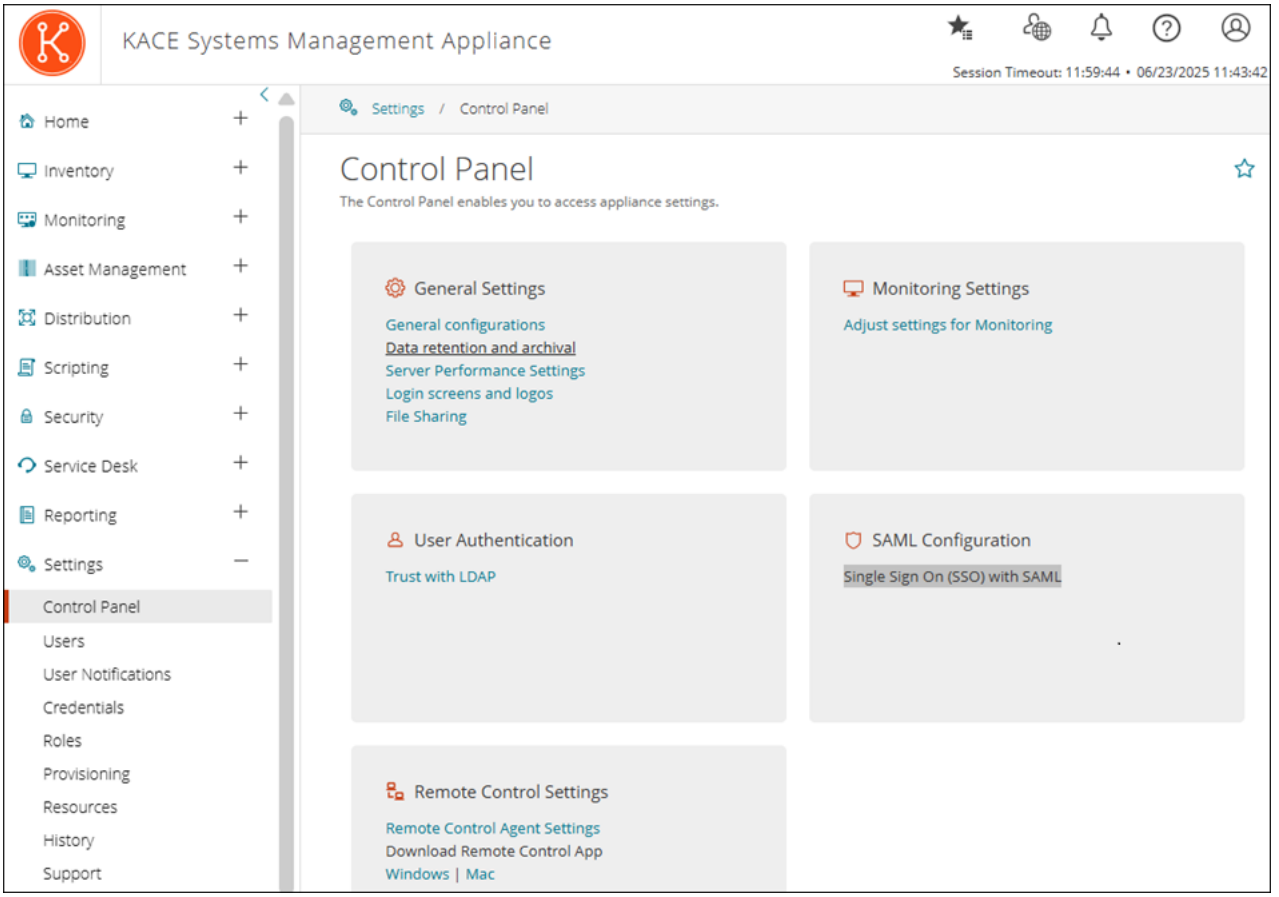
- **Detail pages**. These pages enable you to view and edit details of the selected item.



- **Configuration pages**. These pages enable you to configure settings.



- **Panels**. These pages provide access to related components and settings.



Components available in Admin mode without the Organization component

When the Organization component is not enabled, Admin mode shows all of the Admin-level components and the System-level (appliance-level) settings.

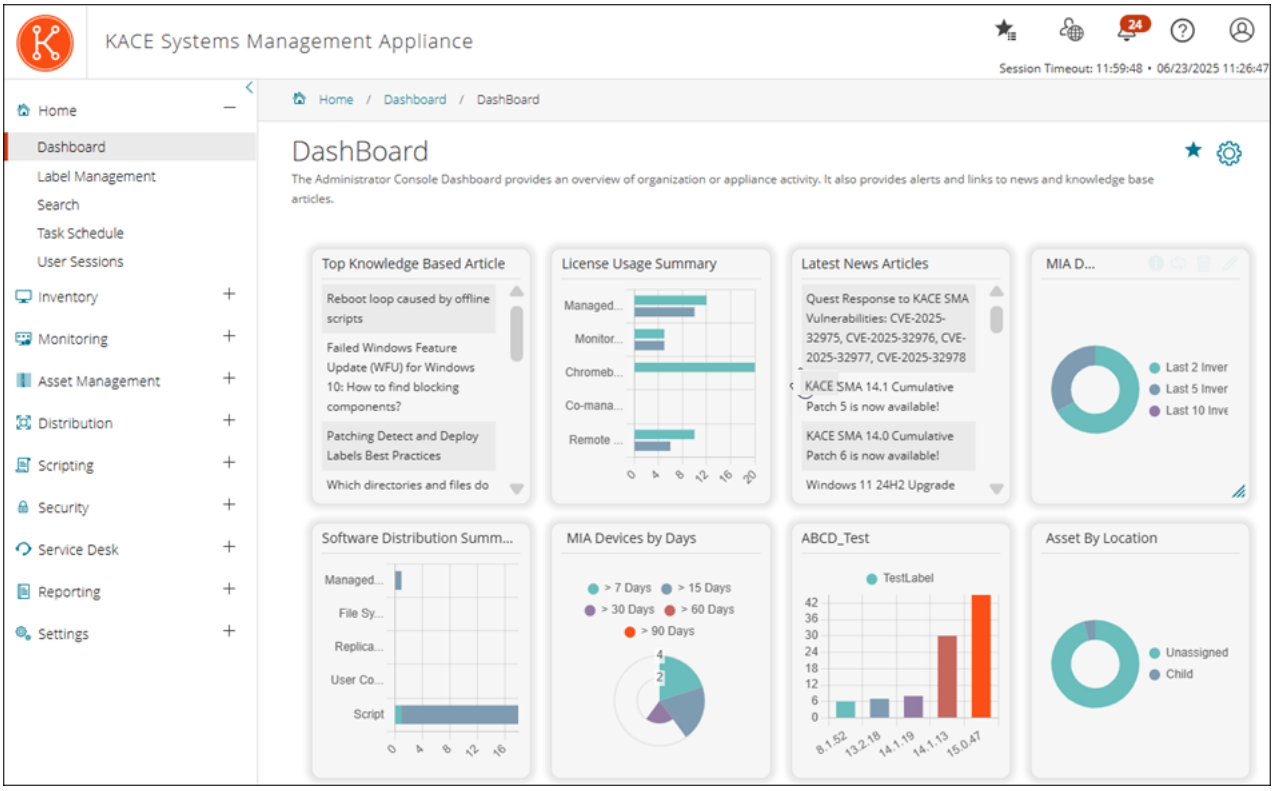

KACE Systems Management Appliance
24
Session Timeout: 11:59:48 • 06/23/2025 11:26:47
Home
Dashboard
Label Management
Search
Task Schedule
User Sessions
Inventory
Monitoring
Asset Management
Distribution
Scripting
Security
Service Desk
Reporting
Settings
Home / Dashboard / DashBoard
DashBoard
The Administrator Console Dashboard provides an overview of organization or appliance activity. It also provides alerts and links to news and knowledge base articles.
Top Knowledge Based Article
Reboot loop caused by offline scripts
Failed Windows Feature Update (WFU) for Windows 10: How to find blocking components?
Patching Detect and Deploy Labels Best Practices
Which directories and files do
License Usage Summary
Managed...
Monitor...
Chromeb...
Co-mana...
Remote ...
Latest News Articles
Quest Response to KACE SMA Vulnerabilities: CVE-2025-32975, CVE-2025-32976, CVE-2025-32977, CVE-2025-32978
KACE SMA 14.1 Cumulative Patch 5 is now available!
KACE SMA 14.0 Cumulative Patch 6 is now available!
Windows 11 24H2 Upgrade
MIA D...
Last 2 Inver
Last 5 Inver
Last 10 Inve
Software Distribution Summ...
Managed...
File Sy...
Replica...
User Co...
Script
MIA Devices by Days
> 7 Days
> 15 Days
> 30 Days
> 60 Days
> 90 Days
ABCD_Test
TestLabel
Asset By Location
Unassigned
Child

Table 2. Components available in Admin mode without the Organization component

Component	UI page	Used to...
Home	• Dashboard • Label Management • Search • Task Schedule • User Sessions	Review appliance statistics, manage labels, view historical information, and search for data. See Using the Home component.
Inventory	• Dashboard • Devices • Quarantine • Custom Inventory • Software • Software Catalog • Processes • Startup Programs • Services • Discovery Schedules • Discovery Results • SNMP Inventory Configurations	Manage the devices, software, processes, services, scans, and other items on your network. See: • Managing device inventory • Managing applications on the Software page • Managing Software Catalog inventory • Managing process, startup program, and service inventory • Using Device Discovery • Using SNMP Inventory Configurations to identify specific SNMP objects and non-computer devices to add to inventory
Monitoring	• Devices • Alerts • Profiles • Maintenance Windows • Log Enablement Packages	Manage basic event monitoring for 5 servers with your standard license, gathering event data from core Windows® event logs, syslogs, and application logs. With the Monitoring Module license, manage event monitoring for up to 200 servers.

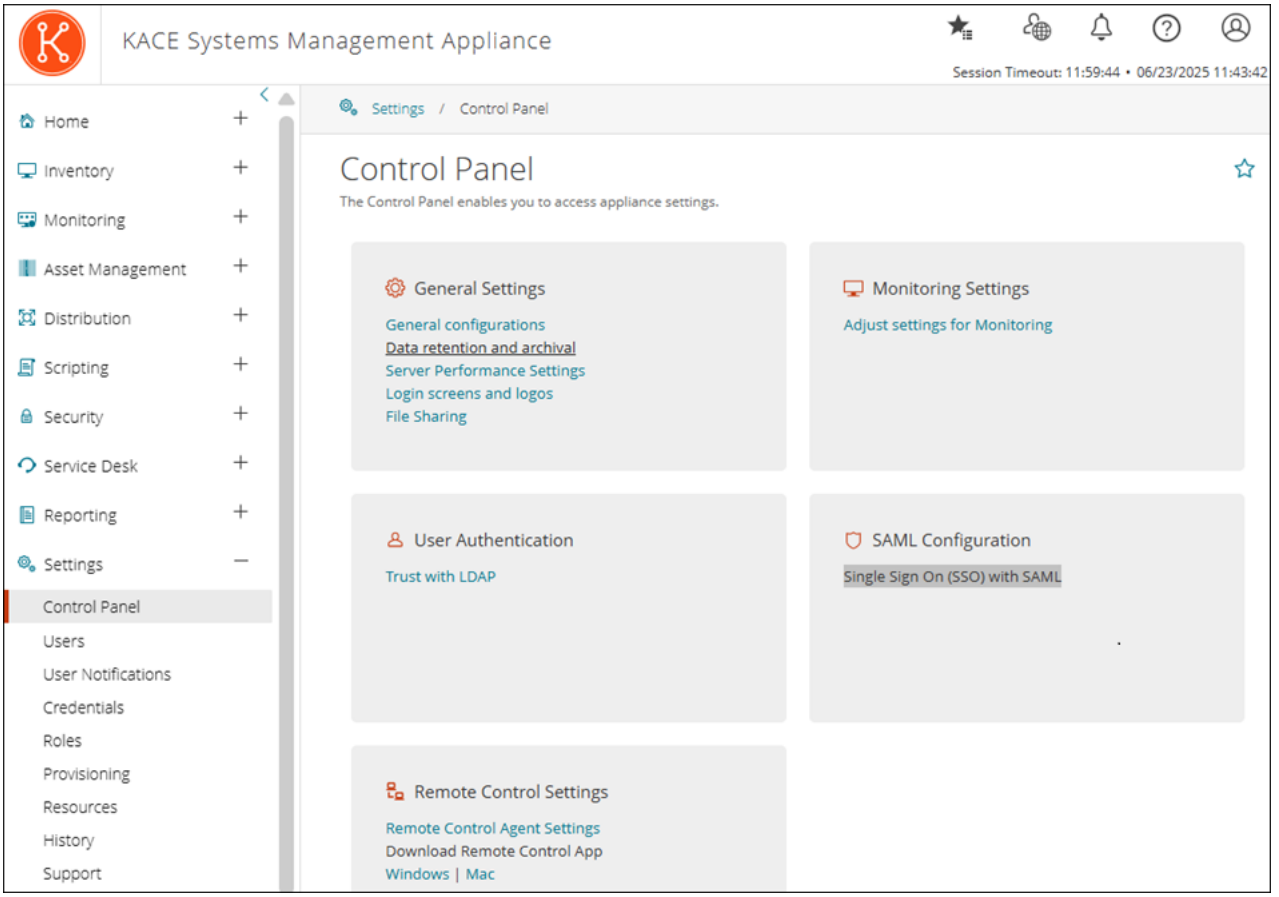
Component	UI page	Used to...
		See Monitoring devices
Assets	• Dashboard • Assets • Asset Types • Contracts • Purchases • Licences • License Compliance • Locations • Import Assets	Track physical assets, such as devices, software, printers, and so on, and view the history of assets and their configuration. See: • Managing inventory • Managing License Compliance
Distribution	• Managed Installations • File Synchronizations • Wake-on-LAN • Replication • Alerts • Task Chains	Distribute and manage software, including updates from Quest, remotely. See Deploying packages to managed devices.
Scripting	• Scripts • Run Now • Run Now Status • Search Scripting Logs	Automate tasks performed on managed devices. See Running scripts on managed devices.
Security	• Dashboard • Patch Management • Windows Feature Updates • Dell Updates • Linux Package Upgrades • Antivirus Quarantine	Reduce the risks from malware, spyware, and viruses. See Patching devices and maintaining security.
Service Desk (also known as *Help Desk* on appliances that have been upgraded from early versions)	• Dashboard • Tickets • User Downloads • Knowledge Base • Announcements • Archive (available only if ticket archival is enabled) • Configuration	Provide a repository of software and documentation for users to access and download. Includes a full-featured service desk for creating and tracking tickets. See Using the Service Desk.
Reporting	• Reports • Report Schedules • Notifications	Run pre-packaged reports and report-creating tools to monitor your appliance implementation.

Component	UI page	Used to...
		See Using reports and scheduling notifications.
Settings	• Control Panel • Users • User Notification • Credentials • Roles • Provisioning • Resources • History • Support • Agent Tokens	Administer your appliance and Agent provisioning. See: • Configuring the appliance • Configuring user accounts, LDAP authentication, and SSO • Managing credentials • Maintaining the appliance • Provisioning the KACE Agent • Importing and exporting appliance resources • Managing settings history • Using Troubleshooting Tools

Components available in Admin mode with the Organization component enabled

When the Organization component is enabled, the Admin mode shows components and settings for the current organization only. Appliance-level components are available in System mode.

If the Organization component is enabled on your appliance, and you log in to `http://`**appliance_hostname**`/admin`, the *Settings* component shows features available to the selected organization only.



All other components are the same, regardless of whether the Organization component is enabled. See Components available in Admin mode without the Organization component for components, and see the following illustration.

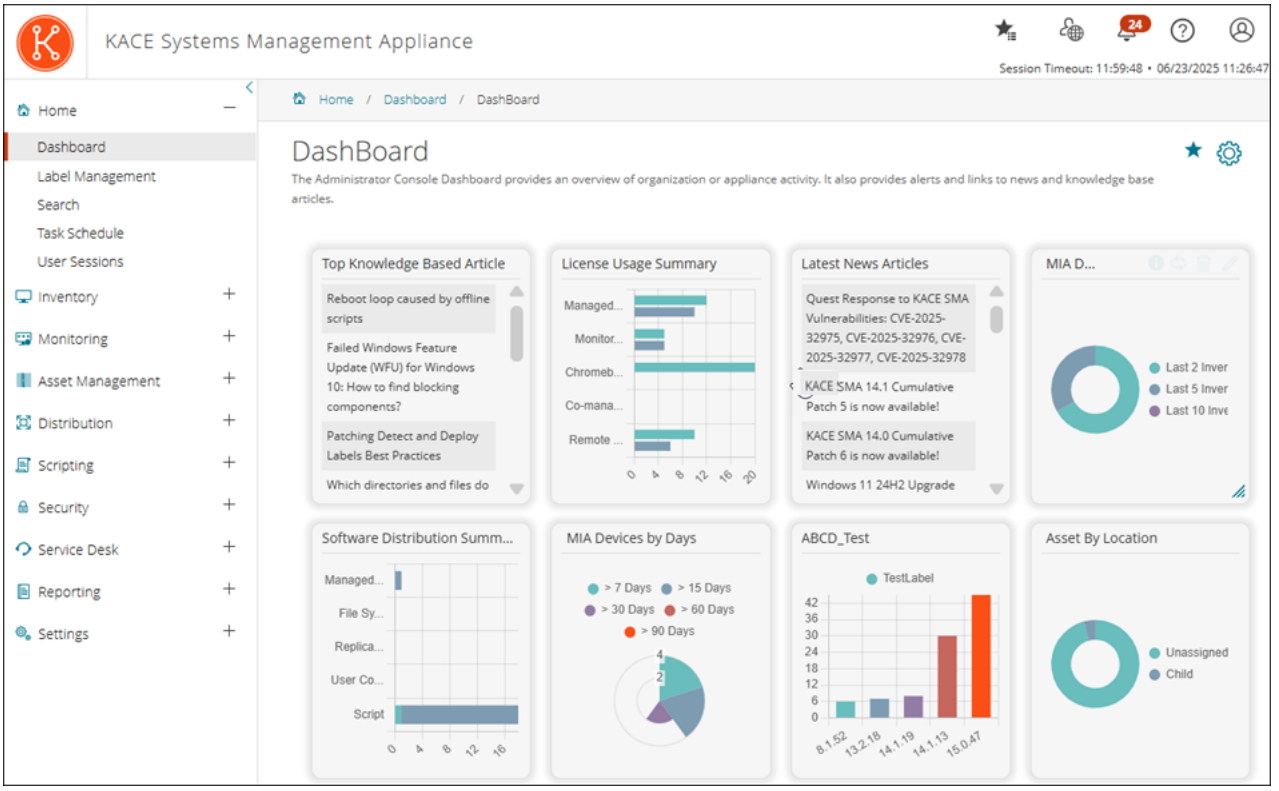


Table 3. Components available in Admin mode with the Organization component enabled

Component	UI page	Used to...
Settings	• Control Panel • Users • Credentials • Roles • Provisioning • Resources • History • Support	Manage general settings for the organization, such as user authentication and Agent provisioning. See: • Configuring the appliance • Configuring user accounts, LDAP authentication, and SSO • Managing credentials • Provisioning the KACE Agent • Importing and exporting appliance resources • Managing settings history • Using Troubleshooting Tools

Components available in System mode with the Organization component enabled

When the Organization component is enabled, System mode shows components related to appliance settings. Organization-level components are available in Admin mode.

When you log in to the appliance System Administration Console, `http://`**appliance_hostname**`/system`, or select **System** in the drop-down list in the top-right corner of the **Administrator Console**, the following components are available.

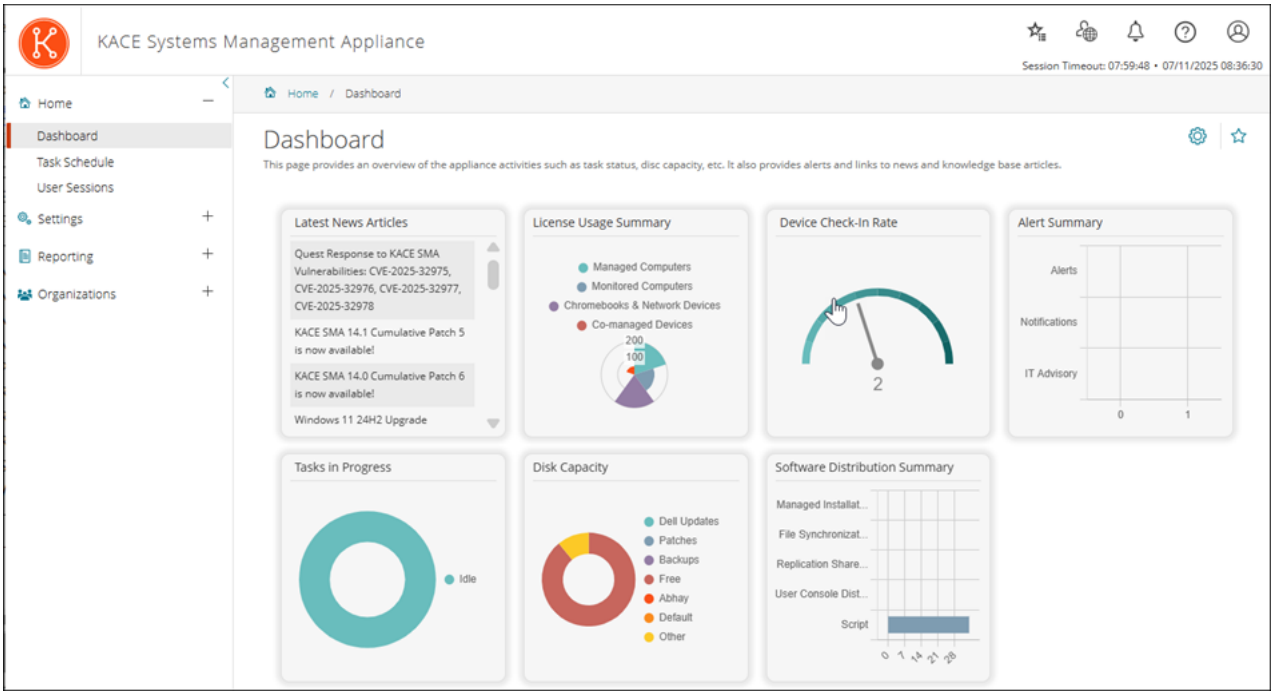


Table 4. Components available in System mode with the Organization component enabled

Component	Sub-tabs	Used to...
Home	• Dashboard • Task Schedule • User Sessions	Review summary statistics for the appliance. See Using the Home component.
Settings	• Control Panel • Administrators • Logs • Appliance Updates • Resources • History • Support • Agent Token	Manage the appliance and access resources such as **Quest Support**. See: • Configuring the appliance • Maintaining the appliance • Importing and exporting appliance resources • Managing settings history • Using Troubleshooting Tools
Reporting	• Reports • Report Schedules	Run pre-packaged reports and report-creating tools to monitor your appliance implementation.

Component	Sub-tabs	Used to...
		See Using reports and scheduling notifications.
Organizations	• Organizations • Roles • Filters • Devices • Quarantine	Add and manage organizations (requires the Organization component). See Creating and managing organizations.

Using the Home component

The Home component includes the Dashboard, Label Management, and Search features.

About Dashboards

Dashboards provide overviews of organization or appliance activity. They also provide alerts and links to news and Knowledge Base articles.

If the Organization component is enabled on the appliance, and you are logged in to the Administrator Console (`http://`**appliance_hostname**`/admin`), the Dashboard shows information for the selected organization. When you are logged in to the System Administration Console (`http://`**appliance_hostname**`/system`), the Dashboard shows information for the appliance, including all organizations.

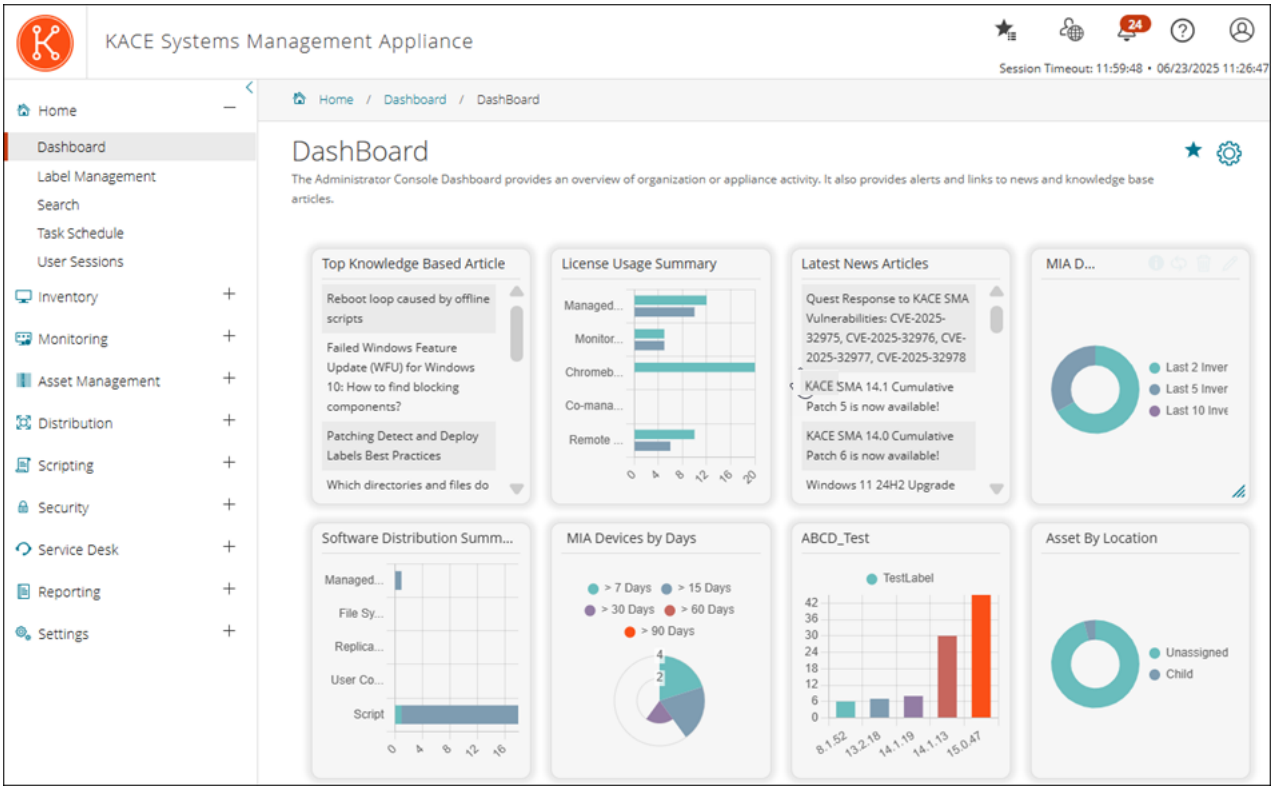
TIP: The appliance updates the summary widgets periodically. To update most of the widgets any time, click the icon and then the **Force Refresh** button. To update an individual widget, hover over the widget, then click the **Refresh** button above the widget. Some widgets may require additional steps.

View the Dashboard in Admin mode

View the Admin mode Dashboard to find summary information for the appliance or, if the Organization component is enabled, for the selected organization.

- Log in to the Administrator Console , `http://`**appliance_hostname**`/admin`. Or, if *Show organization menu in admin header* is enabled, select an organization in the drop-down list in the top-right corner of the page next to the login information.

The *Dashboard* page appears.

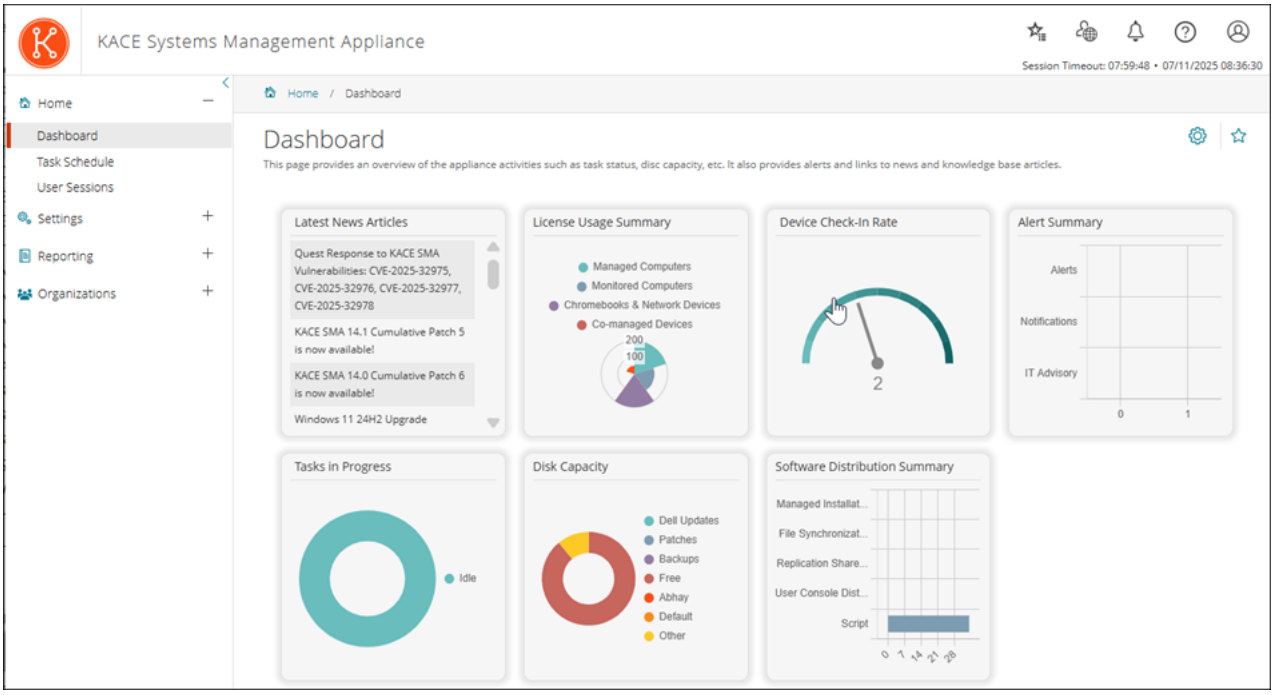


View the Dashboard in System mode

If the Organization component is enabled on your appliance, view the System Dashboard to find summary information for the appliance.

- Log in to the appliance System Administration Console, `https://`**appliance_hostname**`/system`, or select **System** from the drop-down list in the top-right corner of the page.

The *System Dashboard* page appears.



About Dashboard widgets

Dashboard widgets provide overviews of organization or appliance activity.

This section describes the widgets available on the *Dashboard*. If the Organization component is enabled on your appliance, widgets show the information for the selected organization at the Admin level and for the appliance at the System level.

Widget	Description
General widgets	This section provides a high-level overview of your appliance activity. The information appearing in these widgets allows you to focus on specific indicators that can help you understand any potential issues.
Latest News Articles and Top Knowledge Base Articles	These widgets provide links to news and information from Quest. News articles are displayed according to date or importance. Knowledge Base articles are displayed according to their priority in the Technical Support system.
Connections	This widget shows the number of connections to the appliance web server. A high number indicates a high load on the server, which might reduce appliance response time. If the Organization component is enabled on your appliance, the widget shows the information for the selected organization.
File Synchronizations	This widget shows the number of File Synchronizations that are in progress on Agent-managed devices. If the Organization component is enabled on your appliance, the widget shows the information for the selected organization.
Managed Installations	This widget shows the number of Managed Installations that are in progress on Agent-managed devices. If the Organization component is enabled on your appliance, the widget shows the information for the selected organization.

Widget	Description
Current Scripts	This widget shows the number of scripts that are enabled to run on Agent-managed devices. If the Organization component is enabled on your appliance, the widget shows the information for the selected organization.
License Compliance	If you have created License assets for software, this widget shows the number of Agent-managed devices that have a particular licensed software installed, and the number of licenses available. If the Organization component is enabled on your appliance, the widget shows the information for the selected organization. License assets can be created for applications listed on the *Software* page and the *Software Catalog* page, and the license mode for applications must be *Unit License* or *Enterprise* for license information to appear on this widget. Applications with other license modes, such as *Shareware*, *Freeware*, or *Not Specified*, are not displayed on this widget. This widget is for information only, and the appliance does not enforce license compliance. For example, the appliance does not prevent software from being installed on Agent-managed devices if a license is expired or otherwise out of compliance. The following colors indicate threshold levels: • **Red**: Usage is at or above the critical threshold setting. • **Orange**: Usage is at or above the warning threshold setting but below the critical threshold setting. • **Green**: Usage is below the warning threshold setting. To change the threshold levels, see Configure appliance General Settings without the Organization component. For information about managing License assets, see Managing inventory.
Provisioning	This widget shows the status of KACE Agent provisioning or installation tasks. If the Organization component is enabled on your appliance, the widget shows the information for the selected organization.
Provision Platforms	This widget shows the percentage of operating systems installed on Agent-managed devices. If the Organization component is enabled on your appliance, the widget shows the information for the selected organization.
Tasks in Progress	This widget displays the number of tasks in progress on the appliance. This number includes tasks related to scripting, inventory, metering, replication, patching, bootstrapping, and cache queries. You can view the load average on the appliance, and change the task throughput, as needed. See Configure Agent communication and log settings. If the Organization component is enabled on your appliance, the widget is available on the *System Dashboard* page.
Device Check-In Rate	This widget displays the number of devices that have connected to the appliance in the past 60 minutes. If the Organization component is enabled on your appliance, this widget is available at the System level.
Software License Configuration	If you set up License assets for software, and specify the license type, such as site, subscription, or unit, that information is displayed in this widget. If the Organization component is enabled on your appliance, the widget shows the information for the selected organization.

Widget	Description
Disk Capacity	This widget displays the amount of disk space that is free or in use on the appliance. If the Organization component is enabled on your appliance, this widget is available at the System level.
Software Publishers	This widget displays the publishers defined in the Software Catalog, with the highest number of software titles installed on managed devices. If the Organization component is enabled on your appliance, the widget shows the information for the selected organization.
Software Titles	This widget displays the software titles defined in the Software Catalog, with the highest number of installations on managed devices. If the Organization component is enabled on your appliance, the widget shows the information for the selected organization.
Expiring Dell Warranties	This widget displays information on any Dell Warranties, and links to the *Reports* list page for Dell Warranty reports. If the Organization component is enabled on your appliance, the widget shows the information for the selected organization.
Monitoring Alert Summary	This widget displays the number of unacknowledged alerts, grouped by alert level. The following icons indicate alert level: • : **Critical** • : **Error** • : **Warning** • : **Information** • : **Recovered** If the Organization component is enabled on your appliance, the widget shows the information for the selected organization. **Low-resource alerts.**When the appliance resources are low, Critical alerts appear on the Dashboard, providing the recommended course of action such as contacting Support. These alerts are generated when the appliance is detected to use a high amount of disk, CPU, and memory resources, or when a high number of emails is received. Critical low-resource alerts are displayed when the related condition is detected within the last ten minutes, and it persisted for one hour before being displayed. The settings for these alerts are tracked in the history settings. You can disable that by clearing any of the *Low Resource Alerts* options on the *Settings History Configuration* page. For more information, see .
Monitored Devices	This widget displays the status of the devices for which monitoring has been enabled. If the Organization component is enabled on your appliance, the widget shows the information for the selected organization.
Monitoring Alerts	This widget displays the alert messages for the devices being monitored. If the Organization component is enabled on your appliance, the widget shows the information for the selected organization.
Dell Hardware Expiring Warranty	This widget displays Dell devices with warranties nearing expiration.

Widget	Description
Lenovo Hardware Expiring Warranty	This widget Lenovo devices with warranties nearing expiration.
MIA Devices by Inventory	This widget displays the counts of devices that missed their last 2, 5, and 10 inventory updates.
MIA Devices by Days	This widget displays the counts of devices that missed their inventory updates for the last 7, 15, 30, 60, and 90 days.
Software Distribution Summary	The widget shows the count per software distribution type.
Discovery (Network Scan) Summary	The widget shows the count per discovery type.
Monitoring Alert Summary	The widget shows the counts of unacknowledged alerts by alert level. (for Admin UI only)
License Usage Summary	The widget shows the license usage count per type.
Alert Summary	The widget shows the count per alert type.
Service Desk widgets	This section provides a high-level overview of your Service Desk ticket performance. Use it to quickly review the state of your tickets and look for any indicators that can improve your customer experience. For example, you can review the numbers of overdue tickets and focus on specific issues, as needed. **NOTE:** Service Desk widgets display data for the default queue associated with the logged-in user. If there is no default set for the user, or if *All Queues* is set as the default, the widgets display data from all the queues owned by the user. **NOTE:** If the user does not own any queues, or if their default queue is no longer valid, the widgets do not display any data.
Shortcuts	This widget contains links to common Service Desk actions. Use them to quickly initiate specific tasks, such as creating a new KB (Knowledge Base) article, scheduling a report, and so on.
Views	This widget contains links to common Service Desk pages and wizards, including any custom views that you created. Use them to quickly navigate to specific pages, such as *My Recent Tickets*, *All Unassigned Tickets*, and *Tickets Due Today*. It also displays link to custom views, as applicable. The list of custom views is sorted alphabetically. If you want the custom views to appear in a specific order, you can prefix their names with numbers, as needed.
Reports	This widget contains links to common Service Desk reports. Use them to quickly generate a specific report, such as *Open Tickets last 7 days by Owner*, *Stalled/Open Tickets by Owner*, and others.
Tickets Opened Today	This widget contains the number of Service Desk tickets that were opened today.

Widget	Description
Active Tickets By Owner Active Tickets By Category Active Tickets By Priority Active Tickets Closed Tickets Overdue Tickets Overdue Tickets By Owner Overdue Tickets Today Tickets Due Today Reopened Tickets	These widgets display the numbers of active, closed, overdue, overdue today, due, due today, or reopened Service Desk tickets, grouped into any of the following categories: • Category • Priority • Owner • Queue • Range The resulting data can appear in a *Bar Chart* or a *Donut Chart*. To change the widget title, choose how you want to group the tickets, or select the chart type, click in the widget. In the dialog box that appears, make your edits and click **Save**.
Average Ticket Resolution Time	This widget displays the average number of days the ticket resolution takes over that last 30 days, grouped into any of the following categories: • Category • Priority • Owner • Queue • Month The resulting data can appear in a *Bar Chart* or a *Doughnut Chart*. To change the widget title, choose how you want to group the tickets, or select the chart type, click in the widget. In the dialog box that appears, make your edits and click **Save**.
Overdue Tickets Count	This widget displays the number of Service Desk tickets that are currently overdue.
Device widgets	This section provides a high-level overview of your managed devices. Use it to quickly review the state of your devices and look for any indicators that can improve their performance. For example, you can review the percentages of available disk space, and focus on specific issues, as needed.
Devices By Memory	This widget shows a bar chart, where each bar represents a number of devices that have an indicated amount of RAM installed on them.

Widget	Description
Devices By Processor	This widget shows a bar chart, where each bar represents a number of devices that have a specific processor configuration.
Devices by Disk Capacity	This widget shows a donut chart, where each section of the chart indicates the percentage of free disk space on the managed devices. Clicking the widget title displays a report with links to the associated devices. Hovering over each section of the chart displays the percentage of managed devices that have the selected percentage of free disk space. For example, if you hover over the red part of the chart, the widget displays the percentage of devices whose free disk space is lower than 25%.
Managed Operating Systems	This widget shows the percentage of managed devices that are running each operating system. If the Organization component is enabled on your appliance, this widget shows the percentage of devices in the selected organization.
Devices By Manufacturer	This widget shows the top device manufacturers represented in device inventory. If the Organization component is enabled on your appliance, this widget shows the percentage of devices in the selected organization.
Devices By Model	This widget shows the top device models represented in the device inventory. If the Organization component is enabled on your appliance, this widget shows the percentage of devices in the selected organization.
Devices By Subtype	This widget shows a donut chart, where each section of the chart indicates the percentage of the managed devices by device subtype.
VMware Device Counts	This widget shows the counts of each VMware device type, such as vCenters, ESXi hosts, virtual machines, and provisioned virtual machines. Clicking the widget title displays the *Devices* list page.
VMware Device Reports	This widget contains links to five popular VMware inventory reports. Clicking the widget title displays the *Reports* list page with the *Virtual Infrastructure* filter applied.
VMware ESXi Device By Status	This widget displays a donut chart showing the current status of ESXi devices. There are four possible values: *OK*, *Warning*, *Error* and *Unknown*. Clicking the widget title displays a new VMware inventory report that lists all ESXi devices by current status.
VMware ESXi Version Counts	This widget shows the counts of the top five ESXi versions. Clicking the widget title displays a new VMware inventory report that shows all ESXi devices by version.
Asset Management widgets	This section provides a high-level overview of your asset usage. Use it to quickly review the state of your assets and look for any indicators that can improve your asset configuration. For example, you can focus on how your software licenses are used and identify which software titles need to have their license renewed.
Assets By Type	This widget shows a donut chart, where each section of the chart indicates the percentage of your assets by their asset type, such as device, software, location, license, and others. Hovering over each section of the chart displays the percentage of the assets of the selected type.
Assets By Status	This widget shows a donut chart, where each section of the chart indicates the percentage of your assets by their status, such as Active, Disposed, Missing, or other.

Widget	Description
	Hovering over each section of the chart displays the percentage of the assets in the selected status.
Cost ($) of Unused Licenses By Product	This widget shows a bar chart, where each bar represents the cost of unused licenses for each product. You can use this information to reassign or cancel unused licenses, and to redirect your resource where they are most needed.
License Compliance	If you have created License assets for software, this widget shows the number of Agent-managed devices that have a particular licensed software installed, and the number of licenses available. If the Organization component is enabled on your appliance, the widget shows the information for the selected organization. License assets can be created for applications listed on the *Software* page and the *Software Catalog* page, and the license mode for applications must be *Unit License* or *Enterprise* for license information to appear on this widget. Applications with other license modes, such as *Shareware*, *Freeware*, or *Not Specified*, are not displayed on this widget. This widget is for information only, and the appliance does not enforce license compliance. For example, the appliance does not prevent software from being installed on Agent-managed devices if a license is expired or otherwise out of compliance. The following colors indicate threshold levels: • **Red**: Usage is at or above the critical threshold setting. • **Orange**: Usage is at or above the warning threshold setting but below the critical threshold setting. • **Green**: Usage is below the warning threshold setting. To change the threshold levels, see Configure appliance General Settings without the Organization component. For information about managing License assets, see Managing inventory.
Software Titles	This widget displays the software titles defined in the Software Catalog, with the highest number of installations on managed devices. If the Organization component is enabled on your appliance, the widget shows the information for the selected organization.
Software Publishers	This widget displays the publishers defined in the Software Catalog, with the highest number of software titles installed on managed devices. If the Organization component is enabled on your appliance, the widget shows the information for the selected organization.
Assets by Location	This widget shows a donut chart, where each section of the chart indicates the percentage of your assets by their location. Hovering over each section of the chart displays the percentage of the assets in the selected location.
Software Installed But Not Used in 60 Days	This widget shows a bar chart, where each bar represents a software title and the corresponding number of instances of that product that have not been in use in the last 60 days. You can use this information to further investigate whether these titles are needed, to reassign or uninstall unused software, and to redirect your resource where they are most needed.

Widget	Description
Expiring Software License Maintenance	This widget shows a vertical bar chart, where each bar represents the number of software licenses that are about expire in the given time period.
Expired Software License Maintenance	This widget shows a donut chart representing the ration of expired and current licenses. Hovering over each section of the chart displays the percentage of the software licenses that are either expired or current, as selected.
Expiring Contracts	This widget shows a vertical bar chart, where each bar represents the number of contracts that are about expire in the given time period.
Expired Contracts	This widget shows a donut chart representing the ration of expired and current contracts. Hovering over each section of the chart displays the percentage of the contracts that are either expired or current, as selected.
Software License Configuration	If you set up License assets for software, and specify the license type, such as site, subscription, or unit, that information is displayed in this widget. If the Organization component is enabled on your appliance, the widget shows the information for the selected organization.
Security widgets	This section provides an overview of patch compliance in your environment, and the information about patching processes. Use it to quickly review the level of system patches installed on managed devices and look for any indicators that can improve your system security.
Critical Patch Compliance	This widget shows the deployment progress of patches that are marked as critical. If the Organization component is enabled on your appliance, the widget shows the information for the selected organization.
Dell Updates	This widget displays the number of Dell applications, BIOSs, and firmware updates that can be applied to managed devices. The updates are categorized as *Moderate*, *Important*, or *Critical*, depending on the urgency of the update. After a Dell Update schedule is created, data appears in the widget. See Configure Dell Update schedules. If the Organization component is enabled on your appliance, the widget shows the information for the selected organization.
Compliance By Machine	This widget displays a donut chart, where each section of the chart indicates the percentage of patch compliance for each managed device. Hovering over each section of the chart displays the percentage of the patch compliance for the selected device. You can change the information that appears in the widget by choosing the patch publisher, operating system, label, classification, severity, KB number, and availability date. You can also switch between any chart type that is applicable. You can also install multiple instances of this widget on the Security Dashboard using a different set of parameters in each instance.
Compliance By Patch	This widget provides a donut chart, where each section of the chart indicates the percentage of compliance for each applicable patch. Hovering over each section of the chart displays the percentage of the compliance for the selected patch. You can change the information that appears in the widget by choosing the patch publisher, operating system, label, classification, severity, KB number, and availability date. You can also switch between any chart type that is applicable. You can also

Widget	Description
	install multiple instances of this widget on the Security Dashboard using a different set of parameters in each instance.
Patch Installation Progress	This widget shows the progress of patching tasks that are running on managed devices. If the Organization component is enabled on your appliance, the widget shows the information for the selected organization.
Patches Deployed	This widget displays the number of patches that are currently deployed. You can change the information that appears in the widget by choosing the patch publisher, operating system, label, classification, severity, KB number, and availability date. You can also switch between any chart type that is applicable. You can also install multiple instances of this widget on the Security Dashboard using a different set of parameters in each instance.
Patches Failed	This widget displays the number of patches that failed to deploy. You can change the information that appears in the widget by choosing the patch publisher, operating system, label, classification, severity, KB number, and availability date. You can also switch between any chart type that is applicable. You can also install multiple instances of this widget on the Security Dashboard using a different set of parameters in each instance.
Patches Released	This widget displays the number of patches that are released and available for deployment. You can change the information that appears in the widget by choosing the patch publisher, operating system, label, classification, severity, KB number, and availability date. You can also switch between any chart type that is applicable. You can also install multiple instances of this widget on the Security Dashboard using a different set of parameters in each instance.
Patching Tasks Completed	This widget shows the progress of patching tasks, such as detect, deploy, and rollback tasks, on managed devices. If the Organization component is enabled on your appliance, the widget shows the information for the selected organization.
Security Reports	This widget contains links to common patching reports. Use them to quickly generate a specific report, such as *Critical and Recent Bulletin List* , *Devices not compliant by patch*, and others.
Security Views	This widget contains links to common patching pages and wizards, including any custom views that you created. Use them to quickly navigate to specific pages, such as the *Patch Catalog*. If you have any custom views, they are sorted alphabetically. If you want the custom views to appear in a specific order, you can prefix their names with numbers, as needed.
Windows 10 Releases	This widget shows a bar chart, with each item in the chart representing a particular Windows 10 release and the number of managed devices running that version. This can give you an idea of how many devices are candidates for published Windows 10 updates.
Windows 11 Releases	This widget shows a bar chart, with each item in the chart representing a particular Windows 11 release and the number of managed devices running that version. This can give you an idea of how many devices are candidates for published Windows 11 updates.

Widget	Description
Device Patch Status Breakdown by CVSS	This widget shows the number of patched and unpatched devices by CVSS severity scores.
Patch Status Breakdown by CVSS	This widget shows the number of patches by patch status and CVSS severity scores.
Patch by CVSS Score	This widget shows the patch counts by CVSS severity scores.
Exposure by CVSS Score	This widget shows the number of unpatched devices and patches by CVSS severity levels.

Customize Dashboard pages

You can customize Home Dashboard page to show or hide widgets as needed.

1. Do one of the following:
   - **Log in to the appliance Administrator Console, `https://appliance_hostname/admin`. Or, if *Show organization menu in admin header* is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.**
   - **Log in to the appliance System Administration Console, `https://appliance_hostname/system`, or select System from the drop-down list in the top-right corner of the page.**

   The *Dashboard* or *System Dashboard* page appears.
2. Hover over the widget, then use any of the following buttons:
   # : Refresh the information in the widget.
   # : Display information about the widget.
   # : Edit the widget.
   # : Remove the widget.
   # : Resize the widget.
   # : Drag the widget to a different position on the page.
3. The widgets are editable, allowing you to modify the information that they display. To edit a widget, click and in the dialog box that appears, modify the required information. You can also edit the chart type. Based on the chart type you select from the drop down list, the relevant fields populate.
4. Click the button in the top-right corner of the page to view the list of available widgets.

   For information on how to add widgets to the dashboard refer Adding a Widget.

Work with Dashboard Settings

When you click the icon, the dashboard settings panel displays. You get to see the following options:

Dashboard Name	Description

Switch Dashboard	You can switch to different dashboards. For more information, refer to Switching Dashboard.
Dashboard Settings	You can customize the look and feel of the widgets. For more information, refer to Setting Home Dashboard
Add New Dashboard	You can add a new dashboard. For more information, refer to Adding a New Dashboard
Add Widget	You can add widgets to the dashboard. For more information, refer to Adding a Widget
Email Dashboard	You can share a dashboard snapshot through email. For more information, refer to Emailing Home Dashboard
Force Refresh	You can refresh all the widget data on the dashboard. For more information, refer to Refreshing Home Dashboard Data Manually

Switching Dashboard

You can seamlessly navigate between multiple dashboards within the application interface. This is especially useful in environments where dashboards are tailored for different roles, tasks, or organizational contexts. By switching dashboards, you can improve focus and efficiency by quickly accessing the most relevant set of widgets and data visualizations needed for your specific responsibilities.

To switch a dashboard,

1. Click the icon to open the Switch Dashboard panel.
2. You can view the Sort By and Search fields. There is a list of dashboards that you have created.
3. You can perform any of the following action:
   - **In the Sort By field, select the desired dashboard from the drop-down list, and then click the selection.**
   - **In the Search field, enter a keyword to refine the list and then click the selection.**
   - **From the displayed dashboard names list, select the desired dashboard, and then click the selection.**

   The selected dashboard opens.

Setting Home Dashboard

You can customize the look and feel of the widgets and the dashboards.

You can change the color used in the dashboard charts, edit the name dashboard name and its description, change the display of the widgets.

To customize a dashboard,

1. Click the icon to open the Switch Dashboard panel.
2. Make changes to the fields as required:

Fields	Description
Name	Add/Edit name for the dashboard. This is displayed on the dashboard.
Description	Add/Edit description of the dashboard. This describes the dashboard.

Choose Your Colors	Click on the color selector to choose your dashboard chart colors. Drag and drop the colors to arrange them in the desired order. The colors at the top of the list will be used by each chart first.
Layout	Chose one of the layout options. The widgets and other elements are displayed in the selected layout.
Make Default	Optional. Select the option if you want to make the dashboard as a default one. **NOTE:** This field is available only for the Home Dashboard.

3. Click Save.

   The changes gets reflected on the dashboard.

NOTE: Follow the steps 1 to 3 to add/edit settings for the Inventory dashboard, Asset Management dashboard, Security dashboard, and Service Desk dashboard.

Adding a New Dashboard

You can create different dashboards for various purpose.

- To get tailored insights - You can visualize data relevant to specific roles or tasks.
- For real-time monitoring - You can track system health, compliance, and activity instantly.
- For better decision-making - You can identify trends and issues through charts and graphs.
- To view role-based view - You can customize dashboards for different teams and permissions.
- For improved efficiency - You can access key information at a glance, thus, saving time.
- For automated reporting - You can schedule dashboards to be emailed to stakeholders.
- For audit readiness - You can track performance and compliance metrics for reviews.

Add a new Dashboard

To add a new dashboard,

1. Click the icon to open the dashboard settings panel.
2. Click the Add New Dashboard to open the Add New Dashboard dialog.
3. Enter details in the Name and Description fields.
4. Click Save.

Adding a Widget

You can add widgets to the Home Dashboard. There is a list of widgets in the Add Widgets panel. You can enter a keyword in the Search text box to refine the list, then click on your selection.

You can search for the desired widget in the following ways:

To add widgets to the dashboard,

1. Click the icon and then click Add Widget to open the **Add Widget** panel.
2. Search for the desired widget in the following ways:
   - **In the Filter By drop-down, select the widget by category.**
   - **In the Sort By drop-down, select the widget by title or newest.**
   - **In the Search field, enter a keyword to refine the list.**

The refined result displays.

3. Click the desired widget.

   The widget gets added to the dashboard.

Emailing Home Dashboard

You can share a snapshot of dashboard through email, send it to multiple users, and configure the frequency of email.

To email a dashboard,

1. Click the icon to open the dashboard settings panel.
2. Click the Email Dashboard option to open the Email Dashboard panel.
3. Select appropriate option from the given options:
   a. **Send Now**: You can send an email immediately.
   b. **Schedule**: You can set the frequency of sending a snapshot of dashboard through email.

The detailed steps for each option are given below:

Send email now

To send email immediately,

1. Click **Send Now** to open the Email Dashboard dialog.
2. Enter details in the Email Address, Subject, and Message fields.
3. Choose the layout in which you want the widgets to appear.
4. Click Send.

   The dashboard is sent through email.

Schedule

To set the frequency of sending a snapshot of dashboard through email,

1. Click **Schedule** to open the Schedule dialog.
2. Enter details in the Subject and **Message** fields.
3. Choose the layout in which you want the widgets to appear.
4. To add recipients, select the names from the **Select user to add drop down list**.

   NOTE: You can add multiple recipients from the list.

5. Select the frequency from the drop down list.
6. In the **Next Run** field that appears after you select the **Frequency**, set the date, month, and time for the next email delivery.
7. Click Save. The dashboard is sent through email according to the set schedule.

Refreshing Home Dashboard Data Manually

You can refresh the widgets data to show the latest results on the dashboard.

To update the widgets,

1. Click the icon to open the dashboard settings panel.
2. Click **Force Refresh** to open the Confirm dialog box.
3. Click **Yes** to confirm refresh all widget data on the dashboard.

Bookmark a page as Favorite

You can bookmark frequently accessed pages or favorite pages by marking them with a star icon. You can mark pages as favorites, manage favorite pages, and quickly access them.

This feature improves navigation efficiency by allowing users to bookmark frequently accessed pages. This feature is useful for administrators managing large environments where quick access to repetitive workflow is essential. The Favorites feature offers the following capabilities:

- It is available in both Admin and System UI.
- It supports up to 50 favorites per UI.
- The bookmarks are saved for each user and per organization.
- It supports only static pages and it does not support dynamic or context-driven pages.
- It includes drag-and-drop reordering, search, and delete options.
- If a user's access to a module is revoked after it was bookmarked, and the user clicks the bookmarked item from the favorites list, then the user is logged out.

Bookmarking a Page

There is a blank star icon ☆ that appears at the top-right corner of each page.

To bookmark a page,

1. Click the ☆ icon on the page to open the Favorite dialog.
2. Enter a suitable name for the page, in the text box.
3. Click Save.

   The ☆ icon changes to ★, indicating the page is bookmarked. The page appears in the bookmarked pages list.

Viewing the Favorite pages list

You can view the list of favorite pages.

To view the favorite pages,

1. Click the ★ icon to open the Favorite pane.

   The bookmarked pages list displays here. You can search the pages using the Search option.

Editing or Removing a Bookmark

You can modify, remove, or unmark previously bookmarked page (indicated by a blue star).

1. To Edit a bookmark
   a. Click the ★ icon to open the **Favorite** dialog.
   b. In the **Title** field, update the bookmark name.
   c. Click Save.

      The name reflects in the bookmark pages list.
2. To Delete a bookmark
   a. Click the ★ icon to open the **Favorite** dialog.
   b. Click Delete to open the **Confirm** dialog.
   c. Click Yes.

The name gets deleted from the bookmark pages list.

Reordering Bookmarks

You can reorder the bookmarks in the Favorite list.

To reorder the bookmarks,

- Drag and drop entries in the list to change the sequence.
- The new order is saved and reflected in the user's list.

View task schedules

The *Task Schedule* page displays a list of tasks scheduled for the current hour, day, or the week, as selected, using their start times and an estimated duration based on machine counts and task types. Any tasks that have detail pages associated with them, such as scripts, can be accessed by clicking the task name in the table.

The **Administrator Console** displays the tasks associated with the selected organization and any System tasks, like the *Backup Window*. When you view this page in the **System Administration Console**, it displays all tasks from all organizations (separated by the organization), along with any available System tasks.

Any task chains that appear in the page are represented with connecting lines. For more information about task chains, see Using Task Chains.

Tasks associated with multiple agents and devices appear in gradient color line, where the length of the line does not reflect the task duration or any historical data. Solid color lines appears indicates tasks with a fixed duration. A blue vertical bar in the graph represents the current date and time.

1. Do one of the following:
   - **Log in to the appliance Administrator Console, `https://appliance_hostname/admin`. Or, if *Show organization menu in admin header* is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.**
   - **Log in to the appliance System Administration Console, `https://appliance_hostname/system`, or select System from the drop-down list in the top-right corner of the page.**

   The *Dashboard* or *System Dashboard* page appears.
2. On the left navigation bar, in the **Home** section, click **Task Schedule**.

   The *Task Schedule* page appears.
3. To switch between different levels of detail, click **Hour**, **Day**, or **Week**, as required.

View the appliance version, model, and license information

The **About appliance** link in the *Help* panel displays the appliance version, model, and license information.

1. Log in to the User Console, Administrator Console, or System Console.
2. In the upper right of the Administrator Console, click **Help**.

   A help pane appears on the right containing high-level information about the related Administrator Console page. The bottom of the help pane includes the following buttons:

   # **Appliance Administrator Guide**(): Provides access to the KACE System Management Appliance help contents.

   # **Knowledge Base** (): Allows you to browse the Knowledge Base articles associated with the related **Administrator Console** page.

> **NOTE:** This option is only available in the **Administrator Console** and the System Console. It does not appear in the **User Console**.

Video Tutorials (): Allows you to browse one or more training videos associated with the related **Administrator Console** page. You can play a video on the help pane, in a smaller window outside of the selected page, or on the target Knowledge Base page that hosts the video.

> **NOTE:** This option is only available if related videos exist on the Support Portal. Also, it only appears in the **Administrator Console** and the System Console. It does not appear in the **User Console**.

Chat (): Starts a chat with a KACE System Management Appliance product specialist.

> **NOTE:** This option is only available in the **Administrator Console** and the System Console. It does not appear in the **User Console**.

Open Ticket (): Links to the Support page (https://support.quest.com/create-service-request) that allows you to create a service request.

> **NOTE:** This option is only available in the **Administrator Console** and the System Console. It does not appear in the **User Console**.

Support (): Links to the **Settings > Support** page. This page provides resources for troubleshooting system management issues and contacting **Quest Support**.

> **NOTE:** This option is only available in the **Administrator Console** and the System Console. It does not appear in the **User Console**.

Mobile App (): Displays a dialog containing links for downloading the KACE GO Mobile App. The app is available for iOS and Android platforms.

> **NOTE:** This option is available if the appliance is configured to interact with the K1 GO Mobile App. It only appears in the **Administrator Console** and the System Console. It does not appear in the **User Console** For more information on enabling mobile access, see Configuring Mobile Device Access.

About (): Displays information about your KACE System Management Appliance installation.

> **NOTE:** This option is only available in the **Administrator Console** and the System Console. It does not appear in the **User Console**.

3. Click the **About** link located at the bottom-right corner of the panel.

The appliance license information is displayed.

The appliance version, model, and serial numbers.

The license expiration date, in `month/day/year` format.

The number of Managed Computers, Monitored Computers, Chromebooks & Network Devices, and Remote Control Computers that your license entitles you to manage.

  # **Managed Computers**: The number of Managed Computers your license entitles you to manage. **Managed Computers** are devices in the inventory that 1) have Windows, Mac, Linux, or UNIX operating systems, 2) are categorized as PCs or servers, and 3) were not added to inventory manually, through the WSAPI, or through mobile device management.

  # **Monitored Computers**: The number of Monitored computers your license entitles you to manage. **Monitored Computers** are servers that 1) meet the requirements for Managed Computers and 2) have Monitoring enabled.

  # **Chromebooks & Network Devices**: **Endpoints** that count toward your license limit include devices that 1) have been added to the inventory but do not meet the definition of Managed Computers or Monitored Computers and 2) were not added to inventory manually, through the WSAPI, or through

mobile management. Examples of Assets include printers, projectors, network gear, and storage devices. The endpoints you create and manage using the Asset Management component do not count toward the license limit.

- Your product license agreement entitles you to manage a specified number of devices. Be aware that devices count toward these limits even if devices are MIA (missing in action) or no longer in use. However, devices that are added to inventory manually, or through the API, do not count toward license limits. For more information, see http://quest.com/docs/Product_Guide.pdf. To increase your license capacity, go to the Quest website: https://quest.com/buy.
- If the license count is within the threshold of 25 units from limit, a warning alert appears in the user notification list. When the server license count reaches the limit, an error alert is displayed. Also, when the license limit is reached and an agent attempts to add a new device, an error alert appears. For more details about user notifications, see Managing user notifications.

Remote Control Computers: The number of remote control endpoints your license entitles you to manage.

License terms and conditions.

Third-party code attributions.

Optional: View appliance license information with enabled components. See View product licensing information.

View product licensing information

The appliance license information appears in the *Appliance Updates* section of the **Administrator Console**.

1. Go to the appliance *Control Panel*:
   - **If the Organization component is not enabled on the appliance, log in to the appliance Administrator Console, `https://appliance_hostname/admin`, then select Settings > Control Panel.**
   - **If the Organization component is enabled on the appliance, log in to the appliance System Administration Console, `https://appliance_hostname/system`, or select System in the drop-down list in the top-right corner of the page, then select Settings > Control Panel.**
2. Click **Appliance Updates**.
3. In the *License Information* section, click the **Help** button:

   The following information appears:

   # **Managed Computers**: The number of Managed Computers your license entitles you to manage. **Managed Computers** are devices in the inventory that 1) have Windows, Mac, Linux, or UNIX operating systems, 2) are categorized as PCs or servers, and 3) were not added to inventory manually, through the WSAPI, or through mobile device management.

   # **Monitored Computers**: The number of Monitored computers your license entitles you to manage. **Monitored Computers** are servers that 1) meet the requirements for Managed Computers and 2) have Monitoring enabled.

   # **Chromebooks & Network Devices**: **Endpoints** that count toward your license limit include devices that 1) have been added to the inventory but do not meet the definition of Managed Computers or Monitored Computers and 2) were not added to inventory manually, through the WSAPI, or through mobile management. Examples of Assets include printers, projectors, network gear, and storage devices. The endpoints you create and manage using the Asset Management component do not count toward the license limit.

      # Your product license agreement entitles you to manage a specified number of devices. Be aware that devices count toward these limits even if devices are MIA (missing in action) or no longer in use. However, devices that are added to inventory manually, or through the API, do not count toward license limits. For more information, see http://quest.com/docs/Product_Guide.pdf. To increase your license capacity, go to the Quest website: https://quest.com/buy.

      # If the license count is within the threshold of 25 units from limit, a warning alert appears in the user notification list. When the server license count reaches the limit, an error alert is displayed. Also, when the

license limit is reached and an agent attempts to add a new device, an error alert appears. For more details about user notifications, see Managing user notifications.

Co-Managed : The licenses are provisioned through KACE Cloud. The SMA defers licensing responsibility to KACE Cloud and only displays the number of licenses it has deferred. The number shown in SMA is a basic count, and not a reflection of total usage or license availability.

Remote Control Computers: The number of remote control endpoints your license entitles you to manage.

Expires: The license expiration date, in `month/day/year` format.

> **NOTE:** When the appliance maintenance expires, some features such as patching support become unavailable. This causes an error alert to appear on the Home Dashboard. To renew your license, visit https://support.quest.com/contact-us/renewals. For more information about the Dashboard, see Using the Home component.

Components: The components enabled under your license.

Optional: View the product serial number, model number, license terms and conditions, and third-party code attributions. See View the appliance version, model, and license information.

About appliance software updates

The appliance checks with the servers at Quest daily for software updates. These updates are referred to as advertised updates.

If updates are available, an alert appears on the *Home* page of the **Administrator Console** the next time you log in with Administrator account privileges.

Related topics

Upload an update file to the appliance manually.

About labels

Labels are containers that enable you to organize and categorize items, such as devices, so that you can manage them as a group.

For example, you can use labels to identify devices that have the same operating system or that are in the same geographic location. You can then initiate actions, such as distributing software or deploying patches, on all of the devices with that label. Labels can either be manually assigned to specific items or automatically assigned to items when they are associated with criteria, such as SQL or LDAP queries.

You can add labels from the *Labels* section as well as from other sections of the **Administrator Console** where labels are used, such as the *Devices* page.

The following labels are available:

- **Labels**: Labels that are applied manually and used to organize users, devices, software, Managed Installations, and more. See Managing manual labels.
- **Smart Labels**: Labels that are applied and removed automatically based on criteria you specify. For example, to track laptops in a specific office, you could use a label called “San Francisco Office,” and add a Smart Label based on the IP address range or subnet for devices located in the San Francisco office. Whenever a device that falls within the IP address range is inventoried, the Smart Label “San Francisco” is automatically applied. When the device leaves the IP address range, and is inventoried again, the label is automatically removed. See Managing Smart Labels.
- **LDAP Labels**: Labels that are applied to and removed from users and devices automatically based on LDAP or Active Directory® queries. See Managing LDAP Labels.

Related topics

Managing Smart Labels

Searching for information and filtering lists

You can search the appliance databases, and filter list pages, to find information on the appliance.

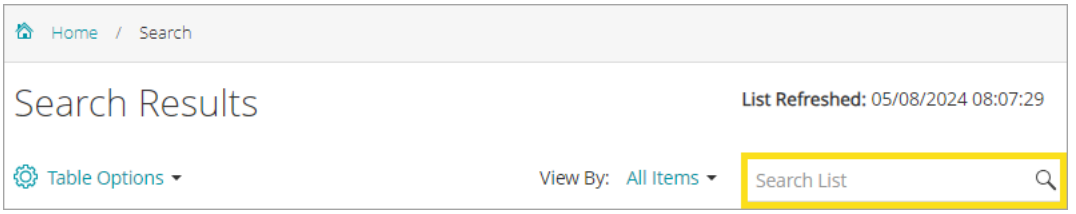
If the Organization component is enabled on your appliance, you can search the database of each organization separately. You cannot search the databases of all organizations at once, and you cannot search at the System level.

Search at the Admin level

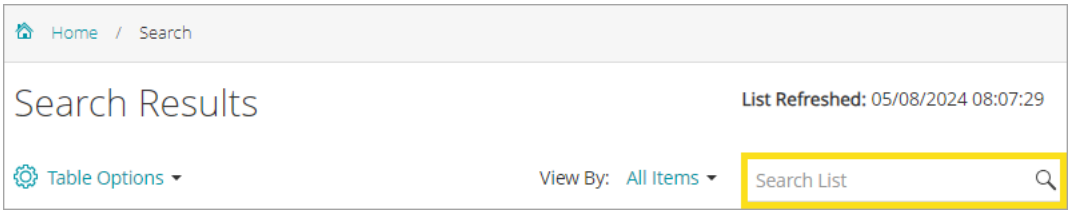
You can search the Admin-level databases to find information on the appliance.

If the Organization component is enabled on your appliance, you can search the database of each organization separately. You cannot search the databases of all organizations at once, and you cannot search at the System level.

1. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
2. Do one of the following:
   - **Click the *Search* button in the top-right corner of the page to display the *Search* field. Then type at least four characters in the *Global Search* field and press Enter or Return. The following illustration shows this *Search* field:**



   - **Click Home > Search. Then type at least four characters in the *Search* field that appears above the list on the right, and press Enter or Return. The following illustration shows this *Search* field:**



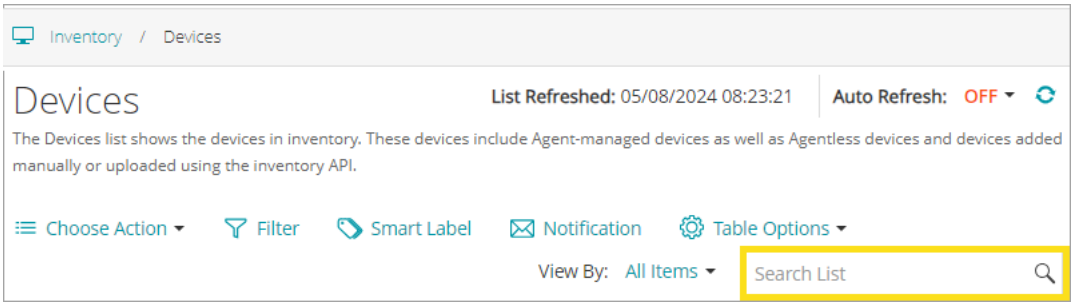
TIP: Use the percent sign (%) as a wildcard. For example, you can use the percent sign in a search string to find all items that match the criteria before and after the percent sign.

Search at the page level

Page-level Search enables you to search for information on the current page.

1. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
2. Go to a list page. For example, on the left navigation bar, click **Inventory**. The *Devices* page appears.
3. On the list page, *Devices* in this example, enter the search text into the **Search** field in the top-right corner of the page. Press **Enter** or **Return** to begin the page level search.

The following illustration shows the *Page-level Search* field:



TIP: Use the percent sign (%) as a wildcard. For example, you can use the percent sign in a search string to find all items that match the criteria before and after the percent sign.

Searching at the page level with advanced options

Advanced page-level Search enables you to search for information on the current page using various combinations of criteria. Advanced page-level Search is available on most list pages, such as the *Devices* page and the *Software* page.

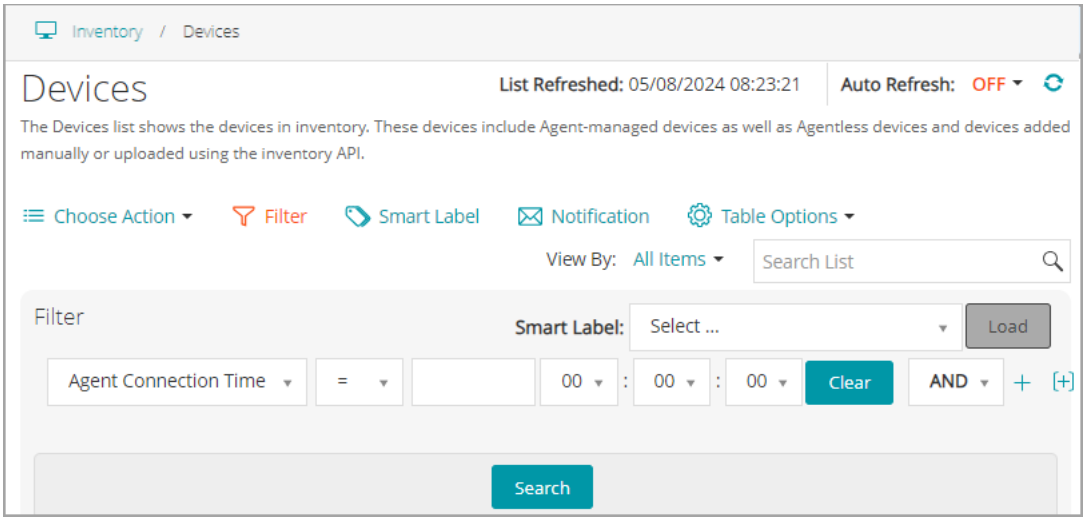
Example: Search for managed devices using Filter criteria

This example shows how to use Advanced page-level Search to find Windows devices that are running low on disk space.

When a scoped user performs an advanced search on devices, and their user role is associated with a Smart Label, the results only include the devices that are associated with the Smart Label. To see additional devices, you can change the scope of Smart Label, as needed. For more information on how to configure a device scope for a user role, see Add or edit User Roles. For details about Smart Labels, see Managing Smart Labels.

1. Go to the *Devices* list:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Inventory**, then click **Device**s.
2. Click the **Filter** tab above the *Devices* list on the right.

    The *Filter* panel appears.



3. Specify the criteria required to find Windows devices:

```
Operating System: Name | contains | Windows
```

4. With **AND** selected in the operator drop-down list, click **Add Line** to add a new line, then specify the criteria required to find devices that are low on disk space:

```
Drive Information: Disk % Capacity | > | 95
```

5. Click **Search**.

The list is refreshed to show devices that match the specified criteria.

Add Smart Labels and Notifications using Advanced Search criteria

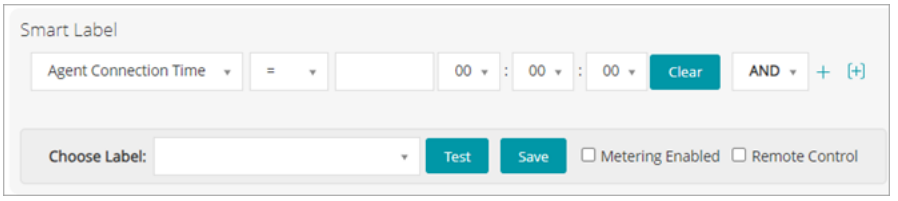
You can add Smart Labels and notifications using criteria in the *Advanced Search* panel.

1. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
2. Go to a list page. For example, on the left navigation bar, click **Inventory** to display the *Devices* page.
3. Click the *Filter* tab above the list on the right and enter the search criteria.

   See Example: Search for managed devices using Filter criteria.

4. Click the **Smart Label** tab above the list on the right.

   The *Smart Label* panel appears, and the selected search criteria remain available.



5. In the *Choose label* drop-down list, do one of the following:

   - **Select an existing label to associate with the Smart Label. Type in the *Choose label* field to search for existing labels.**

     NOTE: If you select a label group instead of a label, you will not be able to apply the Smart Label to a patching schedule. Patching schedules can only use Smart Labels based on a single item.

   - **Enter a new name for the Smart Label in the *Choose label* field, then press Enter or Return.**

   NOTE: Press **Enter** or **Return** after you enter a new Smart Label name to move the text from the search field to the label field.

6. Click **Create**.

   Smart Labels are applied as follows:

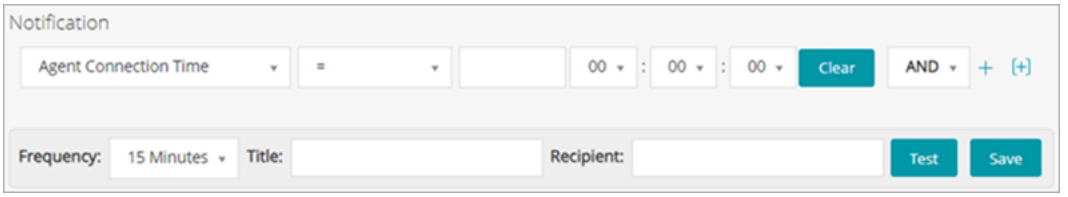
   # Smart Labels are automatically applied to or removed from devices when devices check in to the appliance, based on whether the devices meet the specified criteria.

   # If a specific application Smart Label is edited using **Home** > **Labels** > **Smart Labels**, it is applied to or removed from all applications immediately.

   # Smart Labels are automatically applied to or removed from applications when the items are updated on the *Inventory* > *Software* page, based on whether the items meet the specified criteria.

7. Click the **Notification** tab above the list on the right.

   The *Notification* panel appears, and the selected search criteria remain available.



8. Provide the following information:

Field	Description
Title	The information that you want to appear in the *Subject* line of the email.
Recipient	The email address or addresses of intended recipients. Email addresses must be fully qualified email addresses. To send email to multiple addresses, use commas to separate each address, or use email distribution lists.
Frequency	The interval at which the appliance runs the query to compare the selected criteria with items in inventory. If criteria are met, the notification is sent.

9. **Optional**: To verify the criteria, click **Test Notification**.

   The list is refreshed to show items that match the specified criteria. No email notifications are sent during the test.

10. Click **Create Notification**.

The notification is added and it appears on the *Email Alerts* page.

For information about scheduling the frequency of the notification, see Edit notification schedules.

Related topics

Example: Search for managed devices using Filter criteria

Load Smart Labels from the Filter tab

You can load Smart Labels from list pages on which the *Filter* tab is available.

1. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
2. Go to a list page. For example, click **Inventory** to display the *Devices* list.
3. Click the Filter tab above the list on the right to display the *Filter* panel.
4. At the top of the *Filter* panel, in the *Smart Label* drop-down list, select the Smart Label you want to load.

   The drop-down list shows Smart Labels that match the list page you are viewing. For example, on the *Devices* page, the drop-down list shows Device Smart Labels. In addition, labels are displayed only if the underlying SQL has not been edited outside of the Smart Label wizard. This is because the wizard cannot be used to display custom SQL.

5. Click **Load**.

The criteria of the selected Smart Label appears in the *Filter* panel.

Create Custom Views using Filter criteria

You can create Custom Views using Filter criteria. Custom Views display list items using predefined Filter criteria. Custom Views are available on list pages such as the *Software Catalog* page, the *Assets* page, and the Service Desk *Tickets* page.

Custom Views are user-specific. Users cannot access the Custom Views that are created by other users.

1. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
2. Go to a page that has the Custom View option, such as the *Software Catalog* page or the *Assets* page.
3. Click the **Filter** tab on the top-right corner of the page and enter the search criteria.
4. Click the **Custom View** tab on the top-right corner of the page to display the *Custom View* panel.
5. Select Custom View criteria. For example, to create a view on the *Software Catalog* page that displays all Windows devices that have metered applications in the category of Infrastructure Applications, do the following:
    a. Specify the criteria required to find applications categorized as Infrastructure Applications:

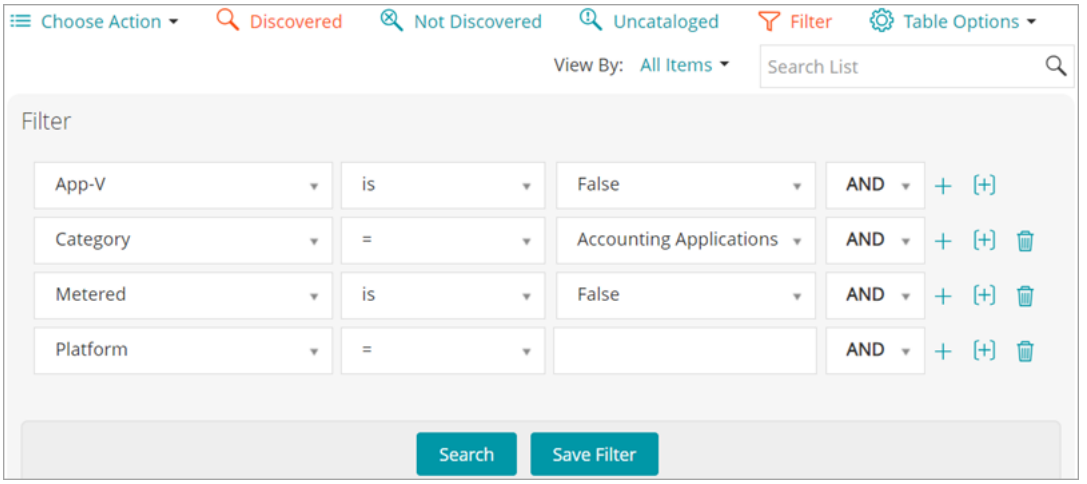
    `Category | = | Infrastructure Applications`

    b. With **AND** selected in the operator drop-down list, click **Add Line** to add a new line.
    c. Specify the criteria required to find applications that are metered:

    `Metered | is | True`

    d. With **AND** selected in the operator drop-down list, click **Add Line** to add a new line.
    e. Specify the criteria required to find Windows devices:

    `Platform | = | Windows`



6. **Optional**: Click **Test** to refresh the list to show items that match the specified criteria.
7. In the *View Name* field, type a name for the Custom View, then click **Create**.

The Custom View appears in the *View By* drop-down list.

Related topics

Example: Search for managed devices using Filter criteria

Access product documentation

The **Administrator Console** provides access to help contents and documentation search. It also allows you to browse related Knowledge Base articles, and to chat with product specialists, when needed.

1. Log in to the User Console, Administrator Console, or System Console.
2. In the upper right of the Administrator Console, click **Help**.

A help pane appears on the right containing high-level information about the related Administrator Console page. The bottom of the help pane includes the following buttons:

- **Appliance Administrator Guide**(): Provides access to the KACE System Management Appliance help contents.
- **Knowledge Base** (): Allows you to browse the Knowledge Base articles associated with the related **Administrator Console** page.

  NOTE: This option is only available in the **Administrator Console** and the System Console. It does not appear in the **User Console**.
- **Video Tutorials** (): Allows you to browse one or more training videos associated with the related **Administrator Console** page. You can play a video on the help pane, in a smaller window outside of the selected page, or on the target Knowledge Base page that hosts the video.

  NOTE: This option is only available if related videos exist on the Support Portal. Also, it only appears in the **Administrator Console** and the System Console. It does not appear in the **User Console**.
- **Chat** (): Starts a chat with a KACE System Management Appliance product specialist.

  NOTE: This option is only available in the **Administrator Console** and the System Console. It does not appear in the **User Console**.
- **Open Ticket** (): Links to the Support page (https://support.quest.com/create-service-request) that allows you to create a service request.

  NOTE: This option is only available in the **Administrator Console** and the System Console. It does not appear in the **User Console**.
- **Support** (): Links to the **Settings > Support** page. This page provides resources for troubleshooting system management issues and contacting **Quest Support**.

  NOTE: This option is only available in the **Administrator Console** and the System Console. It does not appear in the **User Console**.
- **Mobile App** (): Displays a dialog containing links for downloading the KACE GO Mobile App. The app is available for iOS and Android platforms.

  NOTE: This option is available if the appliance is configured to interact with the K1 GO Mobile App. It only appears in the **Administrator Console** and the System Console. It does not appear in the **User Console** For more information on enabling mobile access, see Configuring Mobile Device Access.
- **About** (): Displays information about your KACE System Management Appliance installation.

  NOTE: This option is only available in the **Administrator Console** and the System Console. It does not appear in the **User Console**.

3. Click a link in the page-level Help topic.

   The main Help system appears, displaying the selected topic.
4. Click the **Search** tab in the left pane of the Help system.

All search terms use an implicit Boolean AND statement. For example, if you search for Windows provisioning, Search displays results that contain both words.

TIP: For a PDF version of the Help system, click the Acrobat button on the right side of the main Help system navigation bar ( ).

5. **Administrator or System Console only**. Search for Knowledge Base articles associated with the related Administrator Console or the System Console page.
    a. At the bottom of the help pane, click .

        The help pane displays a list of related Knowledge Base articles.

    NOTE: Knowledge Base articles are currently only available in English.

    b. Use the navigation buttons to look for a specific article.
    c. Search the listed articles for a specific keyword, as needed.
    d. When you find a desired article, click the link in the help pane.

        The selected Knowledge Base article appears on a new tab in your browser.

    IMPORTANT: To see the article contents, you must log in to the Quest Support site using your Quest user name and password.

6. **Administrator or System Console only**. Search for Knowledge Base articles associated with the related Administrator Console or the System Console page.
    a. At the bottom of the help pane, click .

        The help pane displays a list of related training videos.

    NOTE: To access the videos, you must log in to the Quest Support site using your Quest user name and password. Training videos are currently only available in English.

    b. Use the navigation buttons to look for a specific video, as applicable.
    c. To play a video, click the Play Video button.

        The selected video starts playing on the help pane.

    d. Continue to play a video on the help pane, or use a different display option, such as *Picture-In-Picture*, *Fullscreen*, or *Popout player*, to display it outside of the selected page. These controls are located at the bottom of the video.

7. **Administrator or System Console only**. Chat with a product specialist.
    a. Click .

        The *Chat with Support* dialog box appears.

    b. Type your *Full Name*, *Email Address*, and *Purpose of your Chat*, as applicable, and click **Start Chat**.

        The *Chat with Support* dialog box refreshes, showing a list of existing Knowledge Base (KB) articles that may contain information about the specified topic. The list of topics may appear on multiple pages, depending on the type of the requested information.

    c. Review the list of KB articles. Use the page navigation controls at the bottom of the list, if applicable. To read a KB article, click the title in the list.
    d. If none of the listed KB articles provide the information you need, click **None of the solutions above solved my issue, continue with chat**.

    NOTE: You can only use this feature when product specialists are available to respond to your questions. If Live Chat is not available, this is indicated in the dialog box.

        The *LIVE CHAT* dialog box appears. The *Full Name*, *Email Address*, and *Purpose of your Chat* boxes are populated using the information specified in the *Chat with Support* dialog box.

    e. Click **Start Chat**.

        The *LIVE CHAT* dialog box refreshes.

f. In the *LIVE CHAT* dialog box, type your question, and click **SEND** to start chatting with a product specialist.

8. **Administrator or System Console only**. Open a Support ticket.
   a. Click .

      Your browser displays the *Submit a Service Request* page (https://support.quest.com/create-service-request) in a new tab or window.

   b. Use this page to open a service ticket, as required.
9. **Administrator or System Console only**. Click .

   The Settings > Support page appears. This page provides resources for troubleshooting system management issues and contacting Quest Support.
10. **Administrator or System Console only, when mobile access is enabled on the appliance.**

    NOTE: For more information on enabling mobile access, see Configuring Mobile Device Access.

    a. Click .

       A dialog box appears, allowing you to download KACE GO. The app is available for iOS and Android platforms from their respective app stores.

    b. Click the link for your mobile device OS, as needed, to download the app.

       For more information about downloading and configuring KACE GO, seeDownload and use KACE GO.
11. **Administrator or System Console only**. Review information about your KACE System Management Appliance installation.
    a. Click .

       A dialog box displaying product information appears.

    b. To close it, click **Close**.
12. To close the help pane, click **Need Help**.

Log in to the Administrator Console: First login following initial network configuration

After the network settings are configured and the appliance restarts, you can log in to the appliance **Administrator Console** from any computer on the LAN (local area network).

During the first login following initial network configuration, you must provide your appliance license key and set the password for the **admin** account.

NOTE: Your browser setting determines the language displayed in the **Administrator Console** the first time you log in. To change this setting after you log in, see Configuring locale settings.

1. Open a web browser and enter the Administrator Console URL:

   `http://`appliance_hostname`/admin`. For example, `http://kace_sma/admin`.
2. Provide the following information:

Option	Description
License Key	Enter the license key you received in the **Welcome** email from Quest. Include the dashes. If you do not have a license key, contact **Quest Support** at https://support.quest.com/contact-support.

Option	Description
Password	Enter a password for the default **admin** account, which is the account you use to log in to the appliance **Administrator Console**. The default **admin** account is the only account on the appliance at this time. If you forget the password for this account, the system might have to be reset to factory defaults which can result in loss of data. **NOTE:** If you have multiple types of KACE appliances, Quest recommends that you use the same password for the **admin** account on all appliances. Using a common password enables you to link the appliances later.
Company Name	Enter the name of your company or group.
Timezone	Select the timezone where the appliance is located.

3. Click **Apply Settings and Reboot**.

   The appliance restarts.
4. When the appliance has restarted, refresh the browser page.
5. Accept the End User License Agreement (EULA), then log in using the login ID `admin` and the password you chose on the initial setup page.
6. Select or clear the check boxes next to the notification fields to enable or disable email notifications for the administrator account. You can change these settings later as needed. See Manage appliance administrator email notifications.

Option	Description
Enable Quest Security Notifications	Enable Quest to send security notifications to the email address of this administrator. This feature is available only to System-level administrator accounts. It is not available to Admin-level administrator accounts, or non-administrator user accounts.
Enable Quest Sales and Marketing Notifications	Enable Quest to send sales and marketing notifications to the email address of this administrator. This feature is available only to System-level administrator accounts; it is not available to Admin-level administrator accounts, or non-administrator user accounts.

The **Administrator Console** appears and the appliance is ready for use.

Getting started

To use the appliance, you need to configure appliance settings to match your network configuration.

In addition, you can set up Labels, User Authentication, Replication Shares, Credentials Management, Assets, License Compliance, and Service Desk features to meet the needs of your environment. If the Organization component is enabled on your appliance, you can add or edit organizations and organization settings as needed.

Configuring the appliance

Appliance configuration consists of setting up network, security, locale, and other settings on the appliance.

Requirements and specifications

Appliance technical specifications describe appliance capacity and requirements for managing devices.

For the latest information about appliance hardware, requirements for managed devices, and browser requirements for accessing the **Administrator Console**, see the *Technical Specifications* available on the product documentation page: https://support.quest.com/kace-systems-management-appliance/technical-documents.

Power-on the appliance and log in to the Administrator Console

When the appliance is powered on for the first time, you can log in to the appliance **Administrator Console** from any computer on your LAN, provided that a DHCP server is available to assign an IP address to the appliance. This enables you to use the setup wizard to configure initial network settings.

- If you have the virtual version of the virtual appliance, download the appliance software and set up the virtualization infrastructure. For more information, see the setup guide for the virtual appliance. Go to https://support.quest.com/kace-systems-management-appliance/release-notes-guides.
- If you are installing the physical version of the appliance, review and follow the safety instructions in the **Dell PowerEdge R430 Getting Started With Your System** document and any other safety instructions shipped with the appliance. The Quest appliance is a specially configured platform and does not require you to install or remove internal components, update firmware, or modify BIOS settings. To set up the appliance, follow the instructions in this document only.
- In the A record of your internal DNS (domain name system) server, enter the appliance's hostname. The A record defines the hostname for the MX record, and this enables users to send email tickets to the Service Desk. By default, the appliance's host name is `k1000`, but you can change it during initial setup.
- Decide whether to use a split DNS. Using a split DNS is useful if the appliance connects to the internet using a reverse proxy, or if you place the appliance in a perimeter network or screened subnet. A DMZ adds an additional layer of security to a LAN (local area network).
- (Optional) Obtain a static IP address for the appliance.

If a DHCP server is not available, you can configure network settings using the **Command Line Console**. See Access the Command Line Console.

NOTE: For information about logging in to KACE as a Service, see the **KACE as a Service Setup Guide**. Go to https://support.quest.com/kace-systems-management-appliance/release-notes-guides.

1. If you are configuring the virtual version of the appliance, power on the virtual machine to boot the appliance.

   This first-time startup takes 5 to 10 minutes.

   The Command Line Console login screen appears showing the appliance's DHCP network settings.
2. On any computer connected to your LAN, open a browser and go to the URL shown on the Command Line Console login screen. For example, `http://kace_sma.local/admin`.

   The *Software Transaction Agreement* **page appears.**
3. Accept the agreement.

   The *Initial Setup* **wizard appears.**
4. Verify that you have the information required to configure the appliance, then click **Next**.
5. Review the information on the *Diagnostic Support Console* page that appears, and record the secret key and offline tokens in a secure place, as instructed.
6. On the *Licensing and Administrator Settings* page, provide the following information:

Option	Description
License Key	The license key you received in the **Welcome** email from Quest. Include the dashes. If you do not have a license key, contact **Quest Support** at https://support.quest.com/contact-support.
Company Name	The name of your company or group.
Administrator Email	The email address where you want to receive communications from Quest.
Password	The password for the default **admin** account, which is the account you use to log in to the appliance **Administrator Console**. The default **admin** account is the only account on the appliance at this time. If you forget the password for this account, the system might have to be reset to factory defaults, which can result in loss of data. **NOTE:** If you have multiple types of KACE appliances, Quest recommends that you use the same password for the **admin** account on all appliances. Using the same admin account password enables you to link the appliances later. See Linking Quest KACE appliances.
Two-Factor Authentication	If you want to provide stronger security for users logging into the appliance, set this to *Enabled*. This feature adds an extra step to the login process. It relies on the Google Authenticator app to generate verification codes. The app generates a new six-digit code at regular intervals. When enabled, end users will be prompted for the current verification code each time they log in.

Option	Description
	NOTE: If you enable this feature, ensure that appliance server's clock is accurate, as well as the device running Google Authenticator. Google Authenticator relies on current time to create the token. If server's clock is not synchronized with those of the devices running Google Authenticator, token validation may fail, which may result in account lockouts.

7. Follow the onscreen instructions to complete the initial setup.

   When the initial setup is complete, the appliance restarts and the Administrator Console login page appears.

   NOTE: If you changed the appliance IP address, go to the new address to display the login page.

8. Log in to the Administrator Console using the login ID admin and the password you chose during initial setup.

   If Two-Factor Authentication was enabled on the *Licensing and Administrator Settings* page, the *Configure Two-Factor Authentication* page appears.

9. **Two-Factor Authentication only**. Follow the instructions on the *Configure Two-Factor Authentication* page to generate a Google Authenticator verification code using your smart phone. In the *Verification Code* field, type the Google Authenticator code, and click **Finish Configuration**. A new verification code is required on each subsequent login.

   To skip this step, click Skip Configuration. You can only bypass this step during a configured transition window. For more information, see Configure security settings for the appliance.

The **Administrator Console** appears and the appliance is ready for use. Your browser setting determines locale formats used for date and time information displayed in the **Administrator Console** the first time you log in. For information about changing the language settings, see Configuring locale settings.

Access the Command Line Console

The **Command Line Console** is a terminal window interface to the appliance. You can use this interface to configure appliance settings, just as you would in the appliance **Administrator Console**. This is useful if a DHCP server is not available and you cannot log in to the **Administrator Console**.

The **Command Line Console** is not used with K1 as a Service.

1. If you have a virtual version of the appliance, power on the virtual machine to boot the appliance.

   The Command Line Console login screen appears.

2. At the prompts, enter:

   Login: **`konfig`**

   Password: `konfig`

3. Choose the language to use for the Command Line Console. Use the up- and down-arrow keys to move between fields.
4. Configure network settings. See Change appliance network settings.

   TIP: Use the right- and left-arrow keys to select options in a field; use the up- and down-arrow keys to move between fields.

5. Use the down-arrow key to move the cursor to *Save*, then press **Enter** or **Return**.

   The appliance restarts.

Tracking configuration changes

If History subscriptions are configured to retain information, you can view the details of the changes made to settings, assets, and objects.

This information includes the date the change was made and the user who made the change, which can be useful during troubleshooting.

Related topics

About history settings

Configuring System-level and Admin-level General Settings

If the Organization component is enabled on your appliance, General Settings are available at the System level and at the Admin level. If the Organization component is not enabled on your appliance, all General Settings are available at the Admin level.

If the Organization component is enabled on your appliance, see:

- Configure appliance General Settings with the Organization component enabled.
- Configure Admin-level or organization-specific General Settings.

If the Organization component is not enabled, see:

- Configure appliance General Settings without the Organization component.

Configure appliance General Settings with the Organization component enabled

If the Organization component is enabled on your appliance, configure appliance General Settings at the System level.

If the Organization component is not enabled on your appliance, see Configure appliance General Settings without the Organization component.

1. Go to the System-level *General Settings* page:
    a. Log in to the appliance System Administration Console, `http://`**appliance_hostname**`/system`, or select **System** from the drop-down list in the top-right corner of the page.
    b. On the left navigation bar, click **Settings**, then click **Control Panel**.
    c. On the *ControlPanel*, click **Customize General Configurations** link under the **General Settings** section, to display the *General Settings* page.
2. In the *General Settings* tab, provide the following information:

Option	Description
Company Name	Enter the name of your company.
Command Line Console Locale	Select the language to use in the **Command Line Console**, which uses the `konfig` user account.
Company Email Suffix	Enter the domain from which your users send email. For example: quest.com.

Option	Description
Appliance Administrator Email	Enter the email address of the appliance administrator. System-related messages, including critical alerts, are sent to this address.
Session Timeout	Set the number of inactive hours to allow before closing user sessions and requiring users to log in again. The default is 1. The **User Console** and **Administrator Console** have Timeout Session counters to alert users of this time limit. Only periods of inactivity are counted. The counter restarts when the user performs any action that causes the console to interact with the appliance server, such as refreshing a window, saving changes, and changing windows. When the counter reaches the limit, the user is logged out, unsaved changes are lost, and the login screen appears. The Timeout Session counter appears in the upper right of each console.
Require organization selection at login	Display the *Organization* drop-down list on the **Administrator Console** login page, `http://`**appliance_hostname**`/admin`, where **appliance_hostname** is the hostname of your appliance. This enables you to choose an organization when you log in. If this option is disabled, the *Organization* drop-down list is not displayed on the login page, and you can only log in to the Default organization from `http://`**appliance_hostname**`/admin`. If organization fast switching is enabled, however, you can switch between organizations after you log in to the Default organization.
Show organization menu in admin header	Display the *fast-switching* drop-down list in the top-right corner of the **Administrator Console** next to the login information. This drop-down list makes it possible to bypass the login page when you switch from one organization to another. To appear in the drop-down list, organizations must have the same **admin** account password; only those organizations whose **admin** account passwords match appear in the list. Changes to the drop-down list are displayed only after you log out and then log in again.

3. **Optional**. In the *Beta Notifications* section, indicate if you want to participate in the Beta program.

   Beta program participants receive notifications when a Beta version of the appliance becomes available. These notifications appear as alerts on the on the Home dashboard.

   These notifications may target specific configurations. Enabling them does not trigger automated upgrades to Beta versions, or automatically register this appliance for the Beta program. Beta enrollment is still required to participate, and details are provided in the notifications.

   For more information about the Home dashboard, see Using the Home component.

   a. Select **Enable beta notifications from KACE**.
   b. If you want these notifications to appear only in the System Administration Console, select **Restrict beta notifications to System UI**.

      Leaving this option cleared causes the Beta notifications to appear in both the Administrator Console and System Administration Console.

4. In the *Agent Tasks* section under the *Device Settings* tab , view or configure KACE Agent task throughput:

Option	Description
Last Task Throughput Update	This value indicates the date and time when the appliance task throughput was last updated.
Current CPU Load	The value in this field depicts the load on an appliance at any given point of time. For the appliance to run normally, the value in this field must be between 0.0 and 10.0.

Option	Description
Current CPU Maximum	The value in this field depicts the load on an appliance at any given point of time. For the appliance to run normally, the value in this field must be between 0.0 and 10.0.
Task Throughput	The value that controls how scheduled tasks, such as inventory collection, scripting, and patching updates, are balanced by the appliance. **NOTE:** This value can be increased only if the value in the Current CPU Load is not more than 10.0, and the Last Task Throughput Update time is more than 15 minutes.

5. In the *Duplicate Machine Detection Settings (Advanced)* section, configure the following options to prevent duplicate device records

When the appliance receives inventory from a device without an existing inventory record (which is determined by the use of a new/unknown KUID), it scans the device's properties that you select in this section to determine whether this is a new device or an existing one. If it determines that the device belongs to an existing inventory record, it merges the new device record with the existing one.

Option	Description
Required to match an existing machine record	Select one or more of the following check boxes to indicate which device properties you want the appliance to use to identify potentially duplicated devices. • **Machine Name** • **BIOS Serial Number** • **Manufacturer** • **Operating System Family**
MAC Addresses	Specify the number of MAC addresses that are associated with the machine record that you to match with the existing device records.

6. In the User Console section, modify the text as needed:

Option	Description
Title	The heading that appears on the **User Console** login page.
Welcome Message	A welcome note or description of the **User Console**. This text appears below the title on the **User Console** login page.

7. In the *Acceptable Use Policy* section, select policy settings:

Option	Description
Enabled	Enable the appliance to display your policy, and require users to accept the terms of your policy, when they access the **Administrator Console**, **User Console**, or **Command Line Console**, or log in using SSH or FTP.
Title	The heading of the policy to be displayed on the login page of the **User Console**.
Message	Details of the policy, which are displayed below the *Title* on the login page. Users must agree to the terms of the policy before they can log in to the **User Console**.

8. In the *Reporting User Account* tab, specify the password for the reporting system:

Option	Description
Reporting Username	(Read-only) The username used to generate reports. The report username provides access to the database (for additional reporting tools), but does not give write access to anyone.
Reporting Password	The report user password. This password is used only by the reporting system and MySQL™.

9. In the *Data Retention* tab, select the number of days to retain log information. Log entries that are older than the selected number of days are automatically deleted from the log. See View appliance logs.
10. In the *User Notification Retention* section, select the number of days to retain user notification. Any user notifications that are older than the selected number of days are automatically deleted from the Notifications pane. See Configure user notifications.
11. In the *Share with Us* tab, select data sharing options:

    To validate the your product license, Quest collects minimal license-related information, such as the MAC Address of the appliance, the version of the appliance software, the license key, and the number of managed devices, regardless of the data sharing options selected in this section.

Option	Description
Share summary usage data...	(Recommended) Share summary information with Quest. This information includes appliance status, uptime, and load averages, as well as the number of devices, Managed Installations, and applications being managed by the appliance. This option is recommended because it provides additional information to **Quest Support** if you need assistance. In addition, data shared with Quest is used when planning product enhancements.
Share detailed usage data...	(Recommended) Share detailed information with Quest. This information includes Agent and appliance crash reports, user interface usage statistics, and inventory information, such as application titles. Quest uses this information to help improve the Software Catalog for dynamic feeds to the appliance **Administrator Console**. To enable the feed, you need to select **Share detailed Usage data...**. This setting shares information about usage data and crash reports. The feed is available only if **Share Summary Usage Data...** is selected, and it is available only on pages related to software or deployment, such as the software, Managed Installation, and File Synchronization detail pages. The feed is not available on the *Software Catalog* detail page. Clear this option to prevent the appliance from sharing inventory data. However, clearing this option does not remove any information that has already been shared. For more information, contact **Quest Support**.
Share extended patch diagnostics	(Recommended) Share detailed patch diagnostics with Quest.

12. To use custom Administrator Console, User Console, or report logos and background colors, in the *Login Screen Options* sections, provide the following information.

Option	Description
System Console Login Background Color **Admin Console Login Background Color**	You can access the appliance from the following levels: • **Administrator Console** shows organization-related features. • **System Administration Console** provides access to appliance-related features. • **User Console** makes applications available to users on a self-service basis. It also enables users to file Service Desk support tickets to request help or report issues. To

Option	Description
User Console Login Background Color	access the **User Console**, go to `http://<appliance_hostname>/user` where `<appliance_hostname>` is the host name of your appliance. For each of these web-based interfaces you can specify a different background color of the login screen. Any colors specified on the organization level override system-level settings. Click and use the color chooser to specify the color that you want to appear in the background of the login screen. You can select the color using the mouse, or specify the RGB values, as needed. When you close the color chooser, the *HTML Color Code* field on the right displays the HTML code of the selected color. To undo your selection, click **Reset** and start over. **NOTE:** The color chooser is not supported in Internet Explorer 11.
System Console Logo **Admin Console Logo** **User Console Logo** **Report Logo**	In each applicable section, click **Choose File**, and specify the graphic file that you want to use as the custom logo in the available web interfaces and in system-generated reports. The supported graphic file formats are `.bmp`, `.gif`, `.jpg`, and `.png`. Any logos configured on the organization level override system-level settings. To see default logos and sample customized versions, refer to the following illustrations.

Figure 1. Default User Console logo

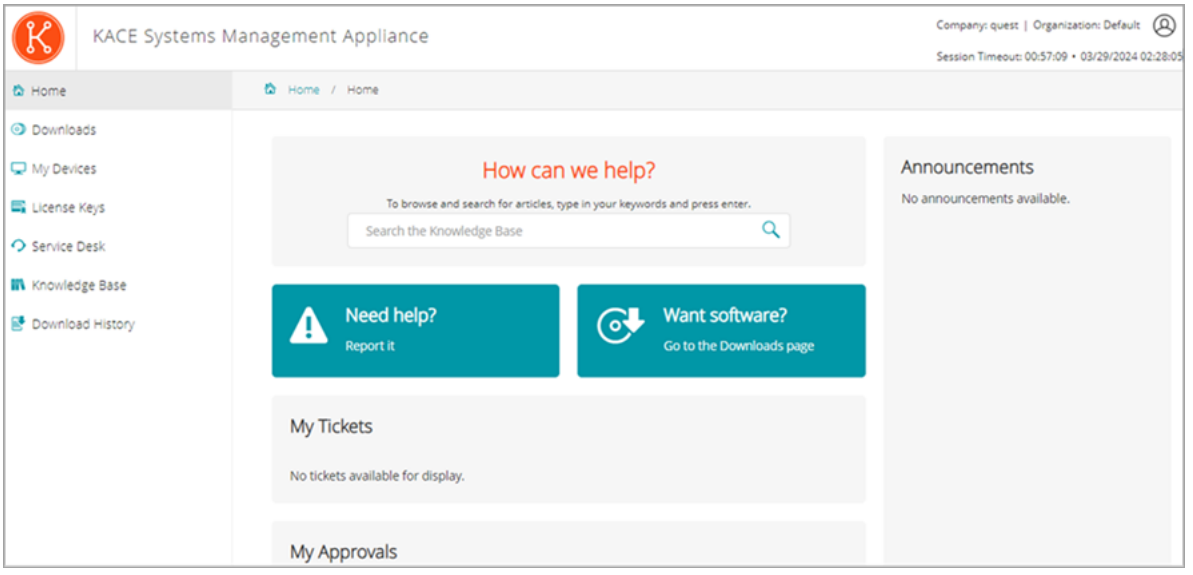


Figure 2. Custom User Console logo

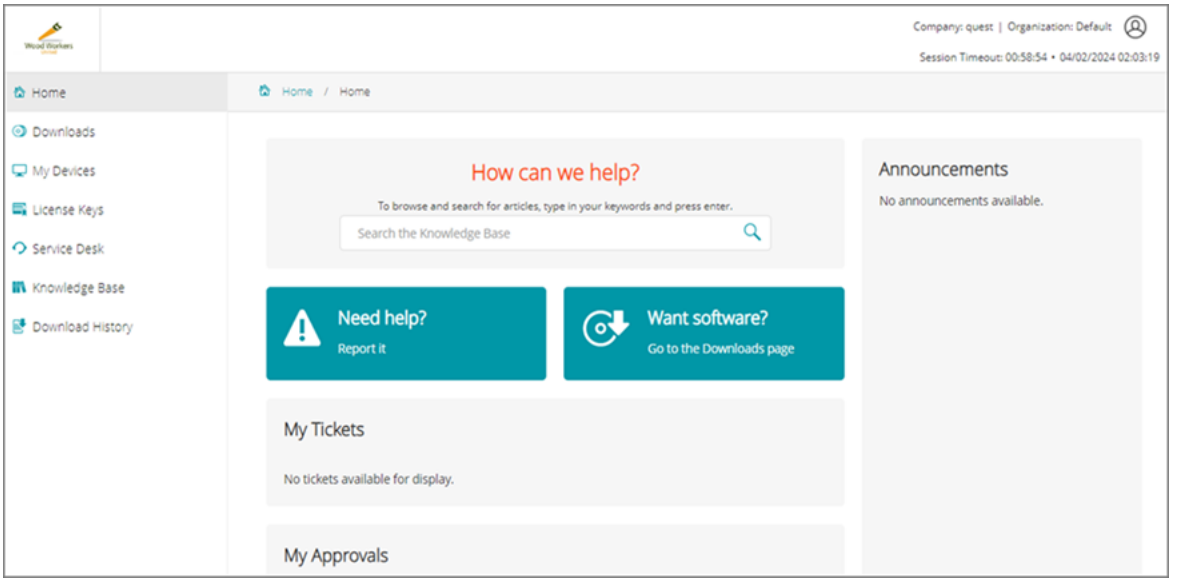


Figure 3. Default report logo

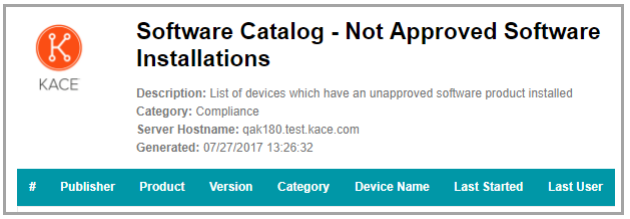
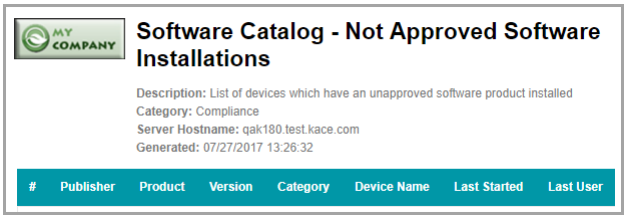


Figure 4. Custom report logo



13. If you manage Lenovo devices, you can retrieve their warranty information. To do that, in the *Manufacturer Warranty API Keys* section, provide the Lenovo API keys to obtain the warranty data. Lenovo requires only a key. These values are stored encrypted in the database.

IMPORTANT: To obtain warranty information, you must configure the manufacturer's warranty API keys. For complete instructions, visit https://go.kace.com/to/k1000-help-warranty.

When configured, the device warranty information appears on the *Device Details* page in the *Inventory Information* group when you select an Lenovo device. For more information, see Groups and sections of items in device details.

Option	Description
Lenovo	Select this option if you want to obtain warranty information for your managed Lenovo devices. If this option is selected and you clear it, the Lenovo key is removed from the database.

Option	Description
Key	The API key for obtaining warranty information for managed Lenovo devices.

14. Click **Save and Restart Services**.

Related topics

Configuring locale settings

Creating and managing organizations

Configure Admin-level or organization-specific General Settings

If the Organization component is enabled on your appliance, configure organization-specific General Settings at the Admin level. You configure the General Settings for each organization separately.

See Adding, editing, and deleting organizations.

If the Organization component is not enabled on your appliance, see Configure appliance General Settings without the Organization component.

1. Go to the Admin-level *General Settings* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click *Settings*. On the *Control Panel*, under the **General Settings** section, click **Customize General Configurations** link to display the *General Settings* page.
2. In the *General Options* section, view or enter the following information.

Option	Description
Last Updated and **Organization Name**	(Read-only) The date the information was changed and the name of the organization. *Organization Name* can be edited at the System level. See Add or edit organizations.
Company Name	Enter the name of your company.
Administrator Email	Enter the email address of the appliance administrator. System-related messages, including critical alerts, are sent to this address.
Company Email Suffix	Enter the domain from which your users send email. For example: example.com.

3. Optional: In the *Locale Settings* section, specify locale settings. See Configuring locale settings.

Option	Description
Organization Locale	Select the locale to use for the selected organization's **Administrator Console** and **User Console**. If you have multiple organizations, you can select different locales for each one. See: • Adding, editing, and deleting organizations • Configuring locale settings

4. Optional: In the *Samba Share Settings* section, select file sharing options then click **Save Samba Settings**. If File Shares are disabled, you need to enable them at the System level before you can enable them for the organization. See Configure security settings for the appliance.

Option	Description
Enable File Sharing	Use the appliance's client share to store files, such as files used to install applications on managed devices. The appliance's client share is a built-in Windows file server that can be used by the provisioning service to assist in distributing the Samba client on your network. Quest recommends that this file server only be enabled when you perform application installations on managed devices.
File Share User 'admin' Password	Enter the password to use for admin account access to the file share directory.

5. In the *Ignore Client IP Address Settings* section, enter the IP address or addresses to ignore. Separate each address with a comma. Ignoring IP addresses is useful when multiple devices could report themselves with the same IP address, such as a proxy address.
6. In the *License Usage Warning Configurations* section, select the percentage to use for the warning threshold and critical threshold for software license usage. If you have configured software License assets, threshold information is displayed on the license-related widgets on the *Dashboard*
7. In the *Data Retention and Archival* section, select the options for retaining data in the appliance database.

Option	Description
Device Uptime Data	The number of months that device uptime information is retained in the appliance database. Device uptime refers to the number of hours of each day that managed devices are running. You can retain this data for a specified number of months, **Forever**, or never save it (**Disabled**).
Metering Data	The number of months that metering data is retained in the appliance database. Metering data is information about how applications are installed and used on the Windows and Mac devices that you manage. Metering data that is older than the selected number of months is deleted on the first day of every month. See About metering information.
Retain Uncataloged data in the Software Catalog	Whether to retain information about Uncataloged applications in the appliance database. Uncataloged applications are executables that are in the appliance inventory but that do not appear in the Software Catalog, and the appliance retains information about those applications by default. For organizations with a large number of managed devices, however, retaining this data might greatly increase the size of the database. This size increase could increase the time it takes to load pages in the **Administrator Console** and the time it takes to perform database backups. Select this check box to retain data for Uncataloged software in the appliance database. Clear the check box to disable data retention. If data retention for Uncataloged software is disabled: • Agents on managed devices continue to upload full inventory information, and raw data related to applications is fingerprinted. If data sharing is enabled, data is

Option	Description
	also uploaded to the Quest KACE Software Catalog. See Configure data sharing preferences. • The appliance continues to store information related to Cataloged applications and Locally Cataloged applications in the organization database. • Information related to Uncataloged applications is not stored in the organization database, and the Uncataloged applications list in the **Administrator Console** is empty. • Reports for Cataloged applications continue to work as expected. However, reports related to Uncataloged applications show only those applications that are part of Cataloged software titles.
Microsoft Defender Threat Data	The number of months that Microsoft Defender threat data is retained in the appliance database.
User Session Data	You can retain retain the User Sessions records for specified period. Select the desired period from the drop-down list.
Asset Archive Pending Threshold	Type the select the number of days that you want to keep the assets marked for archiving, before actually archiving them. The default value is 3 days.
Enable User Archival	Enables user archival and allows for the control over how users are archived. indicate if you want to enable user archival, as needed.

8. In the *Enable User Archival* , indicate if you want to enable user archival, as needed.
   a. To have the ability to archive user accounts, select the **Enable User Archival** check box.

   NOTE: When user archival is enabled, user accounts can only be deleted only if they are marked as archived.

   b. In the *Archive Tag* field, type a label that you want to associate with the state of archived users. For example, `Archived` or `Inactive`.
   c. Indicate if you want to maintain Service Desk ticket and asset associations with archived users. Set each of the *Ticket Associations* and *Asset Associations* fields to one of the following options:

   # **Maintain Users**: Select this option if you want to continue to associate tickets or assets with archived users. If you select this option, the configured *Archive Tag* appears next to the archived user name, to indicate that the user is no longer active.

   # **Remove Users**: Select this option if you want to remove all ticket or asset associations with archived users.

For more information on how to archive user accounts, see Archive user accounts.

9. In the *Device Assignment* section, indicate how you want to match users with devices: **One-time sync**, **Continuous sync**, or **Disabled**.
10. In the *Device Actions* section, click **Add New Action**, the select the scripted actions to enable.

    Device Actions are scripted actions that can be performed on managed devices. There are several pre-programmed actions available. To add your own action, select **Custom Action** in the *Action* menu, then enter the command in the *Command Line* text box.

    The following variables are available for device actions:

    KACE_HOST_IP

    KACE_HOST_NAME

KACE_CUSTOM_INVENTORY_*

When device actions run, the appliance replaces variables with their appropriate values.

For KACE_CUSTOM_INVENTORY_ * replace the asterisk (*) with the name of a software application associated with a custom inventory rule. When the device action runs, the name is replaced with the custom inventory rule value for the device. Enter the software application name in uppercase characters. The allowed characters are: [A-Z0-9.-]."

NOTE: Most actions in the *Action* drop-down list require you to install additional applications for them to function. For example, using DameWare requires you to install TightVNC on your device as well as on the device you want to access.

This feature is only supported on Windows devices. The Windows device you are running the device action from must have the KACE Agent version 9.0 or later agent installed and connected.

When you initiate device through the agent, the action executable must be placed in your `%PATH%`. The agent is 32-bit, so on 64-bit Windows devices, use `%windir%/System32` as an alias to the `%windir%/Wow64` directory. If you need to run a program that's located in the `%windir%/System32` directory on a 64-bit Windows system, you must use the `%windir%/SysNative` virtual directory. You can either add `%windir%/SysNative` to your `%PATH%` environment variable or provide a fully-qualified path by prepending `%windir%/SysNative` to your executable when defining your machine action.

11. In the *Patch Schedule* section, if you want disable administrators to apply patches to all devices, select the **Hide All Devices** check box.

    NOTE: You can only apply this setting if you do not have any patch schedules set up to run against all devices. Otherwise, a warning appears.

12. In the *Allowed Bulk Actions* section, indicate if you want to enable bulk actions against KACE Cloud Mobile Device Manager (MDM) and VMware virtual machine devices. When bulk actions are enabled, the associated KACE Cloud MDM and VMware virtual machine commands become available from the **Choose Action** menu on the *Devices* list page.

Option	Description
Enable Bulk KACE Cloud MDM Actions	Select this check box to enable commands against multiple KACE Cloud MDM devices on the *Devices* list page.
Enable Bulk Virtual Machine Actions	Select this check box to enable commands against multiple VMware or Hyper-V virtual machine devices on the *Devices* list page.
Enable Bulk Chrome OS Actions	Select this check box to enable commands against multiple Chrome OS devices on the *Devices* list page.
Enable Bulk Restart Device Command	Select this check box to enable the restart command against multiple devices on the *Devices* list page.
Enable Bulk Microsoft Defender Actions	Select this check box to enable Microsoft Defender commands against multiple devices on the *Devices* list page.

13. To use custom Administrator Console, User Console, report, and KACE Agent alert logos and background colors, in the *Login Screen Options* sections, provide the following information.

Option	Description
Admin Console Login Background Color **User Console Login Background Color**	You can access the appliance from the following levels: • **Administrator Console** shows organization-related features. • **System Administration Console** provides access to appliance-related features. • **User Console** makes applications available to users on a self-service basis. It also enables users to file Service Desk support tickets to request help or report issues. To access the **User Console**, go to `http://<appliance_hostname>/user` where `<appliance_hostname>` is the host name of your appliance. When you select an organization in the **Administrator Console**, you can specify a different background color of the **Administrator Console** and **User Console** login screens. Any colors specified on the organization level override system-level settings. For information on how to configure system-level settings, see Configure appliance General Settings with the Organization component enabled. Click and use the color chooser to specify the color that you want to appear in the background of the login screen. You can select the color using the mouse, or specify the RGB values, as needed. When you close the color chooser, the *HTML Color Code* field on the right displays the HTML code of the selected color. To undo your selection, click **Reset** and start over. **NOTE:** The color chooser is not supported in Internet Explorer 11.
Admin Console Logo **User Console Logo** **Report Logo** **Agent Alert Logo**	In each applicable section, click **Choose File**, and specify the graphic file that you want to use as the custom logo in the **Administrator Console**, **User Console**, system-generated reports, and in KACE Agent alert that appear on managed devices. The supported graphic file formats are `.bmp`, `.gif`, `.jpg`, and `.png` with the exception of KACE Agent alerts that only support `.bmp` files. Any logos configured on the organization level override system-level settings. To see default KACE Agent alerts and sample customized versions, refer to the following illustrations. For examples of default and custom logos in the **Administrator Console**, **User Console**, and system-level reports, see Configure appliance General Settings with the Organization component enabled.

Figure 5. Default Alert logo

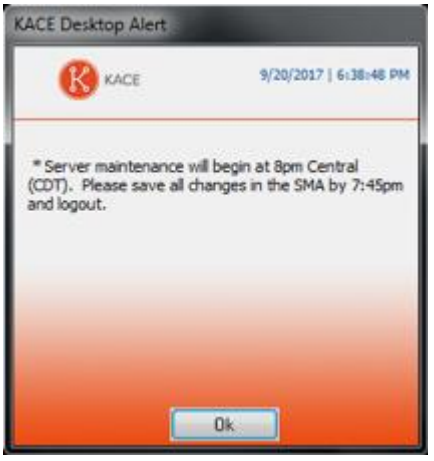
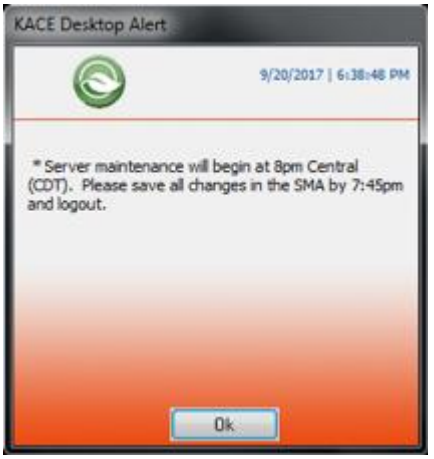


Figure 6. Custom Alert logo



14. Click **Save and Restart Services**.
15. If you have multiple organizations, repeat the preceding steps for each organization.

Configure appliance General Settings without the Organization component

If the Organization component is not enabled on your appliance, all appliance General Settings are available at the Admin level.

If the Organization component is enabled on your appliance, see Configure Admin-level or organization-specific General Settings.

1. Go to the Admin-level *General Settings* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`.
    b. On the left navigation bar, click *Settings*, then click *ControlPanel*.
    c. On the *ControlPanel*, click **Customize General Configurations** link under the **General Settings** section to display the *General Settings* page.
2. In the *General Options* section, provide the following information:

Option	Description
Last updated	Read-only: The date the information was changed and the name of the organization.
Company Name	Enter the name of your company.
Administrator Email	Enter the email address of the appliance administrator. System-related messages, including critical alerts, are sent to this address.
Company Email Suffix	Enter the domain from which your users send email. For example: example.com.
Session Timeout	Set the number of inactive hours to allow before closing user sessions and requiring users to log in again. The default is 1. The **User Console** and **Administrator Console** have Timeout Session counters to alert users of this time limit. Only periods of inactivity are counted. The counter restarts when the user performs any action that causes the console to interact with the appliance server, such as refreshing a window, saving changes, and changing windows. When the counter reaches the limit, the user

Option	Description
	is logged out, unsaved changes are lost, and the login screen appears. The Timeout Session counter appears in the upper right of each console.

3. In the *Client Drop File Size Filter* section, specify a file size.

Options	Description
Client Drop File Size Filter	A file-size filter for the organization's Client Drop location. The Client Drop location is a storage area (Samba share) for the organization on the appliance. This storage area is used to upload large files, such as application installers and appliance backup files, to the appliance. Uploading files to the Client Drop location is an alternative to uploading files through the **Administrator Console** using the default HTTP mechanism, which can result in browser timeouts for large files. The *Client Drop Size* filter determines whether files uploaded to the organization's Client Drop location are displayed on the *Upload and Associate Client Drop File* list on the *Software Detail* page. For example, if the Client Drop Size filter is set to 1 GB, the *Upload and Associate Client Drop File* list shows files that are 1 GB in size or larger. Files that are less than 1 GB in size are not displayed on the list. Application files are moved from the organization's Client Drop location to the appropriate area when the file is selected on the *Software Detail* page and saved. Appliance backup files that are placed in the Client Drop location are automatically identified as appliance backup files, and they become available for selection on the *Backup Settings* page within five minutes. See Copy files to the appliance Client Drop location.

4. In the User Console section, specify customizations for the User Console text:

Option	Description
Title	The heading that appears on the **User Console** login page. The **User Console** is the web-based interface that makes applications available to users on a self-service basis. It also enables users to file Service Desk support tickets to request help or report issues. To access the **User Console**, go to `http://<appliance_hostname>/user` where `<appliance_hostname>` is the hostname of your appliance.
Welcome Message	A welcome note or description of the **User Console**. This text appears below the title on the **User Console** login page.

5. In the *Acceptable Use Policy* section, select policy settings:

Option	Description
Enabled	Enable the appliance to display your policy, and require users to accept the terms of your policy, when they access the **Administrator Console**, **User Console**, or **Command Line Console**, or log in using SSH or FTP.
Title	The heading of the policy to be displayed on the login page of the **User Console**.

Option	Description
Message	Details of the policy, which are displayed below the *Title* on the login page. Users must agree to the terms of the policy before they can log in to the **User Console**.

6. In the *Log Retention* section, select the number of days to retain log information. Log entries that are older than the selected number of days are automatically deleted from the log. See Access appliance logs to view Microsoft Exchange Server errors.
7. In the *User Notification Retention* section, select the number of days to retain user notification. Any user notifications that are older than the selected number of days are automatically deleted from the Notifications pane. See Configure user notifications.
8. In the *Share With Us* section, specify data sharing options.

NOTE: To validate your product license, Quest collects minimal license-related information, such as the MAC Address of the appliance, the version of the appliance software, the license key, and the number of managed devices, regardless of the data sharing options selected in this section.

Option	Description
Share summary usage data...	(Recommended) Share summary information with Quest. This information includes appliance status, uptime, and load averages, as well as the number of devices, Managed Installations, and applications being managed by the appliance. This option is recommended because it provides additional information to **Quest Support** if you need assistance. In addition, data shared with Quest is used when planning product enhancements.
Share detailed usage data...	(Recommended) Share detailed information with Quest. This information includes Agent and appliance crash reports, user interface usage statistics, and inventory information, such as application titles. Quest uses this information to help improve the Software Catalog for dynamic feeds to the appliance **Administrator Console**. To enable the feed, you need to select **Share detailed Usage data...**. This setting shares information and it is available only on pages related to software deployment, such as the software, Managed Installation, and File Synchronization detail pages. The feed is not available on the *Software Catalog* detail page. Clear this option to prevent the appliance from sharing inventory data. However, clearing this option does not remove any information that has already been shared. For more information, contact **Quest Support**.
Share extended patch diagnostics	(Recommended) Share detailed patch diagnostics with Quest.

9. In the *Locale Settings* section, specify locale preferences. These preferences determine the formats used for date and time information displayed in the Administrator Console.

Option	Description
Organization Locale	The locale to use for the organization's **Administrator Console** and **User Console**.

Option	Description
Command Line Console Locale	The locale to use in the **Command Line Console**, which uses the `konfig` user account.

10. In the *Ignore Client IP Address Settings* section, enter the IP address or addresses to ignore. Separate each address with a comma. Ignoring IP addresses is useful when multiple devices could report themselves with the same IP address, such as a proxy address.
11. In the *License Usage Warning Configurations* section, select the percentage to use for the warning threshold and critical threshold for software license usage. If you have configured software License assets, threshold information is displayed on the license-related widgets on the *Dashboard*.
12. In the *Update Reporting User Password* section, provide the password of the account required to run reports on the organization. You cannot change the *Database Name* or the *Report Username*.
13. In the *Data Retention and Archival* tab, select the options for retaining data on the appliance. You can retain this data for a specified number of months, **Forever**, or never save it (**Disabled**).

Option	Description
Device Uptime Data	The amount of uptime data to save for devices. Device uptime data refers to the number of hours of each day that your managed devices are running. You can retain this data for a specified number of months, **Forever**, or never save it (**Disabled**).
Metering Data	The number of months that metering data is retained in the appliance database. Metering data is information about how applications are installed and used on the Windows and Mac devices that you manage. Metering data that is older than the selected number of months is deleted on the first day of every month. See About metering information.
Retain Uncataloged data in the Software Catalog	Whether or not to retain information about Uncataloged applications in the appliance database. Uncataloged applications are executables that are in the appliance inventory but that do not appear in the Software Catalog, and the appliance retains information about those applications by default. For organizations with a large number of managed devices, however, retaining this data might greatly increase the size of the database. This could increase the time it takes to load pages in the **Administrator Console** and the time it takes to perform database backups. Select this check box to retain data for Uncataloged software in the appliance database. Clear the check box to disable data retention. If data retention for Uncataloged software is disabled: • Agents on managed devices continue to upload full inventory information, and raw data related to applications is fingerprinted. If data sharing is enabled, data is also uploaded to the Quest KACE Software Catalog. See Configure data sharing preferences. • The appliance continues to store information related to Cataloged applications and Locally Cataloged applications in the organization database. • Information related to Uncataloged applications is not stored in the organization database, and the Uncataloged applications list in the **Administrator Console** is empty. • Reports for Cataloged applications continue to work as expected. However, reports related to Uncataloged applications show only those applications that are part of Cataloged software titles.

Option	Description
User Data Session	You can retain retain the User Sessions records for specified period. Select the desired period from the drop-down list.

14. In the *Device Actions* section, click **Add New Action**, the select the scripted actions to enable.

    Device Actions are scripted actions that can be performed on managed devices. There are several pre-programmed actions available. To add your own action, select **Custom Action** in the *Action* menu, then enter the command in the *Command Line* text box.

    The following variables are available for device actions:

    KACE_HOST_IP

    KACE_HOST_NAME

    KACE_CUSTOM_INVENTORY_*

    When device actions run, the appliance replaces variables with their appropriate values.

    For KACE_CUSTOM_INVENTORY_ * replace the asterisk (*) with the name of a software application associated with a custom inventory rule. When the device action runs, the name is replaced with the custom inventory rule value for the device. Enter the software application name in uppercase characters. The allowed characters are: [A-Z0-9.-]."

    NOTE: Most actions in the *Action* drop-down list require you to install additional applications for them to function. For example, using DameWare requires you to install TightVNC on your device as well as on the device you want to access.

    This feature is only supported on Windows devices. The Windows device you are running the device action from must have the KACE Agent version 9.0 or later agent installed and connected.

    When you initiate device through the agent, the action executable must be placed in your `%PATH%`. The agent is 32-bit, so on 64-bit Windows devices, use `%windir%/System32` as an alias to the `%windir%/Wow64` directory. If you need to run a program that's located in the `%windir%/System32` directory on a 64-bit Windows system, you must use the `%windir%/SysNative` virtual directory. You can either add `%windir%/SysNative` to your `%PATH%` environment variable or provide a fully-qualified path by prepending `%windir%/SysNative` to your executable when defining your machine action.

15. To use custom Administrator Console, User Console, report, and KACE Agent alert logos and background colors, in the *Login Screen Options* sections, provide the following information.

Option	Description
Admin Console Login Background Color **User Console Login Background Color**	You can access the appliance from the following levels: • **Administrator Console** shows organization-related features. • **System Administration Console** provides access to appliance-related features. • **User Console** makes applications available to users on a self-service basis. It also enables users to file Service Desk support tickets to request help or report issues. To access the **User Console**, go to `http://<appliance_hostname>/user` where `<appliance_hostname>` is the host name of your appliance. When you select an organization in the **Administrator Console**, you can specify a different background color of the **Administrator Console** and **User Console** login screens. Any colors specified on the organization level override system-level settings. For information on how to configure system-level settings, see Configure appliance General Settings with the Organization component enabled. Click and use the color chooser to specify the color that you want to appear in the background of the login screen. You can select the color using the mouse, or specify the RGB values, as needed. When you close the color chooser, the *HTML Color*

Option	Description
	Code field on the right displays the HTML code of the selected color. To undo your selection, click **Reset** and start over. **NOTE:** The color chooser is not supported in Internet Explorer 11.
Admin Console Logo **User Console Logo** **Report Logo** **Agent Alert Logo**	In each applicable section, click **Choose File**, and specify the graphic file that you want to use as the custom logo in the **Administrator Console**, **User Console**, system-generated reports, and in KACE Agent alert that appear on managed devices. The supported graphic file formats are `.bmp`, `.gif`, `.jpg`, and `.png` with the exception of KACE Agent alerts that only support `.bmp` files. Any logos configured on the organization level override system-level settings. To see default KACE Agent alerts and sample customized versions, refer to the following illustrations. For examples of default and custom logos in the **Administrator Console**, **User Console**, and system-level reports, see Configure appliance General Settings with the Organization component enabled.

Figure 7. Default Alert logo

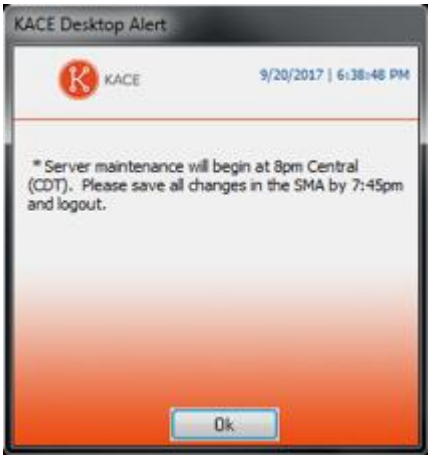
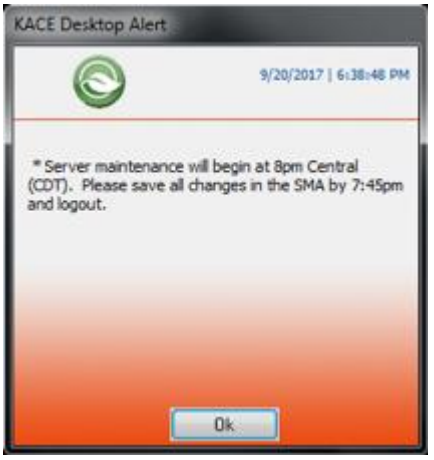


Figure 8. Custom Alert logo



16. If you manage Lenovo devices, you can retrieve their warranty information. To do that, in the *Manufacturer Warranty API Keys* section, provide the Lenovo API keys to obtain the warranty data. Lenovo requires only a key. These values are stored encrypted in the database.

IMPORTANT: To obtain warranty information, you must configure the manufacturer's warranty API keys. For complete instructions, visit https://go.kace.com/to/k1000-help-warranty.

When configured, the device warranty information appears on the *Device Details* page in the *Inventory Information* group when you select an Lenovo device. For more information, see Groups and sections of items in device details.

Option	Description
Lenovo	Select this option if you want to obtain warranty information for your managed Lenovo devices. If this option is selected and you clear it, the Lenovo key is removed from the database.
Key	The API key for obtaining warranty information for managed Lenovo devices.

17. Click **Save and Restart Services**.

    The appliance restarts.

Configure appliance date and time settings

Configure appliance date and time settings in the Settings section of the **Administrator Console**. If the Organization component is enabled on your appliance, date and time settings are available at the System level.

It is important to keep the appliance date and time settings accurate, because many calculations are based on these settings.

1. Go to the appliance *Control Panel*:
   - **If the Organization component is not enabled on the appliance, log in to the appliance Administrator Console, `https://appliance_hostname/admin`, then select Settings > Control Panel.**
   - **If the Organization component is enabled on the appliance, log in to the appliance System Administration Console, `https://appliance_hostname/system`, or select System in the drop-down list in the top-right corner of the page, then select Settings > Control Panel.**
2. Click any of the following in the **Date and Time Settings** section:
   # Set appliance timezone
   # Enable Network Time Protocol
   # Manually set appliance clock

   The *Date and Time Settings* page appears.
3. Specify the following settings:

Option	Description
Timezone	Select a timezone in the drop-down list.
Time Setting	Select an option: • **Configure Network Time Protocol**. Use an Internet time server. If you select this option, provide the server web address in the *Server* field. • **Manually configure date and time**. Set the appliance clock manually. Specify the time and date in the drop-down lists. The *Hour* drop-down list uses a 24-hour clock format.

Option	Description
Server	Use an Internet time server to set the appliance time. Enter the web address of the time server in the text box. For example: time.example.com.

4. Click **Save and Reboot**.

   The web server restarts and the settings are applied.

   NOTE: During the restart, active connections might be dropped. When changes are saved, the page automatically refreshes after 15 seconds. After the appliance web server restarts, the updated date and time appear in the bottom right of the **Administrator Console**.

Managing user notifications

User notifications on the appliance alert you about specific events that require your attention.

These alerts appear on the Notification pane, accessible by clicking the bell icon in the top-right corner of the screen. Administrators can review or edit notification configurations, as needed.

Review user notification alerts

The appliance displays user notification alerts in the Administrator Console when it encounters certain predefined conditions.

The list of triggered user notifications can be accessed using the bell icon, located in the top-right corner of the screen. Use this icon to show or hide the Notification pane, as needed. An orange indicator appears on the bell icon when new notifications are reported. After reviewing all new notifications, the indicator disappears.

Each notification alert that appears in the list is triggered by the related notification configuration. For more details, see Configure user notifications.

The background color of an alert indicates the alert severity: info (blue), warning (yellow), warning (red). This is also determined in the notification configuration.

Notification items always include a time stamp, indicating when the alert occurred. They remain on the list for a configured amount of time, even if the appliance re-boots. You can edit the notification retention period on the *General Settings* page, as applicable. For more details, see Configure appliance General Settings with the Organization component enabled.

Some notifications include links that you can use to drill down to the object associated with the notification. For example, if you see a license expiration notice, the link in the notification takes you directly to the license instance that is about to expire.

If a notification applies to more than one item, such devices or licenses, in most cases multiple notification alerts appear, one for each applicable item. When the appliance runs a patch schedule against one or more devices, patch completion messages appear in the notification panel when ten percent of each target device is completed, for the first ten devices. For more information about patch schedules, see Configure patch schedules.

Also, when a notification configuration is associated with one or more users, the resulting notification alerts are displayed only to those users in the **Administrator Console**. When notification configurations are not linked to any users this way, all users with administrative permissions logged into the **Administrator Console** can see the related notifications. This mechanism does not apply to the **System Administration Console** which always shows all notifications to all users.

You can sort and view the notifications based on defined Categories and Types. You can apply filters by Category, Type, or both simultaneously to narrow down the notifications list.

You can delete individual notifications by clicking the Delete icon in the top-right corner of each entry in the list. To clear the list of notifications, click **Dismiss All**.

1. Do one of the following:

   - **Log in to the appliance Administrator Console, `https://appliance_hostname/admin`. Or, if *Show organization menu in admin header* is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.**
   - **Log in to the appliance System Administration Console, `https://appliance_hostname/system`, or select System from the drop-down list in the top-right corner of the page.**

   The *Dashboard* or *System Dashboard* page appears.
2. In the top-right corner of the screen, click the bell icon to display the My Notification pane.
3. Review the list of notifications.
4. **Optional**. You can delete individual notifications, or all of them, as applicable.

   # To delete a notification, click the Delete icon in the top-right corner of the notification based on defined **Categories** and **Types**.

   # To delete all notifications, and clear the entire list, in the top-right corner of the My Notification pane, click **Dismiss All**.
5. **Optional**. You can filter the notifications.

   # To filter notifications, click the bell icon in the top-right corner. The list of different **Categories** and **Types** are displayed.

   # To refine the filter, select options from the various **Category** and **Types**.

Configure user notifications

A wide range of predefined notification configurations come included with the appliance.

Administrators can review these configurations on the *User Notifications* page. Additional details about each configuration are displayed on the *User Notification Detail* page after selecting it in the list. Some configurations allow you to enable or disable them, while other settings are read-only.

You can use one or more labels to associate a notification configuration with specific users. This causes the resulting notification alerts to be displayed in the **Administrator Console** only to the users specified by those labels . If a notification configuration is not linked to any users this way, all users with administrative-level permissions can see the related notification alerts in the **Administrator Console**, when they are triggered. These settings do not apply to the **System Administration Console**, that always shows all notifications to all users.

1. Go to the *User Notifications* list page:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Settings**, then click **User Notifications**.
2. On the *User Notifications* page, review the list of notifications.

   For each item, the list displays its name, description, whether the notification is enabled, category, and any labels associated with it. There are several available categories, each focusing on a specific aspect of your environment. You can, for example, sort the list by category, and review all notifications in a specific segment, such as *Security* or *Patching*.
3. To review or edit a specific notification configuration:
   a. Click the name of a user notification.
   b. Observe the contents of the *User Notification Detail* page.

The *Name*, *Description*, and *Category* settings are read-only. Some notification configurations allow you to enable or disable them using the Enabled check box. If this box appears greyed out, the notification configuration is always enabled.

c. Review the *Restrict to Labels* area, and edit the collection of labels, as needed.

When you add labels to a notification configuration, only the users specified by those labels can see the resulting notification alerts as they are being triggered. If a notification configuration does not point to any specific users using this method, its notifications can be displayed to all users with the administrative-level permissions in the Administrator Console. The System Administration Console, however, shows all notifications to all logged-in users regardless of these settings.

To view, add or edit labels associated with the notification configuration:

1. Click **Restrict to Labels**.
2. In the *Select Labels* dialog box that appears, review or edit the list of labels that you want to associate with the user notification. You can add multiple labels to each notification configuration.
3. When done, click **OK** to return to the *User Notification Detail* page.

d. On the *User Notification Detail* page, click **Save**.

Enable Two-Factor Authentication for all users

Two-Factor Authentication (2FA) provides stronger security for users logging into the appliance by adding an extra step to the login process. It relies on the Google Authenticator app to generate verification codes. The app generates a new six-digit code at regular intervals. When enabled, end users will be prompted for the current verification code each time they log in.

To download the Google Authenticator app, visit one of the following sites, as applicable:

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

You can enable 2FA access to the **Administrator Console** and **User Console** for all users in the selected organization using the *Two-Factor Authentication* page in the **Administrator Console**, as described below. Alternatively, you can enable or disable 2FA access to the **Administrator Console** and **User Console** using the **System Administration Console**. For more information, see Configure Two-Factor Authentication for organizations.

1. Go to the Admin-level *Two-Factor Authentication* page:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Settings**, then click **Control Panel** and in the **Security Settings** section click **Enable 2FA**.
2. To enable 2FA for all users in the Administrator Console, under *Enable Two-Factor Authentication for Admin Portal*, select **Required for all Users**.

This option overwrites 2FA settings in the *User Details* page. When 2FA is enabled for all users on this page, it cannot be disabled for individual users on the *User Details* page for any users that are associated with the selected organization (if applicable).

3. To enable 2FA for all users in the User Console, under *Two-Factor Authentication for User Portal*, select **Required for all Users**.

Verifying port settings, NTP service, and website access

Port settings, NTP service, and website access must be configured correctly to enable features such as Agent communications, Software Catalog updates, and patch downloads.

Verify port settings

Appliance ports must be configured correctly to enable device management and database or file access.

- Ensure that the appropriate appliance ports are not blocked by firewall settings:

Port	Use	Direction
20 and 21	(Optional and not recommended) Used to access backup files on the appliance through FTP from outside the firewall.	Inbound to the appliance
22	(Recommended) Used to create an SSH tunnel to quest.com.	Outbound from the appliance
25	(Optional) Used by the appliance SMTP server for email (non-SSL). This is required only if you configure SMTP email. See Configuring SMTP email servers.	Outbound from the appliance
80	(Required unless SSL is enabled) Used for standard HTTP (web) access to the **Administrator Console** and **User Console**.	Inbound to the appliance
110	(Optional) Used for POP3 email (non-SSL)	Inbound to the appliance
161	(Optional) Used for SNMP monitoring. See Discovering devices on your network.	Outbound from the appliance
199	(Optional) Used for unidirectional (read-only) SNMP access to managed devices on the network through SMUX, an SNMP multiplexing protocol. See Configure security settings for the appliance	Outbound from the appliance
443	(Required) Used for SSL access and agent messaging protocol communications. Devices use this port when they check in to the appliance using HTTPS.	Inbound to the appliance

Port	Use	Direction
	The appliance listens on this port for communications from devices on which the KACE Agent is installed.	
587	(Optional) Used by the appliance SMTP server for secure email (SSL enabled). This is required only if you configure secure SMTP email. See Configuring SMTP email servers.	Outbound from the appliance
995	(Optional) Used for POP3 email (SSL enabled).	Inbound to the appliance
3306	(Optional) Used to access the appliance database with external tools. For example, this port is used to run reports on the appliance database using Microsoft Access® or Excel®.	Inbound to the appliance

- Ensure that the appropriate device ports are accessible to the appliance:

Port	Use
7	(Optional) Used by the appliance for UDP traffic on the network, which is used for Wake-on-LAN. See Using Wake-on-LAN.
139	(Optional) Used during KACE Agent provisioning on Windows devices.
161	(Optional) Used for SNMP monitoring. This port should be open and bound to SNMP. See Discovering devices on your network.
445	(Optional) Used during KACE Agent provisioning. See Provisioning the KACE Agent.

- To use an LDAP server for authentication, ensure that the appropriate ports are accessible from the appliance:

Port	Use
389	(Optional) Used for LDAP access.
636	(Optional) Used for secure LDAP access.

Verifying the status of the NTP service

When downloading patches using HTTPS, the NTP (Network Time Protocol) service must be running on the appliance. The NTP service is required because the secure protocol uses the current date stamps from the appliance to ensure certificate validity.

If the NTP service is not running, patch download failures, suggesting invalid certificates, might result.

Make necessary websites accessible to the appliance

To complete patch downloads, access product information, and interact with **Quest Support**, firewall, DNS server, and proxy server settings must allow the appliance to access domains on both port 80 and port 443.

- Ensure that the appliance Administrator Console has links to the following websites:

Website	Description
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
https://st-rmm-kace.api.splashtop.com	Splashtop®

Configuring network and security settings

Appliance network settings include the hostname, web server name, IP address, and other information required to access the appliance over the network.

Change appliance network settings

You can change the appliance network settings to meet the needs of your environment any time after the initial configuration.

For virtual versions of the appliance, network settings are initially configured during the first login to the Administrator Console or the Command Line Console. See Change appliance network settings.

For K1 as a Service, the appliance is preconfigured with a static IP address, subnet mask, and default gateway. For configuration information, see the **KACE as a Service Setup Guide**. Go to https://support.quest.com/k1000-as-a-service/release-notes-guides.

Changing the majority of appliance network settings requires that you reboot the appliance. Total reboot downtime is one to two minutes, provided that the changes result in a valid configuration.

TIP: Testing an external SMTP server does not require the appliance reboot. You can test the SMTP configuration before saving your changes.

1. Go to the appliance *Control Panel*:
   - **If the Organization component is not enabled on the appliance, log in to the appliance Administrator Console, `https://appliance_hostname/admin`, then select Settings > Control Panel.**
   - **If the Organization component is enabled on the appliance, log in to the appliance System Administration Console, `https://appliance_hostname/system`, or select System in the drop-down list in the top-right corner of the page, then select Settings > Control Panel.**
2. Under the **Network Settings** section, click **Configure DNS to display the General** tab on the *Network Settings* page.
3. On the *Network Settings* page, in the *Geneal* section, provide the following information:

Option	Description
DNS Hostname	Enter the hostname of the appliance. The default is k1000.
Web Server Name	Enter the fully-qualified domain name of the appliance. This is the **Hostname** concatenated with **Domain**. For example: k1000.example.com. Devices connect to the appliance using this name. Quest recommends that you add a static IP address entry for the appliance to your DNS server. If you use an SSL certificate, the hostname must be fully qualified and it must match the name on the certificate.
Automatically generate server name	Select this check box to enable the system to generate the appliance web server name using this format: `Hostname.Domain`. For example: `k1000.example.com`. Clear this check box to enter a custom web server name.

4. In the *IPv4 Configuration* tab, provide the following information:

Option	Description
Configure Network Using DHCP	Select this option if you want to use DHCP (Dynamic Host Configuration Protocol) to automatically obtain the IPv4 address and other network configuration information for the appliance.
Configure Network Manually	Select this option if you want to manually specify the IPv4 address, domain, subnet mask, default gateway, and DNS settings for the appliance: • **IP Address**: Enter the static IP address of the appliance. **CAUTION: If the IP address is incorrect, you cannot access the appliance through the web interfaces (Administrator Console and User Console). If this happens, open the appliance Command Line Console, and use the `konfig` login to enter the correct IP address.** • **Domain**: Enter the domain that the appliance is on. For example, `example.com`. • **Subnet Mask**: Enter the subnet (network segment) that the appliance is on. The default is `255.255.255.0`. • **Default Gateway**: Enter the network gateway for the appliance. • **Primary DNS**: Enter the IP address of the primary DNS server the appliance uses to resolve host names. • **Secondary DNS**: (Optional) Enter the IP address of the secondary DNS server the appliance uses to resolve host names.

5. In the *IPv6 Configuration* tab, provide the following information:

Option	Description
Configure Network Using SLAAC	Select this option if you want to use the SLAAC (stateless address auto-configuration), offered by IPv6, to configure the appliance's network settings. SLAAC allows devices to select their own IPv6 addresses based on the prefix that is advertised from their connected interface.
Configure Network Manually	Select this option if you want to manually specify the IPv6 address, prefix length, and default gateway for the appliance: • **IPv6 Address**: Enter the static IPv6 address of the appliance. **CAUTION: If the IP address is incorrect, you cannot access the appliance through the web interfaces (Administrator Console and User Console). If this happens, open the appliance Command Line Console, and use the `konfig` login to enter the correct IP address.** • **Prefix Length**: Enter the number of bits in the IPv6 address prefix. An IPv6 prefix typically consists of 64 bits. • **Default Gateway**: Enter the network gateway for the appliance.
Disable IPv6	Select this option if you want to disable an IPv6 address for the appliance. This is the default setting.

6. **Optional**: To set a proxy server, select the **Enable Proxy Server** in the *Proxy Configuration* tab, then specify proxy server settings:

Option	Description
Type	Enter the proxy type, either HTTP or SOCKS5.
Server	Enter the name of the proxy server.
Port	Enter the port for the proxy server. The default port is 8080.
Enable Basic Proxy Authentication	Select the check box to use the local credentials for accessing the proxy server.
Login	Enter the username for accessing the proxy server.
Password and Confirm Password	Enter the password for accessing the proxy server.

NOTE: The appliance supports proxy servers that use basic, realm-based authentication, requiring usernames and passwords. If your proxy server uses a different kind of authentication, add the appliance's IP address to the proxy server's exception list.

7. To use an external SMTP server, select **Enable SMTP Remote Server (Outbound Relay)** in the *SMTP* tab, then specify SMTP server options:

Option	Description
Server	Specify the hostname or IP address of an external SMTP server, such as **smtp.gmail.com**. External SMTP servers must allow anonymous (non-authenticated) outbound email transport. Ensure that your network policies allow the appliance to contact the SMTP server directly. In addition, the mail server must be configured to

Option	Description
	allow the relaying of email from the appliance without authentication. If you specify an IP address, enclose the address in brackets. For example `[10.10.10.10]`.
Port	Enter the port number to use for the external SMTP server. For standard SMTP, use port 25. For secure SMTP, use port 587.
Login	Enter the username of an account that has access to the external SMTP server, such as **your_account_name**@gmail.com.
Password and Confirm Password	Enter the password of the specified server account.

8. Test the SMTP configuration.
    a. Click **Test Connection**.
    b. In the *Connection Test SMTP* dialog box that appears, type the email address to which you want to send a test email using the newly configured SMTP server, and click **Send Test Email**.

    The *Connection Test SMTP* dialog box refreshes, showing the test results. status of the email operation. If the test fails, verify your configuration, and try again.
9. Click **Save**.

    The appliance reboots. Total reboot downtime is one to two minutes, provided that the changes result in a valid configuration.
10. If you changed the appliance IP address, go to the new address to display the Administrator Console login page.

Configure local routing tables

Configure local routing tables to enable the appliance to route traffic through multiple gateways on a network.

Local routing tables are useful when the physical appliance is located in one office, and managed devices are located in a different location. For example, if the appliance is located in Texas, and managed devices are located in California, the appliance would serve devices on the Texas subnet. Using the a local routing table, the appliance could be pointed to the network in California, so that it could host the California devices as well as the Texas devices.

1. Go to the appliance *Control Panel*:
    - **If the Organization component is not enabled on the appliance, log in to the appliance Administrator Console, `https://appliance_hostname/admin`, then select Settings > Control Panel.**
    - **If the Organization component is enabled on the appliance, log in to the appliance System Administration Console, `https://appliance_hostname/system`, or select System in the drop-down list in the top-right corner of the page, then select Settings > Control Panel.**
2. Click **Local Routing Table** to display the *Local Routing Table Settings* page.
3. Click the **Add** button to add an entry: +.
4. Specify the following settings:

Option	Description
Name	Enter a name for the route.
Destination	Enter the IP address or network for the destination with which you want your appliance to communicate.
Subnet Mask or CIDR	Enter the subnet mask of the specified network. For example: `24`, `255.255.240.0`. This is applied to the host.

Option	Description
Gateway	Enter the IP address of the router that routes traffic between the appliance and the destination network.

5. Click **Add** at the end of the row to save the entry.
6. Click **Save and Reboot** at the bottom of the page to save all changes.

   A warning appears indicating that the Apache™ service needs to be restarted.
7. Click **OK** to continue.

Configure local web server settings and allow access to hosts

You can configure local web server settings to specify an allow list of hosts that are allowed to access the **Administrator Console**, **System Administration Console**, and the **User Console**. After you create the allow list, access is restricted to the hosts on the allow list.

NOTE: After an IP address or domain name is added to the *Allow List*, only that IP address or domain has access. All others are blocked.

1. Go to the appliance *Control Panel*:
   - **If the Organization component is not enabled on the appliance, log in to the appliance Administrator Console, `https://appliance_hostname/admin`, then select Settings > Control Panel.**
   - **If the Organization component is enabled on the appliance, log in to the appliance System Administration Console, `https://appliance_hostname/system`, or select System in the drop-down list in the top-right corner of the page, then select Settings > Control Panel.**
2. In the **Access Control List** section, click the *Limit appliance access to acceptable networks* option to display the *Access Control List Details* page.
3. Specify the following options:

Option	Description
No access restrictions	Select this option to allow access from any web address.
Restrict access as specified below	Select this option to restrict access to web addresses on the Allow List. To enable access to IP addresses on the appliance's subnet in addition to the specified destinations, select **Allow all IP addresses in the same subnet as the appliance**.

4. In the *Allow List* section, click the **Add** button to add an entry: +.
5. Specify the following options.

Option	Description
Destination	Specify the destination: • **adminui**: This is the **Administrator Console**, Admin level. An allow list of IP addresses and/or host names who can log in to `http://`**appliance_hostname**`/admin`. • **userui**: This is the **User Console**. An allow list of IP addresses and/or host names who can log in to `http://`**appliance_hostname**`/user`. • **systemui**: This is the **System Administration Console** (available only if the Organization component is enabled on the appliance). An allow list of IP addresses and/or host names who can log in to `http://`**appliance_hostname**`/system`. • **api**: This is the appliance API. An allow list of IP addresses and/or host names who can access the appliance using its API, including the KACE GO app.
IP Address/ Domain Name	Provide the address to be allowed. This can be either: • A domain or sub-domain name (full or partial) • An IP address (full or partial)
Subnet Mask/ CIDR/Prefix Length	Provide a subnet mask/CIDR (Classless Inter-Domain Routing) to be allowed. This enables a finer-grained subnet control.

6. Click **Save** at the end of the row to save the entry.
7. Click **Save** at the bottom of the page to save all changes.

   A warning appears indicating that the Apache service needs to be restarted.
8. Click **OK** to continue.

NOTE: After an IP address or domain name is added to the *Allow List*, only that IP address or domain can access that page. All others are blocked.

Configure security settings for the appliance

You must configure appliance security settings to enable certain capabilities such as Samba share, SSL, SNMP, SSH, database access, and FTP access.

To enable SSL, you need to have the correct SSL private key file and a signed SSL certificate. If your private key has a password, the appliance cannot restart automatically. If you have this issue, contact **Quest Support** at https://support.quest.com/contact-support.

- Saving changes to security settings reboots the appliance.
- In some cases, the Firefox® browser does not display the **Administrator Console** login page correctly after you enable access to port 443 and restart the appliance. If that happens, clear the Firefox browser cache and cookies, then try again.

1. Go to the appliance *Control Panel*:
   - **If the Organization component is not enabled on the appliance, log in to the appliance Administrator Console, `https://appliance_hostname/admin`, then select Settings > Control Panel.**
   - **If the Organization component is enabled on the appliance, log in to the appliance System Administration Console, `https://appliance_hostname/system`, or select System in the drop-down list in the top-right corner of the page, then select Settings > Control Panel.**
2. In the **Security Settings** section, click *Security Options* to display the *Security Settings* page.
3. In the Security Options tab, specify the following settings:

Option	Description
Enable SSH	Permit SSH logins to the appliance. When SSH is enabled, SSH encrypted communications are permitted over port 22.
Enable backup via FTP	Enable access to the database backup files through a read-only FTP server. This enables you to create a process on another server to access the backup files. If you do not need this access, clear this option.
Make FTP writable	Enable the upload of backup files using FTP. FTP is useful for backup files that are too large for the default HTTP mechanism and cause browser timeouts.
New FTP user password	Require a password for FTP access to the backup files.
Enable Secure Remote Logging via TLS	Specify server IP and port of the remote syslog-ng or rsyslog. TLS Default port is 6514. Enabling remote syslog-ng or rsyslog allows you to send server log data to a remote syslog-ng or rsyslog server. For more details, refer Configure Encrypted Remote Logging to an External Syslog-ng Server.
Enable Secure backup files	Require username and password authentication for access to appliance backup files, which are available by entering a URL in a browser. Clear this option to enable access to backup files through a URL without username or password authentication. This is useful for external process that require access. See About appliance backups.
Enable mDNS	Enable the appliance to respond to multicast Domain Name System (mDNS) and DNS Service Discovery (DNS-SD) requests. This option makes it easier for users and administrators to locate the **Administrator Console** and **User Console**. If you do not need the appliance to respond to these requests, clear this option.
Enable Munin access	Enable the appliance to view server usage and metrics over time.

Option	Description
	NOTE: This allows unrestricted, unauthenticated access to `/munin`.
SNMP Community String	The SNMP community string that enables read-only SNMP access. The default value is public.
MIB Files	Upload vendor-specific MIB (management information base) files. A MIB file allows the trap receiver on the appliance to translate SNMP traps into human-readable messages. These files are optional. • To upload a MIB file, on the *Security Settings* page, under *MIB Files*, in the *Upload MIB* area, click **Browse**, and select a MIB file. • A MIB file must meet certain standards. The appliance validates every MIB file that you upload. If you upload an invalid MIB file, an error message appears along the top of the *Security Settings* page. If you do not want to validate the contents of the MIB file, select the **Skip MIB validation** check box.
Secure Service Desk Attachments	Choose whether to add security for files that are attached to Service Desk tickets: • Select the check box to enable security for files attached to tickets. If you choose this option, users can access files attached to tickets only from within the appliance **Administrator Console** or **User Console**. • Clear the check box to enable users to access files by clicking ticket links from outside the **Administrator Console** or **User Console**.
Enable database access	Enable users to run reports on the appliance database using an external tool, such as Microsoft Access or Excel, over port 3306. If you do not need to expose the database in this way, clear this option. **NOTE:** The appliance database can be accessed from any ODBC-compliant third-party tool if you have installed the (32bit) MySQL ODBC driver. You must select this check box if you want to use this feature. In addition, you will need to configure a data source for your MySQL ODBC driver, and provide the appliance connection information. For more information, refer to your MySQL ODBC driver documentation.
Enable secure database access (SSL)	Enable SSL access to the database and access additional SSL options.
Enable API Access	Selecting this allows external tools and applications including the KACE GO mobile application to interact with the **System Management Appliance**. See Enable API Access for the appliance.
Enable mobile device access	Enable or disable Mobile Device Access to the appliance. Mobile device access enables you to interact with the appliance using the **KACE GO** app on iOS and Android smart phones and tablets. Administrators can use the app to access Service Desk, inventory, and application deployment features. See Configuring Mobile Device Access.
Enable SNMP READ access	Enable unidirectional (read-only) SNMP access to managed devices on the network through port 199 using SMUX, an SNMP multiplexing protocol. See Verify port settings.

Option	Description
	You can query the SMA using SNMP v1, v2, and v3 protocols. • **SNMP version 1 or 2**: This version only requires a valid community string. • **SNMP version 3**: This version implements enhanced security and remote configuration features and requires a valid user name and encryption information. To add a security name, open the **v3** tab, click +, and provide the following information: # **Security Name**: The name of the User-based Security Model (USM) account that sends the SNMP trap. # **Authentication Password**: The password associated with the Security Name. # **Authentication Protocol**: The protocol used for authenticating the user: MD5 or SHA. # **Privacy Password**: The encryption key for the data packet. # **Privacy Protocol**: The encryption protocol: AES or DES. # **Security Level**: Indicates the level of security: # **authPriv**: The identity of the sender is verified and the information is encrypted. # **authNoPriv**: The identity of the sender is verified, but the information is not. # **noAuthNoPriv**: The identity of the sender is not verified and the information is not encrypted.
Enable remote syslog	Enable the appliance to send limited server log data to a remote `Syslog` server. **NOTE:** Log data sent this way is unencrypted and uses UDP (User Datagram Protocol). Before selecting this option, review your organization's guidelines about security and network saturation.
Remote Syslog Server	Specify the fully qualified domain name (FQDN) or IP address and the port number of the remote `Syslog` server. IPv4 and IPv6 addresses are supported. If you do not provide a port number, the appliance uses 514 (UDP), the default port number for `Syslog` traffic.
Enable SNMP Trap monitoring	Enable SNMP (Simple Network Management Protocol), a protocol for monitoring managed devices on a network. SNMP is supported by Dell Open Manage and many third-party products. If you do not want to receive SNMP traps from network devices, clear this option. When you enable this feature on the appliance, and the related devices are also enabled for monitoring, the appliance can receive SNMP traps from the monitored network devices such as printers, projectors, and routers. This feature only applies to network devices managed through the SNMP-managed devices, such as agentless devices using SNMP connections. For information on how to enable device monitoring, see Enable monitoring for one or more devices. SNMP traps are messages initiated by network devices and sent to the trap receiver on the appliance. For example, a router can send a message when its power supply fails. Or, a printer initiates a message when it runs out of paper. The appliance

Option	Description
	receives these traps and generates alerts when certain pre-defined thresholds are reached. • **SNMP version 1 or 2**: This version only requires a valid community string. A community string is required to allow the appliance to receive SNMP trap messages from monitored network devices. The appliance supports multiple security strings. To add a community string, open the **v1/v2** tab, click +, type the community string, and click **Save**. • **SNMP version 3**: This version implements enhanced security and remote configuration features and requires a valid user name and encryption information. To add a security name, open the **v3** tab, click +, and provide the following information: # **Security Name**: The name of the User-based Security Model (USM) account that sends the SNMP trap. # **Engine ID**: The ID of the SNMP application engine that sends the SNMP trap. # **Authentication Password**: The password associated with the Security Name. # **Authentication Protocol**: The protocol used for authenticating the user: MD5 or SHA. # **Privacy Password**: The encryption key for the data packet. # **Privacy Protocol**: The encryption protocol: AES or DES. # **Security Level**: Indicates the level of security: # **authPriv**: The identity of the sender is verified and the information is encrypted. # **authNoPriv**: The identity of the sender is verified, but the information is not. # **noAuthNoPriv**: The identity of the sender is not verified and the information is not encrypted.
Brute Force Prevention	Specify the number of failed login attempts and the time for which the account is disabled. Brute force prevention restricts a user account from logging in to all user interfaces and the API. For multi-organization appliances, this behavior is organization specific per user and applies to accounts in the System user interface.

4. In the *Two-Factor Authentication* tab, configure the Two-Factor Authentication (2FA) feature. 2FA provides stronger security for users logging into the appliance by adding an extra step to the login process. It relies on the Google Authenticator app to generate verification codes. The app generates a new six-digit code at regular intervals. When enabled, end users will be prompted for the current verification code each time they log in.

   NOTE: If you enable this feature, ensure that appliance server's clock is accurate, as well as the device running Google Authenticator. Google Authenticator relies on current time to create the token. If server's clock is not synchronized with those of the devices running Google Authenticator, token validation may fail, which may result in account lockouts.

   a. Specify the following options. They appear listed in the order of precedence, as you enable them from top to bottom. For example you can only enable 2FA for the User Console if you have previously configured 2FA for the Administrator Console.

   # **Enable Two-Factor Authentication for the System Portal**: Select this check box if you want to use 2FA for the **System Administration Console**. To enable 2FA for all users, select **Required for all Users**.

NOTE: This option is only available on appliances with multiple organizations.

Enable Two-Factor Authentication for the Admin Portal: This option only appears if you enabled 2FA for the **System Administration Console**, or if your appliance has only one organization. Select this check box if you want to use 2FA for the **Administrator Console**. Next, specify the users that will require 2FA during login by selecting one of the following options:

- **Required for all Users**: **Appliances with one organization only**. To enable 2FA for all users, select this option.
- **Defined by Organization**: **Appliances with multiple organizations only**. Apply the same 2FA configuration to all users in each Organization in the **Administrator Console**, as applicable.
- **Required for all Users**: **Appliances with multiple organizations only**. Enable 2FA for all users in the **Administrator Console**.
- **Not required**: **Appliances with multiple organizations only**. Disable 2FA for all users in the **Administrator Console**.

Enable Two-Factor Authentication for the User Portal: This option only appears if you enabled 2FA for the **Administrator Console**. Select this check box if you want to use 2FA for the **User Console**. Next, specify the users that will require 2FA during login by selecting one of the following options:

- **Defined by Organization**: Apply the same 2FA configuration to all users in each Organization in the **User Console**, as applicable.
- **Required for all Users**: Enable 2FA for all users in the **User Console**.
- **Not required**: Disable 2FA for all users in the **User Console**.

b. Under **Transition Window**, specify the amount of time during which users who require 2FA will be able to bypass the 2FA configuration step.

For example, if a user forgets their phone at home and is therefore unable to generate a new code, they can still access the portal during the period of time specified here.

5. Use the settings in the *Brute Force Prevention* area to prevent multiple consecutive attacks from obtaining access to the appliance using false credentials. You can configure the number of failed authentication attempts within a specified time frame, after which the appliance prevents any logins for that user.

The default setting is three attempts during a five-minute period. You can change these values, as needed.

When the appliance disables a user account from logging in, other users are not affected and can log in to the appliance with valid credentials.

6. **Optional**: In the *Appliance Encryption Key* section, click **Generate Key** to generate a new encryption key. This key is used to enable Quest Support to access your appliance for troubleshooting using a tether. It is not necessary to generate a new key unless you believe that the current key has been compromised. See Enable a tether to Quest KACE Support.

The time stamp shows the time the key was generated.

7. In the *Single Sign On* tab, specify authentication settings:

Option	Description
Disabled	Prevent the appliance from using single sign on. Single sign on enables users who are logged on to the domain to access the appliance **Administrator Console** and **User Console** without having to re-enter their credentials on the appliance login page.
Active Directory	Use Active Directory for authentication. Active Directory uses the domain to authenticate users on the network. See Using Active Directory for single sign on.

8. In the **Samba** tab, specify the following settings:

Option	Description
For appliances with the Organization component enabled: **Enable Organization File Shares** For appliances without the Organization component: **Enable File Sharing**	Use the appliance's client share to store files, such as files used to install applications on managed devices. The appliance's client share is a built-in Windows file server that can be used by the provisioning service to assist in distributing the Samba client on your network. Quest recommends that this file server only be enabled when you perform application installations on managed devices. **NOTE:** If the Organization component is enabled on your appliance, you can select additional file sharing options for each organization. See Enable file sharing at the System level.
Samba minimum protocol, **Samba maximum protocol**	Select the minimum and maximum Samba protocol, as required. The following options are available in each setting: • **SMB2**: Re-implementation of the SMB protocol. Used by Windows Vista and later versions of Windows. SMB2 has sub protocols available. By default SMB2 selects the SMB2_10 variant. • **SMB2_02**: The earliest SMB2 version. • **SMB2_10**: Windows 7 SMB2 version. • **SMB2_22**: Early Windows 8 SMB2 version. • **SMB2_24**: Windows 8 beta SMB2 version. • **SMB3**: Re-implementation of the SMB2 protocol. Used by Windows 8. SMB3 has sub protocols available. By default SMB3 uses the SMB3_11 variant. • **SMB3_00**: Windows 8 SMB3 version (similar to SMB2_24). • **SMB3_02**: Windows 8.1 SMB3 version. • **SMB3_10**: Early Windows 10 technical preview version. • **SMB3_11**: Windows 10 technical preview version.
Require signing	Enables signing in for the Samba protocol.
Disable Guest Access	Disables Samba guest access.
Require NTLMv2 to appliance file shares	Enable NTLMv2 authentication for the appliance files shares. When this is enabled, managed devices connecting to the appliance File Shares require support for NTLMv2 and they authenticate to the appliance using NTLMv2. Although NTLMv2 is more secure than NTLM and LANMAN, non-NTLMv2 configurations are more common and this option is usually turned off. Enabling this option disables **lanman auth** and **ntlm auth** on the Samba server. NTLMv2 Levels 1-4 are supported. If you need NTLM v2 Level 5, consider manually provisioning the KACE Agent. See Manually deploying the KACE Agent.
Require NTLMv2 to off-board file shares	Force certain appliance functions that are supported through the Samba client, such as Agent Provisioning, to authenticate to off-board network file shares using NTLMv2. Even though NTLMv2 is more secure than NTLM and LANMAN, non-NTLMv2

Option	Description
	configurations are more common and this option is usually disabled. Enabling this option enables the **client ntlmv2 auth** option for Samba client functions.

9. **Optional**: In the *SSL* tab, specify SSL settings:

IMPORTANT: Enabling SSL is a one-way automatic shift for managed devices. Devices must be reconfigured manually if you disable SSL.

Option	Description
Enable Port 80 access	Enable access to the appliance over port 80. If you disable port 80 access, contact **Quest Support** to adjust the Agent deployment scripts to handle SSL.
Enable Forward port 80 to port 443	When you verify that SSL is working as expected, you can enable the forwarding of all communication from port 80 to port 443. To do that, select this check box.
Enable SSL	Enable managed devices to connect to the appliance using SSL (HTTPS). Enable this setting only after you have properly deployed the appliance on your LAN in non-SSL mode. To enable SSL, you need to load an SSL certificate as described in step 10.

10. To load an SSL certificate, do one of the following:

If your SSL certificate and private key are in Privacy Enhance Mail (PEM) format, similar to those used by Apache-based web servers:

1. Select **Upload PEM SSL Certificate**.
2. In the *SSL Private Key File* and *SSL Certificate File* fields, select the private key and certificate files.
3. If you want to enable and upload intermediate SSL certificates (also in PEM format), select **Enable Intermediate SSL Certificate**. Intermediate SSL certificates are signed certificates provided by certificate issuers as proxies for root certificates.

If your certificate is in PKCS-12 format:

1. Select **Upload PKCS-12 SSL Certificate**.
2. In the *PKCS-12 File* field, select the file.
3. In the *Password for PKCS-12 file* field, type the password for the PKCS-12 file.

To use the Let's Encrypt service for SSL certificates:

1. Click **Apply Let's Encrypt SSL Certificate**. Let's Encrypt is a free, automated, and open certificate authority (CA). When you get a certificate from Let's Encrypt, their servers validate that you control the domain names in that certificate using a challenge.

   NOTE: The HTTP-01 challenge can only be done on port 80. Specify arbitrary ports makes the challenge less secure, and it is therefore not allowed by the Automatic Certificate Management Environment (ACME) standard. For that reason, the appliance must run on a public-facing box with port 80 open for inbound communication, and a publicly-resolvable DNS. For more details, visit https://letsencrypt.org/docs/challenge-types/.

2. In the *Email Address* field, provide an email address. While Let's Encrypt certificates periodically expire, the appliance uses an automated process to update the certificate before its expiration. The address is used for communication with Let's Encrypt in an unlikely event the certificate expires. You must have a Let's Encrypt account registered using this email address.
3. Select the check box to agree with the terms of service.

To generate certificate requests or load self-signed certificates:

1. Click **Generate CSR (Certificate Signing Request) or Self-Signed SSL Certificate**.
2. In the area that appears, click **SSL Certificate Form**. Follow the instructions in Generate an SSL certificate.

11. In the *CSP* tab, select the **Enable CSP** checkbox to enable CSP (Content Security Policy). Enabling the checkbox adds list of KACE trusted domains automatically.
    - **If you want to add domains or URLs in the list, then in the Additional Allowed Domains section, click +, and specify the Directive and the Domain/URL. For more details, Configuring Content Security Policy**
12. In the *Secure Attachments* in Service Desk section, choose whether to add security for files that are attached to Service Desk tickets:
    - **Select the check box to enable security for files attached to tickets. If you choose this option, users can access files attached to tickets only from within the appliance Administrator Console or User Console.**
    - **Clear the check box to enable users to access files by clicking ticket links from outside the Administrator Console or User Console.**
13. Click **Save and Restart Services** to save changes and restart the appliance.

NOTE: In some cases, the Firefox browser does not display the **Administrator Console** login page correctly after you enable access to port 443 and restart the appliance. If that happens, clear the Firefox browser cache and cookies, then try again.

Configure Encrypted Remote Logging to an External Server

You can now securely forward the system logs from the Systems Management Appliance (SMA) to an external server using the syslog-ng protocol with TLS encryption. This setup enables encrypted one-way communication, ensuring that log data cannot be intercepted or read by unauthorized parties.

The administrators can send all the SMA-generated logs to a remote server over port 6514 using TLS.

Before you begin, you must ensure that-

- the SMA must be accessible through a supported browser.
- the remote server must have syslog-ng installed and configured.
- port 6514 is open for incoming connections on the syslog-ng server.

NOTE: The KACE SMA supports integration with any logging system that can be configured to use TLS. While the document provides examples for integrating with syslog-ng and rsyslog, our support is not limited to these tools.

Configuring Encrypted Remote Logging

1. Go to the appliance *Control Panel*:
    - **If the Organization component is not enabled on the appliance, log in to the appliance Administrator Console, `https://appliance_hostname/admin`, then select Settings > Control Panel.**
    - **If the Organization component is enabled on the appliance, log in to the appliance System Administration Console, `https://appliance_hostname/system`, or select System in the drop-down list in the top-right corner of the page, then select Settings > Control Panel.**
2. In the **Security Settings** section, click *Security Options* to display the *Security Settings* page.
3. Select the **Enable Secure Remote Logging via TLS** checkbox.
4. Enter the IP address of the syslog-ng or rsyslog server.
5. Specify the destination port (default is 6514). You may use a custom port if required-ensure it is open for incoming connections on the remote server.
6. Click **Save and Restart Services**.

When the configuration is enabled, the SMA generates a public certificate and private key. The public certificate remains on the SMA, while the private key must be uploaded to the syslog-ng or rsyslog server.

7. After the service restarts, download the server TLS files for configuration by clicking the Server key and Server certificate.

   The files get downloaded on your machine. The server key file is used to authenticate the server, while the server certificate file is used to encrypt the connection between the SMA and the remote syslog server.

8. Configure the logging service for syslog-ng or rsyslog.

   a. Configure Syslog server to receive logs from KACE System Management Appliance.

   # Open the syslog-ng.conf file.

   # Update the paths to the server key and certificate files. Add the following configuration at the end of the file:

```
source tls_source {
    tcp(
        ip(0.0.0.0)
        port(6514)
        tls(
            key_file(" ("/usr/local/etc/syslogng/serverkey.pem")
            cert_file("/usr/local/etc/syslogng/servercert.pem")
            peer-verify(optional-untrusted)
        )
    );
};
```

   # Configure the log path

```
log { source(tls_source); destination(messages); };
```

   NOTE: Sometimes you may see the HOSTNAME twice in a log statement. If this is an issue, you can use a custom destination to fix it.

```
destination d_custom {
    file("/var/log/syslog"
        template("${DATE} ${HOST} ${MESSAGE}\n")
    );
};
log {source(tls_source); destination(d_custom);};
```

   NOTE: Sometimes you might notice duplicate logs appearing on your syslog-ng server. This can happen when the same destination is specified in multiple log paths. To fix this, it's recommended to consolidate all sources into a single log path statement, as shown in the example below:

```
log { source(tls_source);source(s_src);
       filter(f_messages); destination(d_messages); };
```

   # Restart the syslog-ng service.

   b. Configure rsyslog remote server to version **v8.2504.0** or later. The below configuration works with **v8.2504.0**.

   # Upgrade to rsyslog latest version.

```
sudo add-apt-repository ppa:adiscon/v8-stable
sudo apt-get upgrade rsyslog
Add package > sudo apt-get install rsyslog-gnutls
```

   # Locate and open the rsyslog.conf file, then add the following configuration at the end of the file.

```
global(
   defaultNetstreamDriver="gtls"
)
module(load="imtcp")
# Input for the first certificate
input(
   type="imtcp"
   port="6514"
   StreamDriver.Name="gtls"
   StreamDriver.Mode="1"
   StreamDriver.AuthMode="anon"
   StreamDriver.CertFile="/etc/rsyslog.d/servercert.pem"
   StreamDriver.KeyFile="/etc/rsyslog.d/serverkey.pem"
)
```

Restart rsyslog service.

9. Go to KACE System Management Appliance System UI > **Security Settings,** and click the **Test** button to ensure a secure connection is established.

   If the connection is successful, a confirmation message appears.

NOTE: The servercert.pem and serverkey.pem files are generated by the SMA and can be downloaded from the Security Settings page. The server key file is used to authenticate the server, while the server certificate file is used to encrypt the connection between the SMA and the remote syslog server. You should update the configuration file names **"servercert.pem" and "serverkey.pem"** with the actual file names you downloaded from the SMA.

Certificate Renewal Notification

- A certificate expiration check runs periodically.
- If a certificate is due to expire within 30 days, users receive a notification in the SMA UI.
- Users can renew the certificate using the **Renew Certificate** option and must repeat the process of uploading it to the server and verifying the connection.

- The configuration supports both Linux and Windows as syslog-ng servers, as long as syslog-ng is installed and properly configured.
- The administrators are responsible for managing the certificates.

Configure Active Directory as the single sign on method

Active Directory single sign on enables users who are logged on to the domain to access the appliance **Administrator Console** and **User Console** without having to re-enter their logon credentials each time.

Before you connect the appliance to an Active Directory server, verify that:

- Network and DNS settings are configured to enable the appliance to access the Active Directory server. See Change appliance network settings.
- The time settings on the Active Directory server match the time settings on the appliance. For information on setting the time on the appliance, see Configure appliance date and time settings.

1. Go to the appliance *Control Panel*:
   - **If the Organization component is not enabled on the appliance, log in to the appliance Administrator Console, `https://appliance_hostname/admin`, then select Settings > Control Panel.**
   - **If the Organization component is enabled on the appliance, log in to the appliance System Administration Console, `https://appliance_hostname/system`, or select System in the drop-down list in the top-right corner of the page, then select Settings > Control Panel.**
2. In the *Single Sign On* tab of the *Security Settings* page, select **Active Directory**, then provide the following information:

Option	Description
Domain	The host name of the domain of your Active Directory® server, such as example.com.
Username	The user name of the administrator account on the Active Directory server. For example, username@example.com.
Password	The password of the administrator account on the Active Directory server.
Computer Object Container	The name of the computer object container of the administrator account on the Active Directory server.
Computer Object Name	The name of the computer object container of the administrator account on the Active Directory server.
Service Account Container	The name of the service account container of the administrator account on the Active Directory server.

3. Click **Join**.

The appliance performs the following tests, which require read-only permission, to determine whether the domain is configured correctly to allow the appliance to join the domain:

```
#   Check for supported operating system and correct operating system patches
#   Check for sufficient disk space to install QAS
#   Check that the hostname of the system is not 'localhost'
#   Check if the name service is configured to use DNS
#   Check resolv.conf for proper formatting of name service entries and that
    the host can be resolved
#   Check for a name server that has the appropriate DNS SRV records for Active
    Directory
#   Detect a writable domain controller with UDP port 389 open
#   Detect Active Directory site if available
#   Check if TCP port 464 is open for Kerberos kpasswd
#   Check if UDP port 88 and TCP port 88 are open for Kerberos traffic
#   Check if TCP port 389 is open for LDAP
#   Check for a global catalog server and if TCP port 3268 is open for
    communication with global catalog servers
#   Check for a valid time skew against Active Directory
#   Check for the QAS application configuration in Active Directory
#   Check if TCP port 445 is open for Microsoft CIFS traffic
```

These tests do not need write access and they do not check for permission to write to any directory. In addition, these tests do not verify username and password credentials. If the credentials are incorrect, the appliance might not be able to join the domain even if the tests are successful.

A message appears stating the results of the test. To view errors, if any, click **Logs**, then in the *Log* drop-down list, select **Server Errors**.

4. **Optional**: Select **Force Join** to join the server to ignore errors and join the domain.
5. Click **Save**.

When users are logged in to devices that are joined to the Active Directory domain, they can access the appliance **User Console** without having to re-enter their credentials. If users are on devices that are not joined to the Active Directory domain, the login window appears and they can log in using a local appliance user account. See Add or edit System-level user accounts.

NOTE: To use single sign on with Microsoft Edge and Firefox browsers, users must configure their browser settings to use the appropriate authentication. See Configuring browser settings for single sign on.

Generate an SSL certificate

You can generate a self-signed SSL certificate, or generate a certificate signing request for third-party certificates, using the **Administrator Console**.

1. Go to the appliance *Control Panel*:
   - **If the Organization component is not enabled on the appliance, log in to the appliance Administrator Console, `https://appliance_hostname/admin`, then select Settings > Control Panel.**
   - **If the Organization component is enabled on the appliance, log in to the appliance System Administration Console, `https://appliance_hostname/system`, or select System in the drop-down list in the top-right corner of the page, then select Settings > Control Panel.**
2. In the **Security Settings** section, click *Configure SSL* to open the SSL tab on the *Security Settings* page.
3. In the *SSL* section, click **Enable SSL**.

   Additional SSL options are displayed.
4. Click **Generate CSR (Certificate Signing Request) or Self-Signed SSL Certificate**, then click **SSL Certificate Form** to display the *SSL Certificate Form* page.

   NOTE: If a certificate signing request has previously been generated, it appears on the page. To generate a new request, you need to update the information in the *Configure* section, then click **Save** before you click **Generate Self-Signed Certificate**.
5. In the *SSL Certificate Form* page , provide the following information:

Option	Description
Company Name	The name of your company.
Organization Name	The name of your organizational unit or business group.
Common Name	The common name of the appliance you are creating the SSL certificate for.
Email	Your email address.
City Name	The name of your locality.
State or Province Name	The name of your state or province.
Country Name	The name of your country.
Subject Alternative name	Alternative name of the appliance you are creating the SSL certificate for. It can have multiple comma separated entries.

6. Click **Save**.

   If this is the first time the *SSL Certificate Form* has been saved, the *Certificate Signing Request* section appears. If the form has previously been saved, the *Certificate Signing Request* section is updated.
7. Do one of the following:
   - **To generate a certificate using a third-party certificate issuer:**
     1. Copy all of the text in the *Certificate Signing Request* section, including the lines `"-----BEGIN CERTIFICATE REQUEST-----"` and `"-----END CERTIFICATE REQUEST-----"` and everything in between, then send it to the certificate issuer or the person who provides your company with web server certificates.

2. When you receive a certificate from the third party, return to the *Security Settings* page and upload the certificate. See Configure security settings for the appliance.

- **To generate a self-signed certificate:**

1. Click **Generate Self-Signed Certificate** to generate and display the certificate below the *Certificate Signing Request* section.
2. Click **Deploy Self-Signed Certificate**, then click **Yes**.
3. On the *Security Settings* page, click **Save and Restart Services**.

Self-signed certificates are converted to PEM files, named `kbox.pem`, and the files are placed in KACE Agent data folders.

NOTE: Your private key appears in the *Private Key* field. It is deployed to the appliance when you deploy a valid certificate. Do not send the private key to anyone. It is displayed here in case you want to deploy this certificate to another web server.

NOTE: The certificate and private key for SSL are not included in the appliance's daily backups for security reasons. Retain these two files for your own records.

Configuring session timeout settings

Session timeout is a System-level setting that specifies the amount of inactive time that can pass before users are automatically logged out of the **Administrator Console** or **User Console**. Auto-refresh settings are user-level settings that determine the frequency with which console pages are refreshed.

Set session timeout

You can configure session timeout to meet your security requirements.

1. Go to the appliance *Control Panel*:
   - **If the Organization component is not enabled on the appliance, log in to the appliance Administrator Console, `https://appliance_hostname/admin`, then select Settings > Control Panel.**
   - **If the Organization component is enabled on the appliance, log in to the appliance System Administration Console, `https://appliance_hostname/system`, or select System in the drop-down list in the top-right corner of the page, then select Settings > Control Panel.**
2. In the **General Settings** section, click the Customize general configurations option to display the General Options tab on the *General Settings* page.
3. In the top section, configure the session timeout:

Options	Description
Session Timeout	Set the number of inactive hours to allow before closing user sessions and requiring users to log in again. The default is 1. The **User Console** and **Administrator Console** have Timeout Session counters to alert users of this time limit. Only periods of inactivity are counted. The counter restarts when the user performs any action that causes the console to interact with the appliance server, such as refreshing a window, saving changes, and changing windows. When a session reaches 60 seconds before the timeout, a message box appears, allowing you to extend the session, or to log off. Once the counter reaches the limit, the user is logged out, unsaved changes are lost, and the login screen appears. The Timeout Session counter appears in the upper right of each console.

4. Click **Save and Restart Services**.

Configuring locale settings

Locale settings determine the language used for text in the Command Line Console, Administrator Console, and User Console. Locale settings determine the formats used for date and time information displayed in the **Administrator Console** and **User Console**. All text in the interfaces is displayed in English regardless of locale settings.

The locale options available through your license agreement. See View the appliance version, model, and license information.

How locale settings are applied

Locale settings are applied in a particular order.

When choosing the locale for text in the **Command Line Console**, **Administrator Console**, and **User Console**, the appliance uses the following priority:

1. **User**: If the user locale is set, use it.
2. **Organization**: If the user locale is not set, use the organization setting (available only if the Organization component is enabled on the appliance).
3. **Browser**: If neither the user nor organization locales are set, use the browser setting.
4. **System** (**Command Line Console**): If the user, organization, and browser locales are not set, use the System setting.
5. **Default**: If none of the preceding options are set, use the default locale (English).

Configure locale settings for the Administrator Console and the Command Line Console

You can configure the locale setting for the **Administrator Console** at the System-level. This also controls the locale of the **Command Line Console**, which is accessed through the `konfig` user account.

Locale settings determine the formats used for date and time information displayed in the Administrator Console. All text in the interface is displayed in English regardless of locale settings. Locale settings also determine the date and time formats used in email sent from the Service Desk.

1. Go to the appliance *Control Panel*:
   - **If the Organization component is not enabled on the appliance, log in to the appliance Administrator Console, `https://appliance_hostname/admin`, then select Settings > Control Panel.**
   - **If the Organization component is enabled on the appliance, log in to the appliance System Administration Console, `https://appliance_hostname/system`, or select System in the drop-down list in the top-right corner of the page, then select Settings > Control Panel.**
2. Click **Customize general configurations** under the **General Settings** section to display the *General Settings* page.
3. If the Organization component is enabled on your appliance, do the following:
   a. Select a locale in the *Default Locale* drop-down list in the top section under the *General Options* tab.
   b. Click **Save** at the bottom of the page.
4. If the Organization component is not enabled on your appliance, do the following:
   a. In the *Locale Settings* section, select a locale from the *Organization Locale* drop-down list.
   b. In the *Locale Settings* section, select a locale from the Command Line Console drop-down list.
   c. Click **Save**.

The locale you selected is used for the **Administrator Console** and the **Command Line Console**.

Configure locale settings for the User Console

The appliance supports several locales. The **Administrator Console**, **System Administration Console**, and online help can be displayed in English, French, German, Japanese, Portuguese (Brazil), and Spanish.

In addition to these languages, you can translate the **User Console** into other non-supported locales, such as Afrikaans (South Africa), as needed. When you translate the **User Console** to a non-supported language, its help contents appear in English, while other elements of the appliance, such as the **Administrator Console**, **System Administration Console**, and the associated online help, are displayed in the selected language.

By default, the browser locale determines the language in which the **User Console** is displayed. When the **User Console** is translated to another languages and properly configured (as described below), any users whose browsers use that locale display the **User Console** in the translated language.

1. Go to the appliance *Control Panel*:
   - **If the Organization component is not enabled on the appliance, log in to the appliance Administrator Console, `https://appliance_hostname/admin`, then select Settings > Control Panel.**
   - **If the Organization component is enabled on the appliance, log in to the appliance System Administration Console, `https://appliance_hostname/system`, or select System in the drop-down list in the top-right corner of the page, then select Settings > Control Panel.**
2. Click **Configure "User Console" localization** under the **Localization** section to display the *User Console Localization Settings* page.
3. Export the text strings associated with the locale from which you want to translate to a Gettext portable object (PO) file, along with a portable object template (POT) for translation. For more information about Gettext PO files, see https://www.gnu.org/software/gettext/manual/html_node/PO-Files.html.
   a. On the *User Console Localization Settings* page, under *Export Gettext PO (portable object) File*, in the *Export* tab, select the locale which you want to translate from the *Export Locale Gettext PO (portable object) File* drop-down list. The list that appears includes all of the supported languages, as well as any languages to which you previously translated the User Console.
   b. Click **Export**.

   After a few moments, a ZIP file with the following contents is available for download:

   # A PO (portable object) file contains all of the **User Console** text strings that exist in your selected locale.
   # A POT (portable object template) file contains a template file, used to generate the empty PO file using the GetText utilities (optional).
4. Translate the User Console text strings, as required, and create a PO file.
5. Import the translated User Console strings.

   You can use a PO file editor to translate the strings in the PO file. For more information, see:

   # **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%20https://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. On the *User Console Localization Settings* page, in the *Import* tab, select the locale which you want to translate from the *Import Locale Gettext PO (portable object) File* drop-down list. Click **Import Locale**, and select the locale you want to associate with the PO file you are importing. This is the locale to which the User Console is translated using the translations from the imported PO file when the browser locale matches.
   b. Under *Translated PO (portable object) File*, click **Choose File**, and navigate to the translated PO file.

c. Click **Import**.

6. If you want to delete any locales that you previously imported, under *Delete an Uploaded Locale*, click *Delete Locale*, and select the locale that you want to delete. Click **Delete**.

Configure locale settings for organizations

If the Organization component is enabled on your appliance, you configure locale settings for each organization separately.

Locale settings determine the formats used for date and time information displayed in the Administrator Console and User Console. All text in the interfaces is displayed in English regardless of locale settings. Locale settings also determine the date and time formats used in email sent from the Service Desk.

1. Go to the *General Settings* page:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Settings**, then click **General Settings**.
2. If the Organization component is enabled on your appliance, do the following:
   a. In the *Locale Settings* under *General Operations* tab, select a locale in the *Organization Locale* drop-down list.
   b. Click **Save** at the bottom of the page.
   c. If you have multiple organizations, repeat the preceding steps for each organization.
3. If the Organization component is not enabled on your appliance, do the following:
   a. In the *Locale Settings* section, select a locale from the *Organization Locale* drop-down list.
   b. In the *Locale Settings* section, select a locale from the Command Line Console drop-down list.
   c. Click **Save**.

The selected locale is applied. Organization users who log in to the **Administrator Console** and **User Console** see the formats for this locale, provided that the browser settings are also set to display the locale. However, user locale settings take precedence over organization locale settings.

Configure locale settings for users

You can configure locale settings for each user. User locale settings take precedence over organization and System-level locale settings.

Locale settings determine the formats used for date and time information displayed in the **Administrator Console** and **User Console**. All text in the interfaces is displayed in English regardless of locale settings.

1. Go to the *User Detail* page:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Settings**, then click **Users**.
   c. Click the name of a user.
2. In the *Locale* drop-down list, select a locale.
3. Click **Save**.

The locale you selected is used when the user logs in to the **Administrator Console** or **User Console**, provided that the browser settings are also set to display the locale. User locale settings take precedence over the locale settings of the user's organization.

Configuring the default theme

In a default installation, the Administration Console appears in a default Light theme for every new user. Two additional themes are available: the Dark and Hybrid themes. You can change the default theme for the appliance. If the appliance theme is not suitable for your use, simply choose a different theme for your profile.

For example, if the Light theme is set by default for the appliance on the System level, and you associate the Dark theme with your user profile, the Dark theme is applied each time you log in.

Configure the default theme for the appliance

In a default installation, the appliance is configured to use the Light theme. You can choose a different theme as the default appliance theme, as needed.

1. Go to the appliance *Control Panel*:
    - **If the Organization component is not enabled on the appliance, log in to the appliance Administrator Console, `https://appliance_hostname/admin`, then select Settings > Control Panel.**
    - **If the Organization component is enabled on the appliance, log in to the appliance System Administration Console, `https://appliance_hostname/system`, or select System in the drop-down list in the top-right corner of the page, then select Settings > Control Panel.**
2. Click **Customize general configurations** under the **General Settings** section to display the *General Settings* page.
3. On the *General Settings* page that appears, click the *Themes* drop-down list, and choose one of the following options: **Light**, **Hybrid**, or **Dark**.

    When you choose the Light or Hybrid theme as the default appliance theme, the login page appears with a white background. A dark background is applied when the Dark theme is applied as the default appliance theme. The color of the login screen always reflects the configured appliance theme, not the theme associated with your user account. For example, if you choose the Dark theme in the Administrator Console, this theme becomes associated with your user account and is applied each time you log in. However if the appliance uses the Light theme by default, your login screen always appears with a white background. After a successful login, the Dark theme is applied.

    NOTE: Reports always appear with a white background, regardless of which theme is selected.

    NOTE: For newly created users, the **Administrator Console** uses the default theme. This can be changed on the next login. For more information, see Configure the default theme for a user.

Configure the default theme for a user

In a default installation, the Light theme is applied to each user profile. You can choose a different theme for your user profile, as needed. For example, if the Light theme is set by default for the appliance on the System level, and you associate the Dark theme with your user profile, the Dark theme is applied each time you log in.

1. Do one of the following:
    - **Log in to the appliance Administrator Console, `https://appliance_hostname/admin`, where appliance_hostname is the host name of your appliance. Or, if** *Show organization menu in admin header*

is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.

- **Log in to the appliance System Administration Console, `https://appliance_hostname/system`, where appliance_hostname is the host name of your appliance, or select System from the drop-down list in the top-right corner of the page.**
- **Log in to the applianceUser Console, `https://appliance_hostname/user`, where appliance_hostname is the host name of your appliance, or select User Console from the drop-down list in the top-right corner of the page.**

2. From the drop-down list in the top-right corner of the page, select **Manage My Profile**.

   The *User Profile* dialog box appears.

3. In the *User Profile* dialog box, on the *Profile* tab, click **Theme**, and select a theme that you want to associate with your user account: **Light**, **Dark**, or **Hybrid**.

   The theme you select this way becomes associated with your user account and is applied each time you log in. You can also configure the default theme for the appliance. For more information, see Configure the default theme for the appliance.

Configure data sharing preferences

Configure data sharing preferences at the System level. Data sharing preferences determine how much of your appliance information is shared with Quest.

To validate your product license, Quest collects minimal license-related information, such as the MAC Address of the appliance, the version of the appliance software, the license key, and the number of managed devices, regardless of the data sharing options selected in this section.

1. Go to the appliance *Control Panel*:

   - **If the Organization component is not enabled on the appliance, log in to the appliance Administrator Console, `https://appliance_hostname/admin`, then select Settings > Control Panel.**
   - **If the Organization component is enabled on the appliance, log in to the appliance System Administration Console, `https://appliance_hostname/system`, or select System in the drop-down list in the top-right corner of the page, then select Settings > Control Panel.**

2. Click **Share with us** to display the *General Settings* page.
3. In the *Share With us* tab, select from the following options:

Option	Description
Share summary usage data...	(Recommended) Share summary information with Quest. This information includes appliance status, uptime, and load averages, as well as the number of devices, Managed Installations, and applications being managed by the appliance. This option is recommended because it provides additional information to **Quest Support** if you need assistance. In addition, data shared with Quest is used when planning product enhancements.
Share detailed usage data...	(Recommended) Share detailed information with Quest. This information includes Agent and appliance crash reports, user interface usage statistics, and inventory information, such as application titles. Quest uses this information to help improve the Software Catalog for dynamic feeds to the appliance **Administrator Console**. The feed is a feature that dynamically displays software deployment tips and other contextual information on relevant pages in the appliance **Administrator Console**. To enable the feed, you need to select **Share detailed Usage data...**. . The feed is available only if **Share Summary Usage Data...** is selected, and it is available only on pages related to software or deployment, such as the software, Managed

Option	Description
	Installation, and File Synchronization detail pages. The feed is not available on *Software Catalog* detail page. Clear this option to prevent the appliance from sharing inventory data. However, clearing this option does not remove any information that has already been shared. For more information, contact **Quest Support**.

4. Click **Save and Restart Services**.

About DIACAP compliance requirements

You can configure the appliance to support regulations, such as DIACAP (Department of Defense Information Assurance Certification and Accreditation Process).

To comply with DIACAP, administrators perform the following tasks:

- Enable the Acceptable Use Policy. See Enable or disable the Acceptable Use Policy.
- Disable SSH and database access. See Configure security settings for the appliance.
- Disable Samba file sharing. See Configure security settings for the appliance.

Enable or disable the Acceptable Use Policy

To comply with policies and regulations, such as DIACAP (Department of Defense Information Assurance Certification and Accreditation Process), you can display an Acceptable Use Policy to users when they access the **Administrator Console**, **User Console**, or **Command Line Console**, or log in using SSH or FTP.

The Acceptable Use Policy is a System-level setting. If the Organization component is enabled on your appliance, you enable or disable the Acceptable Use Policy at the System level for all organizations. You cannot enable or disable the policy for individual organizations.

1. Go to the appliance *Control Panel*:
   - **If the Organization component is not enabled on the appliance, log in to the appliance Administrator Console, `https://appliance_hostname/admin`, then select Settings > Control Panel.**
   - **If the Organization component is enabled on the appliance, log in to the appliance System Administration Console, `https://appliance_hostname/system`, or select System in the drop-down list in the top-right corner of the page, then select Settings > Control Panel.**
2. In the *General Settings* section, click **Customize login screens and logos** to display the *General Settings* page.
3. In the *Acceptable Use Policy* section, select policy settings:

Option	Description
Enabled	Enable the appliance to display your policy, and require users to accept the terms of your policy, when they access the **Administrator Console**, **User Console**, or **Command Line Console**, or log in using SSH or FTP.
Title	The heading of the policy to be displayed on the login page of the **User Console**.
Message	Details of the policy, which are displayed below the *Title* on the login page. Users must agree to the terms of the policy before they can log in to the **User Console**.

4. Click **Save and Restart Services**.

When users go to the Administrator Console, User Console, or Command Line Console, or log in using SSH or FTP, they must first agree to the Acceptable Use Policy before they can log in.

NOTE: If single sign on is enabled, the login page is not displayed, so users do not see the Acceptable Use Policy before being logged in automatically. See About single sign on (SSO).

Enable API Access for the appliance

Enabling API access allows external tools and applications including the KACE GO mobile application to interact with the System Management Appliance (SMA). This setting is required for mobile device access and for any integrations that rely on SMA's API endpoints. API access must be enabled before configuring mobile access.

1. Go to the appliance *Control Panel*:
   - **If the Organization component is not enabled on the appliance, log in to the appliance Administrator Console, `https://appliance_hostname/admin`, then select Settings > Control Panel.**
   - **If the Organization component is enabled on the appliance, log in to the appliance System Administration Console, `https://appliance_hostname/system`, or select System in the drop-down list in the top-right corner of the page, then select Settings > Control Panel.**
2. In the *Security Settings* section, click **Security Options** to display the *Security Settings* page.
3. In the *Security Options* tab, select the *Enable API Access* check box.

   This enables the *Enable mobile device access* checkbox.
4. Select the *Enable mobile device access* check box. For more information, refer Enable Mobile Device Access for the appliance
5. Click **Save**.

Disable API Access for the appliance

Disabling API access ensures that the System Management Appliance is isolated from all the external API interactions. This configuration is ideal for secure environments where integrations with mobile apps or third-party tools are not required.

When API access is disabled, it also disables mobile access and overrides any existing Access Control List configurations, effectively blocking all external communication through the API.

1. Go to the appliance *Control Panel*:
   - **If the Organization component is not enabled on the appliance, log in to the appliance Administrator Console, `https://appliance_hostname/admin`, then select Settings > Control Panel.**
   - **If the Organization component is enabled on the appliance, log in to the appliance System Administration Console, `https://appliance_hostname/system`, or select System in the drop-down list in the top-right corner of the page, then select Settings > Control Panel.**
2. In the *Security Settings* section, click **Security Options** to display the *Security Settings* page.
3. In the *Security Options* tab, clear the *Enable API Access* check box to disable external API access. Once unchecked, the Enable mobile device access checkbox becomes greyed out and inaccessible.
4. Click **Save and Restart Services**.

   NOTE: If the *Enable API Access* checkbox was previously selected, it will be automatically unchecked when the page is saved.

Configuring Mobile Device Access

Mobile Device Access enables you to interact with the appliance using the KACE GO app.

KACE GO is an app that enables administrators to access Service Desk tickets, inventory information, and application deployment features from their smart phones or tablets. The app also allows non-admin users to submit Service Desk tickets, view the status of submitted tickets, and read Knowledge Base articles from their mobile devices. You can download KACE GO from the Apple App Store for iOS devices, or from the Google Play store for Android devices.

NOTE: KACE GO is only available in English.

To use Mobile Device Access, you must enable mobile device access for the appliance and for the users, and download and install KACE GO on a mobile device.

Enable Mobile Device Access for the appliance

By default, Mobile Device Access is disabled. To enable users to access the appliance using the KACE GO app, you must first enable Mobile Device Access for the appliance.

Mobile Device Access is enabled at the System level. If the Organization component is enabled on your appliance, and you enable Mobile Device Access, the feature is enabled for all organizations.

1. Go to the appliance *Control Panel*:
   - **If the Organization component is not enabled on the appliance, log in to the appliance Administrator Console, `https://appliance_hostname/admin`, then select Settings > Control Panel.**
   - **If the Organization component is enabled on the appliance, log in to the appliance System Administration Console, `https://appliance_hostname/system`, or select System in the drop-down list in the top-right corner of the page, then select Settings > Control Panel.**
2. In the *Security Settings* section, click **Security Options** to display the *Security Settings* page.
3. In the *Security Options* tab, select the *Enable API Access* check box.
4. Select the *Enable mobile device access* check box.
5. Download the KACE GO app.
   a. Click **Get Mobile App**.

      A dialog box appears, allowing you to download KACE GO. The app is available for iOS and Android platforms from their respective app stores.

      TIP: You can also access this dialog box from the help pane. For more information, see Access product documentation.

   b. Click the link for your mobile device OS, as needed, to download the app.

      For more information about downloading and configuring KACE GO, see Download and use KACE GO.
6. Click **Save**.

   Mobile Device Access is enabled on the appliance. Before users can access the appliance using the KACE GO app, however, you must enable Mobile Device Access for their accounts. See Enable Mobile Device Access for users.

   If the Organization component is enabled on your appliance, enable Mobile Device Access for user accounts at the Organization or Admin level. Mobile Device Access cannot be enabled or disabled for user accounts at the System level.

Enable Mobile Device Access for users

After you enable Mobile Device Access for the appliance, you must enable access for users. If the Organization component is enabled on your appliance, you enable access for users in each organization separately.

1. Go to the *User Detail* page:

a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
b. On the left navigation bar, click **Settings**, then click **Users**.
c. Click the name of a user.

2. Select the **Mobile Device Access** check box.

TIP: If the Mobile Device Access check box is not displayed, verify that Mobile Device Access is enabled for the appliance.

3. Click **Save**.
4. To enable Mobile Device Access for multiple users:
   a. Select the check boxes for the users on the *Users* page.
   b. Select **Choose Action** > **Mobile Device Access** > **Enable**.

Mobile Device Access is enabled.

Related topics

Enable Mobile Device Access for the appliance

The selected users can download the KACE GO app from the Apple App Store or from Google Play.

Download and use KACE GO

You can download KACE GO to your smart phone or tablet from the Apple App Store for iOS devices, or from the Google Play store for Android devices.

1. On your mobile device, go to the Apple App Store or Google Play, and search for **KACEGO**.
2. Download and start the app.
3. If prompted, choose whether to enable Push Notifications.

When Push Notifications are enabled, the app sends notifications for Service Desk tickets to the mobile device. These notifications are based on the Service Desk Email on Events configuration.

4. Provide the following information and choose initial settings:

Option	Description
Appliance URL	The IP address or fully qualified domain name of the appliance.
User name and Password	The username and password of an account that has Mobile Device Access enabled.
Save Password	Enable the app to remember your password on the device. If you choose this option, Quest requires that you create a PIN (personal identification number) for security. KACE GO does not cache or save user data unless you select **Save Password**.
Use SSL	Enable SSL communications between the device and the appliance. To use this setting, SSL must be enabled on the appliance. If SSL is not enabled on the appliance, and you select **Use SSL**, the login fails.

For more information, see the Help Center in the KACE GO app or go to https://quest.com/products/kace-systems-management-appliance/.

Related topics

Configure email triggers

Disable Mobile Device Access on the appliance

To prevent all users from accessing the appliance using KACE GO, you can disable Mobile Device Access at the appliance or System level.

1. Go to the appliance *Control Panel*:
   - **If the Organization component is not enabled on the appliance, log in to the appliance Administrator Console, `https://appliance_hostname/admin`, then select Settings > Control Panel.**
   - **If the Organization component is enabled on the appliance, log in to the appliance System Administration Console, `https://appliance_hostname/system`, or select System in the drop-down list in the top-right corner of the page, then select Settings > Control Panel.**
2. In the *Security Settings* section, click **Security Options** to display the *Security Settings* page.
3. In the *Security Options* tab, clear the *Enable mobile device access* check box.
4. Click **Save and Restart Services**.

   KACE GO access is disabled for all users. Users who are currently logged in to the appliance using KACE GO are disconnected.

However, individual user settings are retained and reinstated if the feature is subsequently re-enabled on the appliance. For example, if Mobile Device Access was enabled for an account, and you re-enable Mobile Device Access on the appliance, Mobile Device Access is also re-enabled on the account.

Disable Mobile Device Access for users

To prevent selected users from accessing the appliance using KACE GO, you can disable Mobile Device Access at the user level.

1. Go to the *Users* list:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Settings**, then click **Users**.
2. Select the check boxes next to one or more users.
3. Select **Choose Action > Mobile Device Access > Disable**.

Mobile Device Access is disabled for the selected users. If the selected users are currently logged in to the appliance using KACE GO, they are disconnected.

Enable fast switching for organizations and linked appliances

Fast switching makes it possible to switch between interfaces without logging in to each item separately. On appliances with the Organization component enabled, these interfaces include **the Admin and System levels of the Administrator Console** the **User Console**, and linked K-Series appliances,

Fast switching is enabled by default on appliances without the Organization component enabled. In addition, the link to the **User Console** appears by default, provided that the logged-in user has permission to access both the **Administrator Console** and the **User Console**.

To appear in the drop-down list for fast switching, organizations must have the same **admin** account password; only those organizations whose **admin** account passwords match appear in the list. Linked appliances have similar requirements.

1. Go to the *General Settings* page:

a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.

b. On the left navigation bar, click **Settings**, then click **General Settings**.

2. Select the *Show organization menu in admin header* check box.

   NOTE: This setting is available only if the Organization component is enabled on your appliance.

3. **Optional**: Select the *Require organization selection at login* check box to require users to select an organization when they log in.

   NOTE: This setting is available only if the Organization component is enabled on your appliance.

4. Click **Save**.

   Changes are displayed on the login page and in the top section of the Administrator Console after you log out and then log in again. The drop-down list shows the available options.

Related topics

Linking Quest KACE appliances

Linking Quest KACE appliances

Appliance linking enables you to log in to one Quest KACE appliance and access all linked appliances from the **Administrator Console**.

Appliance linking enables you to log in to one appliance and access all linked appliances from the drop-down list in the top-right corner of the **Administrator Console**, without having to log in to each appliance separately. You can link all of the Quest KACE K-Series appliances you manage.

To link appliances you need to:

- Enable fast switching on each appliance that has the Organization component enabled. See Enable fast switching for organizations and linked appliances.
- Enable linking on each K-Series appliance. See Enable appliance linking.

When you enable linking, *Names* and *Keys* are created for each appliance. You then copy and paste the *Names* and *Keys* into the *Linked Appliance Detail* page for each appliance.

You can access multiple Quest KACE appliances from the same **Administrator Console**, but you cannot transfer resources or information among them through linking. See Importing and exporting appliance resources.

NOTE: If you have different types of Quest KACE appliances, and you plan to link them, the **admin** user account for each appliance must have the same password.

Enable appliance linking

You can enable appliance linking in the appliance or System-level General Settings. For KACE SDA instructions, see the Help for that appliance.

1. Go to the appliance *Control Panel*:
   - **If the Organization component is not enabled on the appliance, log in to the appliance Administrator Console, `https://appliance_hostname/admin`, then select Settings > Control Panel.**
   - **If the Organization component is enabled on the appliance, log in to the appliance System Administration Console, `https://appliance_hostname/system`, or select System in the drop-down list in the top-right corner of the page, then select Settings > Control Panel.**
2. Click **Enable appliance linking** under the **Link Settings** section to display the *Linked Appliance Enablement* page.
3. Select the **Enable Appliance Linking** check box.
4. Provide the following information:

Option	Description
Name	A unique, logical name for this appliance. This name appears in the drop-down list in the top-right corner of the page next to the login information when appliances are linked.
Login Expiration	The number of minutes to keep the link open. When this time period expires, you need to provide login credentials when switching to a linked appliance. The default is 120 minutes.
Timeout	The number of minutes the appliance waits for a remote appliance to respond to a linking request. The default is ten seconds.

5. Select the **Enable Federation API access settings** check box.

   NOTE: Enabling this option allows you to configure Federation API settings for linked appliances. For more information, see Enable access to Federation API settings.
6. Click **Save** to display appliance linking information.
7. Copy the text in the *Name* field and the text in the *Key* field and paste it in a central location, such as a Notepad file.
8. Repeat the preceding steps on each appliance you want to link.

When linking is enabled on all appliances, configure the links. See Add Names and Keys to appliances.

Add Names and Keys to appliances

To link Quest KACE appliances, add the appliance names and keys in the **Administrator Console**.

These instructions describe how to link KACE SMAs. For KACE SDA instructions, see the Help for that appliance.

Before you can link appliances, you need to enable linking on each appliance and copy the Name and Key of each appliance to a central location. See Enable appliance linking.

1. Go to the appliance *Control Panel*:
   - **If the Organization component is not enabled on the appliance, log in to the appliance Administrator Console, `https://appliance_hostname/admin`, then select Settings > Control Panel.**
   - **If the Organization component is enabled on the appliance, log in to the appliance System Administration Console, `https://appliance_hostname/system`, or select System in the drop-down list in the top-right corner of the page, then select Settings > Control Panel.**
2. Click **Manage existing links** under the **Linked Appliances** section to display the *Linked Appliances* page.

   NOTE: If appliance linking is not enabled, you are redirected to the *Linked Appliance Enablement* page.
3. On the *Linked Appliances* page, select **Choose Action > New** to display the *Linked Appliance Details* page.

   Or

   Click Enable appliance linking under the Linked Appliances section to display the *Linked Appliance Details* page.
4. In the *Hostname* field, paste the name of the appliance that you want to link.

   This is the name that you copied following the instructions in Enable appliance linking.
5. Select **Disable port 80 access** to use port 443 for secure communications. Communication over both port 80 and 443 are encrypted.
6. In the *Key* field, paste the key of the appliance that you want to link.

   This is the key that you copied following the instructions in Enable appliance linking.
7. Click **Save** to display the *Test Connection* button.
8. Click **Test Connection** to verify the connection between the two linked appliances.

   If the settings are configured correctly, the *Connection Successful* message appears.
9. Log in to the second appliance and repeat the preceding steps to add the first appliance's *Name* and *Key* to the second appliance.
10. Click **Save** to display the **Test Connection** button.
11. Click **Test Connection** to verify the connection between the two linked appliances.

    If the settings are configured correctly, the *Connection Successful* message appears.

When you re-log in to the appliance, the other linked appliances appear on the drop-down list in the top-right corner of the page next to the login information. To switch to an appliance, select its name in the drop-down list.

Enable access to Federation API settings

If your Environment uses Federated KACE SMAs, the Federation API Settings page allows you to enable API access for linked appliances.

The following options must be selected on the *Linked Appliance Enablement* page:

- **Enable Appliance Linking**
- **Enable Federation API access settings**

For more information, see Enable appliance linking.

1. Log in to the appliance Administrator Console , `http://`**appliance_hostname**`/admin`, then click **Settings**.
2. On the appliance *Control Panel*, click **Federation API Settings** to display the *Federation API Settings* page.
3. On the *Federation API Settings* page, select the **Enable access** check box.
4. In the *Remote Systems* area that appears, specify the level of access for each linked appliance, as required.

1. In the row containing the appliance whose role you want to configure, click the *Role* column, and select one of the following options: **Administrator**, **Read Only Administrator**, or **User Console**.
2. Click **Save**.

5. Click **Save** to display appliance linking information.

Disable appliance linking

If Quest KACE appliances have been linked, you can disable linking as needed. After appliance linking is disabled, you can continue to switch to, and control, other appliances until you log off.

NOTE: This section explains how to disable linking on the appliance. For KACE SDA instructions, see the Help for that appliance.

1. Go to the appliance *Control Panel*:
   - **If the Organization component is not enabled on the appliance, log in to the appliance Administrator Console, `https://appliance_hostname/admin`, then select Settings > Control Panel.**
   - **If the Organization component is enabled on the appliance, log in to the appliance System Administration Console, `https://appliance_hostname/system`, or select System in the drop-down list in the top-right corner of the page, then select Settings > Control Panel.**
2. Click **Link Settings** to display the *Linked Appliance Enablement* page.
3. Clear the *Enable Appliance Linking* check box.
4. Click **Save**.

Configuring history settings

You can configure (subscribe to) and view the history of changes made to settings, assets, and objects on the appliance.

About history settings

The appliance enables you to configure (subscribe to) and view the history of changes to settings, assets, and objects.

- **Settings**: Tracked items include general settings as well as settings for MIA devices, patch subscriptions, and user authentication, among others. See Managing settings history.
- **Assets**: Tracked items include devices, cost centers, departments, licenses, locations, applications, vendors, and user-created Asset Types. See Managing asset history.
- **Objects**: Tracked items include alerts, labels, patch schedules, Replication Shares, reports, scripts, and applications among others. See Managing object history.

This history includes the date the change was made, the user who was logged in when the change was made, and the nature of the change. This information can help in troubleshooting system management issues, and you can export this information in CSV (comma-separated value) or custom report format.

History lists are informational only. You cannot use history lists to revert to previous states or undo changes.

Managing settings history

You can configure (subscribe to) and view the history of changes made to settings. Configuration options differ, depending on whether the Organization component is enabled on your appliance.

- If the Organization component is not enabled: View all history lists and configuration settings under **Settings** > **History**. For instructions, see Configure settings history subscriptions for organizations.
- If the Organization component is enabled: View history lists and configuration settings for each organization, and for the System level, separately. For instructions, see .

Configure settings history subscriptions for organizations

You can configure settings history subscriptions for the appliance or, if the Organization component is enabled, for the selected organization.

1. Go to the *Settings History Configuration* page:
    a. Log in to the appliance System Administration Console, `http://`**appliance_hostname**`/system`, or select **System** from the drop-down list in the top-right corner of the page.
    b. On the left navigation bar, click **Settings**, then click **History**.
    c. In the *Subscriptions* section, click **Settings**.

    The options on this page differ, depending on whether the Organization component is enabled on your appliance. For appliances with the Organization component enabled, additional options are available at the System level.
2. In the drop-down list for history retention, select the length of time for changes to be retained by the appliance and to appear in the history list. Select **Forever** to keep all changes. Select **Disabled** to erase the existing history list and prevent the appliance from adding changes to the list.

    IMPORTANT: Setting history retention to very long periods, such as several months or *Forever*, might result in slower page loading for items in the *Inventory* section.
3. In the *Category and Field Selection* section, select the check boxes next to the settings you want to track; clear the check boxes next to the settings you do not want to track.
4. To select fields within a setting:
    a. With the check box for a setting selected, click the **Edit** button next to the setting: .

    The field selection dialog appears.
    b. Choose the fields whose history you want to track, then click **OK**.
5. Click **Save**.
6. **Optional**: If you have multiple organizations, repeat the preceding steps for each organization.

Related topics

Configure settings history subscriptions for organizations

You can configure settings history subscriptions for the appliance or, if the Organization component is enabled, for the selected organization.

1. Go to the *Settings History Configuration* page:
    a. Log in to the appliance System Administration Console, `http://`**appliance_hostname**`/system`, or select **System** from the drop-down list in the top-right corner of the page.
    b. On the left navigation bar, click **Settings**, then click **History**.
    c. In the *Subscriptions* section, click **Settings**.

The options on this page differ, depending on whether the Organization component is enabled on your appliance. For appliances with the Organization component enabled, additional options are available at the System level.

2. In the drop-down list for history retention, select the length of time for changes to be retained by the appliance and to appear in the history list. Select **Forever** to keep all changes. Select **Disabled** to erase the existing history list and prevent the appliance from adding changes to the list.

   IMPORTANT: Setting history retention to very long periods, such as several months or *Forever*, might result in slower page loading for items in the *Inventory* section.

3. In the *Category and Field Selection* section, select the check boxes next to the settings you want to track; clear the check boxes next to the settings you do not want to track.
4. To select fields within a setting:
   a. With the check box for a setting selected, click the **Edit** button next to the setting: .

      The field selection dialog appears.

   b. Choose the fields whose history you want to track, then click **OK**.
5. Click **Save**.
6. **Optional**: If you have multiple organizations, repeat the preceding steps for each organization.

Related topics

View settings history

If history subscriptions are configured to retain information, you can view the history of changes made to settings.

1. Go to the appliance *Control Panel*:
   - **If the Organization component is not enabled on the appliance, log in to the appliance Administrator Console, `https://appliance_hostname/admin`, then select Settings > Control Panel.**
   - **If the Organization component is enabled on the appliance, log in to the appliance System Administration Console, `https://appliance_hostname/system`, or select System in the drop-down list in the top-right corner of the page, then select Settings > Control Panel.**
2. Click *History*.
3. In the *Reporting* section, click **Settings** to display the *Settings History* page.
4. To filter the list, select **Type** or **User** in the *View By* drop-down list, which appears above the table on the right.

   The list is redisplayed and shows only those items that match the *Type* or *User* you selected.

Managing asset history

You can configure (subscribe to) and view the history of changes made to asset information such as devices, cost centers, departments, licenses, locations, applications, vendors and user-created Asset Types.

Configure asset history subscriptions

You can configure asset history subscriptions for the appliance or, if the Organization component is enabled, for the selected organization.

1. Go to the *Asset History Configuration* page:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Settings**, then click **History**.

c. On the *History Panel* in the Subscriptions section, click **Assets**.

2. In the drop-down list for history retention, select the length of time for changes to be retained by the appliance and to appear in the history list. Select **Forever** to keep all changes. Select **Disabled** to erase the existing history list and prevent the appliance from adding changes to the list.

IMPORTANT: Setting history retention to very long periods, such as several months or *Forever*, might result in slower page loading for items in the *Inventory* section.

3. In the *Asset Type and Field Selection* section, select the check boxes next to the Asset Types you want to track; clear the check boxes next to the Asset Types you do not want to track.
4. To select fields within an Asset Type:
   a. With the check box for an Asset Type selected, click the **Edit** button next to an Asset Type: .

      The field selection dialog appears.

   b. Choose the fields whose history you want to track, then click **OK**.
5. Click **Save**.
6. **Optional**: If you have multiple organizations, repeat the preceding steps for each organization.

View asset history

If history subscriptions are configured to retain information, you can view the history of changes made to assets.

1. Go to the *Asset History* list:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Settings**, then click **History**.
   c. On the *History Panel* in the Reporting section, click **Assets**.
2. To filter the list, select **Type** or **User** in the *View By* drop-down list, which appears above the table on the right.

The list is redisplayed and shows only those items that match the *Type* or *User* you selected.

Managing object history

You can configure (subscribe to) and view the history of changes made to objects such as labels, patch schedules, Replication Shares, users, and other objects.

Configure object history

You can configure object history subscriptions for the appliance or, if the Organization component is enabled, for the selected organization.

1. Go to the *Object History Configuration* page:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Settings**, then click **History**.
   c. On the *History Panel* in the *Subscriptions* section, click **Objects**.
2. In the drop-down list for history retention, select the length of time for changes to be retained by the appliance and to appear in the history list. Select **Forever** to keep all changes. Select **Disabled** to erase the existing history list and prevent the appliance from adding changes to the list.

IMPORTANT: Setting history retention to very long periods, such as several months or *Forever*, might result in slower page loading for items in the *Inventory* section.

3. In the *Object Type and Field Selection* section, select the check boxes next to the object types you want to track; clear the check boxes next to the object types you do not want to track.
4. To select fields within an object type:
   a. With the check box for an object type selected, click the **Edit** button next to the object type: .

   The field selection dialog appears.

   b. Choose the fields whose history you want to track, then click **OK**.
5. Click **Save**.
6. **Optional**: If you have multiple organizations, repeat the preceding steps for each organization.

View object history

If history subscriptions are configured to retain information, you can view the history of changes made to objects.

1. Go to the *Objects* page:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Settings**, then click **History**.
   c. On the *History Panel* in the *Reporting* section, click **Objects**.
2. To filter the list, select **Type** or **User** in the *View By* drop-down list, which appears above the table on the right.

The list is redisplayed and shows only those items that match the *Type* or *User* you selected.

Using change history information

You can view an item's change history, search for items in change history lists, delete history records, export history records, and create reports from history records.

View the change history of items

You can view an item's change history when you are viewing details about the item.

1. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
2. Go to the *Detail* page for an item. For example, click **Scripting**, then click the name of a script.
3. Click the **Show All History** link at the top of the page.

   Changes are listed. The page is empty if no changes have been made, or if change history is not enabled.

Search for items in change history lists

You can search for items in change history lists.

1. Go to the history listing for settings, assets, or objects:
   # View settings history
   # View asset history
   # View object history
2. Click the **Filter** tab above the list on the right to display the *Filter* panel.
3. Select search properties, then click **Search**.

The search results are displayed.

Delete history records

You can delete history records from history lists.

1. Go to the history list for settings, assets, or objects:
   # View settings history
   # View asset history
   # View object history
2. Select the check box next to one or more entries.
3. Select **Choose Action** > **Delete**, then click **Yes** to confirm.

Export history records

You can export history records to CSV, Excel, and TSV format.

1. Go to the history list for settings, assets, or objects:
   # View settings history
   # View asset history
   # View object history
2. **Optional**: To export items of a specific type, such as **Addition**, select the item type in the *View-By* drop-down list.

   If you do not filter the list, all list items are exported. Selecting an item's check box does not select the item for export.
3. Select **Choose Action** > **Export** > **format**.

Configuring Content Security Policy

The Content Security Policy (CSP) provides enhanced security measures within the System Manager Appliance (SMA) application.

The Content Security Policy (CSP) provides enhanced security measures within the System Manager Appliance (SMA) application. By enabling CSP, administrators can restrict the types of content the SMA accepts, mitigating potential security risks associated with malicious URLs and unauthorized access. By implementing CSP, system administrators can strengthen the security posture of the SMA deployments and protect sensitive data from unauthorized access.

NOTE: Configuring the CSP directives correctly is important to ensure the appliance operates as intended.

For more details, Enable Content Security Policy

Enable Content Security Policy

The Content Security Policy (CSP) provides enhanced security measures within the System Manager Appliance (SMA) application.

You need to enable the Content Security Policy to ensure compliance with security standards.

NOTE: The CSP tab is not disabled by default.

1. Go to the System-level *General Settings* page:
   - **Log in to the appliance System Administration Console, `http://appliance_hostname/system`, or select System from the drop-down list in the top-right corner of the page.**
   - **On the left navigation bar, click Settings, then click Control Panel.**
   - **On the , in the *Security Settings* section, click Configure network security and accessibility to open the *Security Settings* page.**
2. In the *CSP* tab, select the **Enable CSP** checkbox.

   NOTE: When enabling CSP, a list of KACE trusted domains is automatically added. These items are critical to the functionality of the KACE SMA appliance and are not configurable.
3. If you want to add domains or URLs in the list, then in the Additional Allowed Domains section, click + and specify information in the following fields:

Option	Description
Directive	Policy Directives dictate the type of content that is allowed. Select from the list of directives: • Default-src • Style-src • Script-src • Frame-src • Media-src • Worker-src • Font-src • Img-src
Domain/URL	the location of the content that is allowed for the directive.

4. Click **Save and Restart Services**.

The icons to the right of each row enable you to :

: Add a Directive

: Edit a Directive.

: Change the order of Directives.

: Delete a Directive.

Setting up and using labels to manage groups of items

You can set up manual labels, Smart Labels, LDAP Labels, and label groups to manage groups of items, such as devices.

About labels

Labels are containers that enable you to organize and categorize items, such as devices, so that you can manage them as a group.

For example, you can use labels to identify devices that have the same operating system or that are in the same geographic location. You can then initiate actions, such as distributing software or deploying patches, on all of the devices that in that label. Labels can either be manually assigned to specific items or automatically assigned to items when they are associated with criteria, such as SQL or LDAP queries. You can apply labels to these types of items:

- Inventory items, such as devices, applications, processes, startup items, and services
- Asset items, such as location, license, and vendor
- Discovery results
- Patches
- Dell Update Packages
- Users

Manual labels are applied and removed manually, whereas Smart Labels and LDAP Labels are applied and removed automatically. See:

- About Smart Labels
- About LDAP Labels

About Smart Labels

Smart Labels are labels that are applied and removed automatically based on specified criteria.

For example, to track or manage laptops in a specific location, such as the San Francisco office, you could create Smart Label named **San Francisco Office** based on the IP address range or subnet of devices in that location. When devices are inventoried, the Smart Label, **San Francisco Office** is automatically applied to devices in the IP address range. When devices leave the IP address range and are inventoried again, the label is automatically removed.

Smart Labels are applied to and removed from managed devices when the appliance processes device inventory. So if you create a Smart Label that enables metering on devices, it might take time for the Smart Label to be applied to devices and for devices to report metering information. Metering is enabled for devices that match the Smart Label criteria only after the appliance processes device inventory and the Smart Label is applied.

Related topics

Managing Smart Labels

About LDAP Labels

LDAP Labels are labels that interact with LDAP servers. These labels are automatically assigned to device and user records using LDAP queries or search filters.

There are two types of LDAP Labels:

- **Device**: Labels applied to device records. This is useful if you want to automatically group devices by name, description, and other LDAP criteria. Each time a device is inventoried, this query runs against the LDAP server. the *admin* value in the *Search Filter* field is replaced with the name of the user that is logged in to the device. If a result is returned, the device is assigned the label specified in the *Associated Label Name* field.
- **User**: Labels applied to user records. This is useful if you want to automatically group users by domain, location, budget code, or other LDAP criteria. LDAP Labels are applied to or removed from user records when users are imported to the appliance manually or according to a schedule.

Related topics

Managing LDAP Labels

About label groups

You can organize labels by assigning them to label groups. Label groups share their types with the labels they contain.

Not only can a label group include multiple labels, but a label can be associated with more than one label group. Labels inherit any restrictions of the groups to which they belong.

Related topics

Add, view, or edit label groups

About organization filters

Organization filters are similar to labels, but they serve a specific purpose: Organization filters automatically assign devices to organizations when devices are inventoried.

There are two types of organization filters:

- **Data Filters**: Assigns devices to organizations automatically based on search criteria. When devices are inventoried, they are assigned to the organization if they meet the criteria. This filter is similar to Smart Labels in that it assigns devices to organizations automatically if they match specified criteria.
- **LDAP Filters**: Assigns devices to organizations automatically based on LDAP or Active Directory interaction. When devices are inventoried, the query runs against the LDAP server. If devices meet the criteria, they are automatically assigned to the organization.

Related topics

Managing organization filters

Tracking changes to label settings

If History subscriptions are configured to retain information, you can view the details of the changes made to settings, assets, and objects.

This information includes the date the change was made and the user who made the change, which can be useful during troubleshooting.

Related topics

About history settings

Managing manual labels

You can manage labels from the *Label* section of the **Administrator Console**. Labels can also be added and applied from list pages in other sections, such as *Inventory* and *Security* by selecting **Choose Action** > **Add Label**.

Add or edit manual labels

You can add or edit manual labels as needed.

1. Go to the *Label Detail* page:

a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.

b. On the left navigation bar, in the **Home** section, click **Label Management**.

c. On the *Label Management* panel, click **New Manual Labels** link under the **Labels** section to display the *Labels* page.

Or

On the *Label Management* panel, click View and edit master list of labels under the Labels section to display the *Labels* page.

d. Display the *Label Detail* page by doing one of the following:

Click the name of a label.

Select **Choose Action** > **New** > **Manual Label**.

TIP: Avoid using backslashes (\) in label names. If you need to use a backslash in a label name, add a second backslash (\\) to escape it.

2. Provide the following information:

Option	Description
Name	The name of the label. This name appears on the Labels list.
Description	Any additional information you want to provide.
Alternate Location Path	(Optional) The alternate download location for Managed Installations, File Synchronizations, and other deployments that are performed on items assigned to this label. The location you specify replaces the string KACE_ALT_LOCATION. **CAUTION: You should not have a device in two labels that both specify a value in this field.**
Alternate Location Login	If you specify an alternate download location, specify the path to the location.
Alternate Location Password	If you specify an alternate download location, specify the username and password for the location.
Restrict Label Usage To	(Optional) The categories of items to which the label or label group can be applied. If you do not restrict label usage, the label or label group can be applied to any item. However, if you restrict the label or label group to categories such as Applications and Patches, that label or label group can be applied only to Applications and Patches; it cannot be applied to other items, such as Devices.
Meter Software Usage	Enable metering on devices that have the label assigned. This enables metering on the devices only. To meter software, you need to also enable metering for individual applications.
Allow Application Control	Enable Application Control on devices. Software marked as Not Allowed is prevented from running on devices to which the label is applied.
Restrict to Label Group	(Optional) The label group to which the label is assigned. To assign the label to a label group, click **Edit** next to the *Label Group* field, then select a label group. This is useful if you have a large number of labels and you want to organize them into sub-labels. For example, you could include the labels of your licensed applications in a

Option	Description
	group label named *Licenses*. In addition, labels inherit any restrictions of the groups to which they belong.
Scoped to User Role	The user role associated with this label. When a label is associated with a user role, the user actions are limited to only those devices, scripts, and schedules that are associated with that label. For more information about user roles, see Add or edit User Roles.

3. Click **Save**.

Related topics

Apply the Application Control label to devices

View manual label details

You can view manual label details, such as the members of a label, label usage restrictions, and alternate location information.

1. Go to the *Label Detail* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, in the **Home** section, click **Label Management**.
    c. On the *Label Management* panel, click **View and edit master list of labels** under the **Labels** section to display the *Labels* page.
2. To show or hide label groups, select **Show Label Groups** or **Hide Label Groups** in the *Choose Action* menu.
3. To view the members of a label, click a number in a column, such as *Devices*, *Users*, *Software*, and so on.
4. To view label details, click the linked name of a label.

    The *Label Detail* page appears.
5. In the *Labeled Items* section, click the **Add** button next to the section headers to expand or collapse the view: +.

Delete manual labels

Before you can delete a manual label, you must remove the label from any items to which it is applied. You cannot delete manual labels that are applied to any items.

In addition, if a manual label contains a Smart Label or an LDAP Label, you must delete the Smart Label or LDAP Label before you can delete the manual label. Manual labels cannot be deleted if they contain Smart Labels or LDAP Labels.

1. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
2. Remove the label from any items to which it has been applied. For example, to remove the label from devices:
    a. Click **Inventory**.

        The *Devices* page appears.
    b. In the *View By* drop-down list, select **Label** > **Label Name**.

        The *Devices* page shows the items to which the label is applied.
    c. Select all of the items in the list.
    d. Select **Choose Action** > **Remove Label** > **Label Name**.
3. After the label has been removed from all items, click **Home** > **Labels** > **Label Management**.

The *Labels* page appears.

4. Select the check boxes next to one or more labels.
5. Select **Choose Action** > **Delete**, then click **Yes** to confirm.

Managing Smart Labels

You can add Smart Labels for devices, applications on the Software page, patches, Discovery Results, and Dell Update packages.

Smart Labels cannot be created for applications on the *Software Catalog* page.

Add Smart Labels

You can add Smart Labels from the *Labels* section and from list pages where Smart Labels are used, such as the *Devices* list.

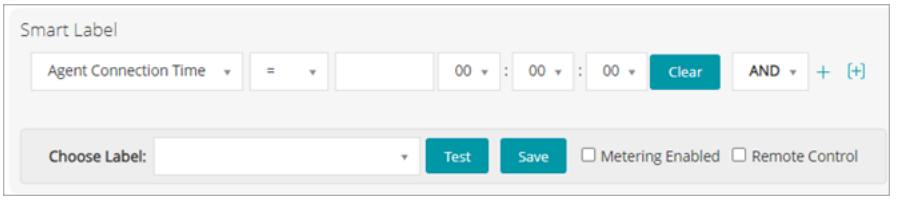
1. Go to the *Label Detail* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, in the **Home** section, click **Label Management**.
    c. On the *Label Management* panel, under the Smart **Labels** section, hover over the **New Smart Label link and click the** desired label criteria from the list to display the *Smart Labels* page.

    Or

    On the *Label Management* panel, click Automatic labeling based on advanced search criteria under the Labels section to display the *Smart Labels* page.

    d. Select **Choose Action** > **New** > **Smart Label type**.

    The appliance displays the *Smart Label* criteria for the type of label that you selected. For example, if you select New > Software Smart Label, the software criteria are displayed. If you select New > Device Smart Label, the *Devices* criteria are displayed.
2. Specify the search criteria using the available fields.
    # To add a row, click **Add line**.
    # To add a subset of rules, select **AND** or **OR** from the operator drop-down list at the right of the Smart Label criteria, then click **Add Group**.



3. Click **Test** to display items that match the specified criteria.
4. Adjust the criteria as needed until the results are what you expect.
5. In the *Choose label* drop-down list, do one of the following:
    - **Select an existing label to associate with the Smart Label. Type in the *Choose label* field to search for existing labels.**

NOTE: If you select a label group instead of a label, you will not be able to apply the Smart Label to a patching schedule. Patching schedules can only use Smart Labels based on a single item.

- **Enter a new name for the Smart Label in the *Choose label* field, then press Enter or Return.**

NOTE: Press **Enter** or **Return** after you enter a new Smart Label name to move the text from the search field to the label field.

6. Click **Save**.

Related topics

Labeling devices to group them

Using Smart Labels with Discovery Results

Example: Combine Smart Labels to identify devices

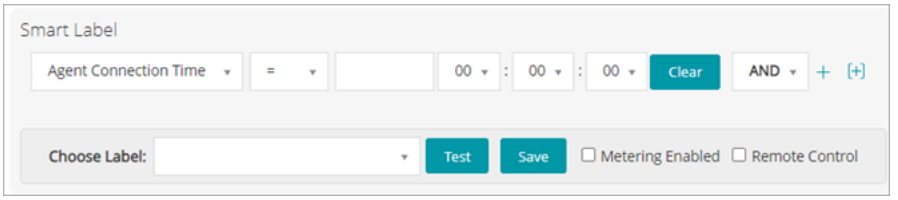
This example demonstrates how to combine three Smart Labels to identify devices running Windows 7 or Windows 8 that do not have the McAfee® VirusScan® application installed.

The following are the three Smart Labels created in this example:

- The first Smart Label, *Win78*, is applied to devices that have Windows 7 or Windows 8 operating systems. This label has a run order of 1.
- The second Smart Label, *MissingVirusScan*, is applied to devices that do not have the VirusScan application installed. This label also has a run order of 1.
- The third Smart Label, *Win78MissingVirusScan*, is applied to devices that have both the *Win78* and *MissingVirusScan* Smart Labels applied. This label has a run order of 2, so that it runs after the first two labels.

1. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
2. Create a device Smart Label to identify the operating system:
   a. On the left navigation bar, click **Inventory**, then click **Device**s.
   b. Click the **Smart Label** tab above the list on the right.

      The *Smart Label* panel appears.



   c. Specify the criteria required for the Windows 7 operating system:

      ```
      Operating System: Name | contains | Windows 7
      ```

   d. With **OR** selected in the operator drop-down list, click **Add Line**, then specify the criteria required for the Windows 8 operating system:

      ```
      Operating System: Name | contains | Windows 8
      ```

   e. In the *Choose label* drop-down list, type a name for the label, such as Win78, then click **Smart Label**.
3. Create a device Smart Label to find devices that are missing the VirusScan application:
   a. In the *Smart Label* panel on the *Devices* page, specify the criteria required to find devices that do not have the VirusScan application installed:

      ```
      Software: Software Titles | does not contain | VirusScan
      ```

b. In the *Choose label* drop-down list, type a name for the label, such as MissingVirusScan, then click **Smart Label**.

4. Create a device Smart Label that uses the Smart Labels created in the preceding steps.
5. Create a Smart Label for the application:
   a. In the *Smart Label* panel on the *Devices* page, specify the criteria to identify devices with the *Win78* Smart Label applied:

      ```
      Device Identity Information: Label Names | = | Win78
      ```

   b. With **AND** selected in the operator drop-down list, click **Add Line**, then specify the criteria to identify devices with the *MissingVirusScan* Smart Label applied:

      ```
      Device Identity Information: Label Names | = | MissingVirusScan
      ```

   c. In the *Choose label* drop-down list, type a name for the label, such as Win78MissingVirusScan, then click **Smart Label**.
6. Set the order in which to run the Smart Labels:
   a. On the left navigation bar, in the **Home** section, click **Label Management**.
   b. On the *Label Management* panel, click **Automatic labeling based on advanced search criteria** under the **Labels** section to display the *Smart Labels* page.
   c. Select **Choose Action** > **Order Labels** > **Device Smart Labels**.

      The *Order Device Smart Labels* **page appears.**

   d. Click the **Edit** button at the far right in the *Win78* label row: .
   e. In the *Order* column, type 1, then click **Save**.
   f. Click the **Edit** button at the far right in the *MissingVirusScan* label: .
   g. In the *Order* column, type 1, then click **Save**.
   h. Click the **Edit** button at the far right in the *Win78MissingVirusScan* label row: .
   i. In the *Order* column, type 2, then click **Save**.
   j. Click **Save** at the bottom of the list.

      The *Win78* **label and the** *MissingVirusScan* **label are set to run before the** *Win78MissingVirusScan* **label. This ensures that Windows 7 and 8 devices that are missing the VirusScan application are labeled before the** *Win78MissingVirusScan* **label runs.**

Edit Smart Labels

You can change the SQL queries used in Smart Labels as needed.

When you change the SQL query used for a software Smart Label, the Smart Label is applied to or removed from items immediately, based on whether the items meet the new criteria. Device Smart Labels are applied to or removed from devices when the device's inventory information is updated.

If you manually edit the SQL of a Smart Label, you can no longer edit the label using the Smart Label template. This is because the template cannot be used to edit custom SQL.

1. Go to the *Label Detail* page:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, in the **Home** section, click **Label Management**.
   c. On the *Label Management* panel, click **Automatic labeling based on advanced search criteria** under the **Labels** section to display the *Smart Labels* page.
   d. Click the name of a Smart Label, or click the **Edit** button to the left of the Smart Label name.

NOTE: If the SQL of the Smart Label has been edited manually, the *Edit* button is not displayed.

2. Do any of the following:
   - **Select or clear the *Enable Metering* check box to enable or disable metering for device Smart Labels.**
   - **Select or clear the *Remote Control* check box to enable or disable remote control for device Smart Labels.**
   - **In the *Assigned Label* field, select the label you want to associate with the Smart Label.**
   - **Click Details to go to the detail page for the assigned label.**
   - **If the Smart Label was created using the Smart Label template, and the SQL has not been edited manually, click the link next to *using the original editor*.**
   - **To edit the Smart Label SQL manually, click the link next to *using this editor*.**

     CAUTION: If you manually edit the SQL of a Smart Label, you can no longer edit the label using the Smart Label template. This is because the wizard cannot be used to edit custom SQL.
3. **Optional**: Click **Duplicate** to create a new Smart Label that uses the same SQL query.
4. Click **Save**.

NOTE: When you click **Duplicate** to create a label, you can assign it to a new label only.

Setting up labels for user accounts

You can use labels to group user accounts the same way you use labels to group devices and software in the *Inventory* section. In addition, you can use Smart Labels to grant levels of access to users. For example, you could use labels to designate who can submit, accept, reject, work on, and resolve Service Desk tickets.

Additionally, any labels you create in the *Inventory* section can work as user labels in Service Desk, provided that you created those labels without restrictions. If the labels were created with restrictions, you can modify them, or create labels in the *Inventory* sections without restrictions.

Add an All Ticket Owners label

To give users permission to own Service Desk tickets, you can create an All Ticket Owners label that you can apply to user accounts.

1. Go to the *Label Detail* page:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, in the **Home** section, click **Label Management**.
   c. On the *Label Management* panel, click **Automatic labeling based on advanced search criteria** under the **Labels** section to display the *Smart Labels* page.
   d. Select **Choose Action** > **New Manual Label**.

   TIP: Avoid using backslashes (\) in label names. If you need to use a backslash in a label name, add a second backslash (\\) to escape it.
2. Provide the following information:

Option	Description
Name	The name of the label. This name appears on the *Labels* list. Type a name such as All Ticket Owners.

Option	Description
Description	Any additional information you want to provide.

3. Click **Save**.

The new label is available in the **Choose Action** > **Apply Label** menu on the *Users* page. To assign the label to Service Desk staff when you import user data, see Importing users from an LDAP server.

Using Smart Labels for patching

You can use Smart Labels to automatically group patches and devices. You can also label patches and devices manually, but Smart Labels are usually more efficient because they are applied and removed automatically.

For example, you can create a Smart Label that matches all Windows 7 patches. Each time one of these patches becomes available to the appliance, the label is applied to the patch. If you set up a patching schedule to automatically detect and deploy devices with this label, the patch is automatically deployed to Windows 7 machines in inventory.

You can create a labeling scheme that organizes patches by operating system and importance, such as **P (Patch) Operating System Importance**. For example:

- P Win7
- P Win7 Critical
- P Win7 Important
- P MS Office
- P Leopard
- P Mac10.8 Critical Test

Similarly, you create device Smart Labels to specify the devices (D), on which you want to install patches:

- D All Desktops
- D All Servers
- D All Laptops

The appliance evaluates the information provided by the Agents when they check in, and it applies device Smart Labels if the data matches the label criteria.

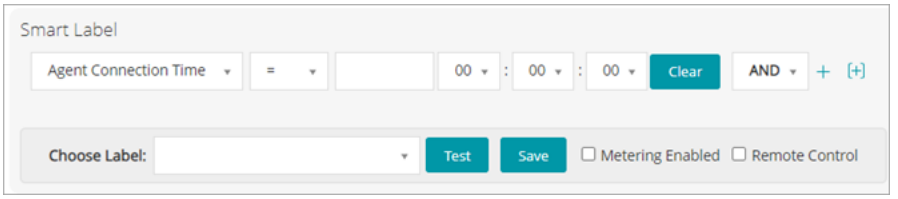
Patch Smart Labels are immediately applied to existing patches that meet the criteria. The label is added to new patches that meet the criteria when they are downloaded.

Add a Smart Label for critical OS patches

You can create a Smart Label to identify critical OS (operating system) patches.

1. Go to the *Patch Catalog* list:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Security**, then click **Patch Management**.
    c. On the *Patch Management* panel, click **Display available patches** under the **Catalogue** section to display the *Patch Catalog* page.
2. Click the **Smart Label** tab above the list on the right.

    The *Smart Label* panel appears.



3. Specify Smart Label criteria:
    a. Specify criteria that identify active patches:

        `Patch Listing Information: Status | is | Active`

    b. Click **Add Line**, then specify criteria that identify critical patches:

        `AND | Patch Listing Information: Severity | is | Critical`

    c. Click **Add Line**, then specify criteria that identify Windows patches:

        `AND | Patch Listing Information: Operating System | is | Windows`

    d. Click **Add Line**, then specify criteria that identify operating system patches:

        `AND | Patch Listing Information: Category | is | OS`
4. Click **Test** to display items that match the search criteria.
5. Adjust the criteria as needed until the results are what you expect.
6. In the *Choose label* drop-down list, do one of the following:
    - **Select an existing label to associate with the Smart Label. Type in the *Choose label* field to search for existing labels.**

        NOTE: If you select a label group instead of a label, you will not be able to apply the Smart Label to a patching schedule. Patching schedules can only use Smart Labels based on a single item.
    - **Enter a new name for the Smart Label in the *Choose label* field, then press Enter or Return.**

    NOTE: Press **Enter** or **Return** after you enter a new Smart Label name to move the text from the search field to the label field.
7. Click **Save**.

The Smart Label is applied to existing patches that meet the criteria. The label is added to new patches that meet the criteria when they are downloaded.

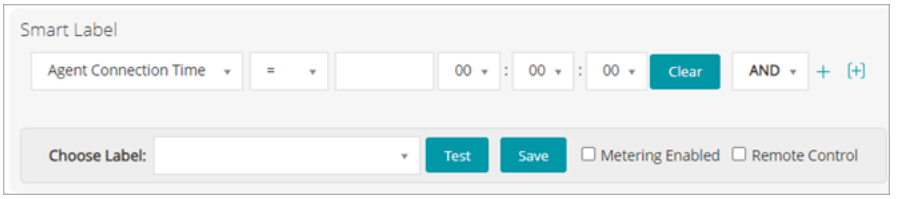
Subscribe to patches. See Subscribing to and downloading patches.

Add a Smart Label for new patches

You can create a Smart Label to quickly identify new patches that must be deployed.

1. Go to the *Patch Catalog* list:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Security**, then click **Patch Management**.
    c. On the *Patch Management* panel, click **Display available patches** under the **Catalogue** section to display the *Patch Catalog* page.
2. Click the **Smart Label** tab above the list on the right.

    The *Smart Label* panel appears.



3. Specify Smart Label criteria:
   a. Specify criteria that identify patches added after a specific date:

      ```
      Patch Listing Information: Release Date | > <date yyyy-mm-dd>
      ```

   b. Click **Add Line**, then specify criteria that identify non-critical patches:

      ```
      AND | Patch Listing Information: Impact | is not | Critical
      ```

   c. Click **Add Line**, then specify criteria that identify active patches:

      ```
      AND | Patch Listing Information: Status | is | Active
      ```

4. Click **Test**.

   All non-critical patches added after the specified date are displayed.

5. In the *Choose label* drop-down list, do one of the following:

   - **Select an existing label to associate with the Smart Label. Type in the *Choose label* field to search for existing labels.**

     NOTE: If you select a label group instead of a label, you will not be able to apply the Smart Label to a patching schedule. Patching schedules can only use Smart Labels based on a single item.

   - **Enter a new name for the Smart Label in the *Choose label* field, then press Enter or Return.**

   NOTE: Press **Enter** or **Return** after you enter a new Smart Label name to move the text from the search field to the label field.

6. Click **Save**.

   The Smart Label is applied to existing patches that meet the criteria. The label is added to new patches that meet the criteria when they are downloaded.

Subscribe to patches. See Subscribing to and downloading patches.

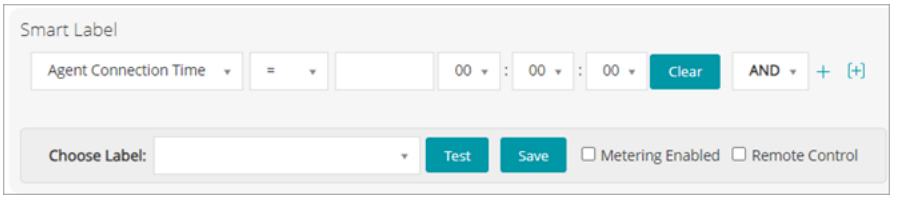
Using Smart Labels with Discovery Results

Smart Labels can be used to automatically assign labels to Discovery Results that meet specified criteria. This includes DNS, Socket, and SNMP results across a single subnet or multiple subnets.

Add Discovery Results Smart Labels

You can add Smart Labels for Discovery Results to group and manage results.

1. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
2. Select **Inventory** > **Discovery Results** to display the *Discovery Results* page.
3. Click the **Smart Label** tab above the list on the right to display the *Smart Label* panel.



4. Select Smart Label criteria:
   - **Select an attribute in the left-most drop-down list. For example: Device Info: Ping Test.**
   - **Select a condition in the middle drop-down list. For example: has.**
   - **Select the status attribute in the next drop-down list. For example: Failed.**
5. Click **Test** to display items that match the search criteria.
6. Adjust the criteria as needed until the results are what you expect.
7. In the *Choose label* drop-down list, do one of the following:
   - **Select an existing label to associate with the Smart Label. Type in the *Choose label* field to search for existing labels.**

     NOTE: If you select a label group instead of a label, you will not be able to apply the Smart Label to a patching schedule. Patching schedules can only use Smart Labels based on a single item.
   - **Enter a new name for the Smart Label in the *Choose label* field, then press Enter or Return.**

   NOTE: Press **Enter** or **Return** after you enter a new Smart Label name to move the text from the search field to the label field.
8. Click **Save**.

The Smart Label is automatically applied to or removed from Discovery Results that meet the specified criteria. The next time the Discovery Schedule runs, the Smart Label is applied to discovered devices.

Changing the run order of Discovery Results Smart Labels

You can specify the order in which Smart Labels run by changing their order values.

Smart Labels have a default order value of 100, and Smart Labels with lower values run before those with higher values. See Assign the Smart Label run order.

Adding Smart Labels for devices

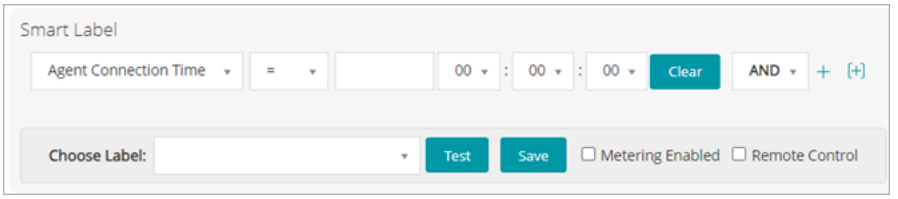
You can create Smart Labels to organize devices by type, such as desktop, server, and laptop. After you create Smart Labels for devices, you can schedule patches to be deployed to devices based on their labels.

Add a Smart Label for desktops

You can create a Smart Label to identify devices that require desktop patches.

1. Go to the *Devices* list:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Inventory**, then click **Device**s.
2. Click the **Smart Label** tab above the list on the right.

   The *Smart Label* panel appears.



3. Specify Smart Label criteria:
    a. Specify the criteria required to eliminate servers:

        ```
        Operating System: Name | does not contain | Server
        ```

    b. Click **Add Line**, then specify the criteria required to eliminate laptops:

        ```
        AND | Manufacturer and BIOS info: Chassis Type | does not contain | Laptop
        ```

    Other useful criteria for identifying desktops include:

    # System Names, if you give all of your desktops a similar name.
    # System Models, such as all systems with **XPS** in the model name.
    # IP addresses, or partial IP addresses using the **contains** criteria.
    # BIOS Serial Numbers, or use the **Includes partial serial number** criteria. This is useful if you have purchased desktops with sequential numbers. For more information, contact your vendor.
    # Software Title, if desktops have a title in common.

4. Click **Test** to display items that match the search criteria.
5. In the *Choose label* drop-down list, do one of the following:

    - **Select an existing label to associate with the Smart Label. Type in the *Choose label* field to search for existing labels.**

        NOTE: If you select a label group instead of a label, you will not be able to apply the Smart Label to a patching schedule. Patching schedules can only use Smart Labels based on a single item.

    - **Enter a new name for the Smart Label in the *Choose label* field, then press Enter or Return.**

    NOTE: Press **Enter** or **Return** after you enter a new Smart Label name to move the text from the search field to the label field.

6. Click **Save** to create the Smart Label.
7. **Optional**: To confirm that the new label appears on the *Labels* list, select **Home** > **Labels** > **Smart Labels** or **Label Management**.

    The new label appears empty at first. When devices are inventoried, the label is applied to them if they match the Smart Label criteria.

8. Test the Smart Label:
    a. Click **Inventory** > **Devices** to display the *Devices* page.
    b. Click the name of a device that matches the criteria, but to which the label has not yet been applied.
    c. On the *Device Detail* page, click **Force Inventory**.

        If the Smart Label is working correctly, the device checks in, and the label is applied to it.

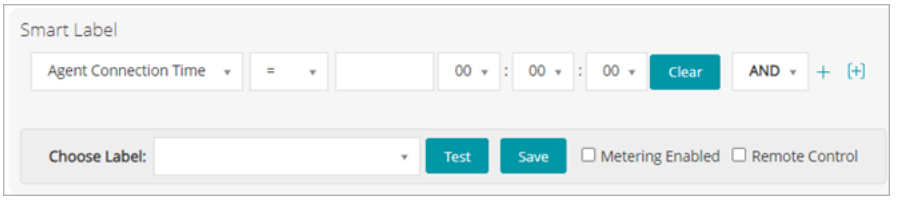
    Force Inventory is available only if the agent messaging protocol connection to an Agent-managed device is active, or for Agentless devices, if the device is reachable.

Add a Smart Label for servers

You can create a Smart Label to identify devices that require server patches.

1. Go to the *Devices* list:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Inventory**, then click **Device**s.
2. Click the **Smart Label** tab above the list on the right.

    The *Smart Label* panel appears.



3. Specify search criteria:
    a. Specify the criteria required to identify servers:

        `Operating System: Name | contains | Server`

    b. Click **Add Line**, then specify the criteria required to eliminate laptops:

        `AND | Manufacturer and BIOS info: Chassis Type | does not contain | Laptop`

    Other useful criteria for identifying servers include:

    # System Names, if you give all of your servers a similar name.
    # IP addresses, or partial IP addresses using the **contains** criteria.
    # BIOS Serial Numbers, or use the **Includes partial serial number** criteria. This is useful if you have purchased servers with sequential numbers. For more information, contact your vendor.
    # Software Title, if servers have a title in common.
4. Click **Test** to display items that match the search criteria.
5. In the *Choose label* drop-down list, do one of the following:

    - **Select an existing label to associate with the Smart Label. Type in the *Choose label* field to search for existing labels.**

        NOTE: If you select a label group instead of a label, you will not be able to apply the Smart Label to a patching schedule. Patching schedules can only use Smart Labels based on a single item.

    - **Enter a new name for the Smart Label in the *Choose label* field, then press Enter or Return.**

    NOTE: Press **Enter** or **Return** after you enter a new Smart Label name to move the text from the search field to the label field.
6. Click **Save**.
7. **Optional**: To confirm that the new label appears on the *Labels* list, select **Home** > **Labels** > **Smart Labels** or **Label Management**.

    The new label appears empty at first. When devices are inventoried, the label is applied to them if they match the Smart Label criteria.
8. Test the Smart Label:
    a. Click **Inventory** > **Devices** to display the *Devices* page.

b. Click the name of a device that matches the criteria, but to which the label has not yet been applied.

c. On the *Device Detail* page, click **Force Inventory**.

If the Smart Label is working correctly, the device checks in, and the label is applied to it.

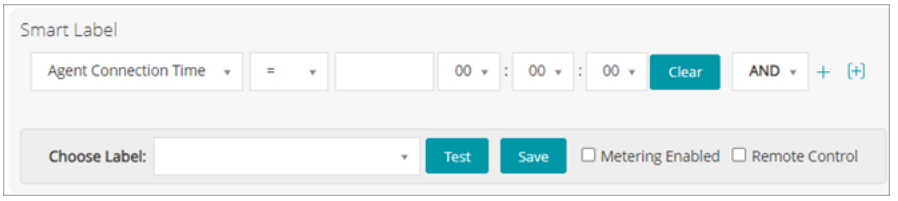
Force Inventory is available only if the agent messaging protocol connection to an Agent-managed device is active, or for Agentless devices, if the device is reachable.

Add a Smart Label for laptops

You can create a Smart Label to identify devices that require laptop patches.

1. Go to the *Devices* list:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Inventory**, then click **Device**s.
2. Click the **Smart Label** tab above the list on the right.

   The *Smart Label* panel appears.



3. Specify search criteria:
   a. Specify the criteria required to eliminate servers:

      `Operating System: Name | does not contain | Server`

   b. Click **Add Line**, then specify the criteria required to identify laptops:

      `AND | Manufacturer and BIOS Info: Chassis Type | contains | Laptop`

   Other useful criteria for identifying laptops include:

   # System Names, if you give all of your laptops a similar name.
   # IP addresses, or partial IP addresses using the **contains** criteria.
   # BIOS Serial Numbers, or use the **Includes partial serial number** criteria. This is useful if you have purchased laptops with sequential numbers. For more information, contact your vendor.
   # Software Title, if laptops have a title in common.
4. Click **Test** to display items that match the search criteria.
5. In the *Choose label* drop-down list, do one of the following:

   - **Select an existing label to associate with the Smart Label. Type in the *Choose label* field to search for existing labels.**

     NOTE: If you select a label group instead of a label, you will not be able to apply the Smart Label to a patching schedule. Patching schedules can only use Smart Labels based on a single item.

   - **Enter a new name for the Smart Label in the *Choose label* field, then press Enter or Return.**

     NOTE: Press **Enter** or **Return** after you enter a new Smart Label name to move the text from the search field to the label field.
6. Click **Save** to create the Smart Label.
7. **Optional**: To confirm that the new label appears on the *Labels* list, select **Home** > **Labels** > **Smart Labels** or **Label Management**.

The new label appears empty at first. When devices are inventoried, the label is applied to them if they match the Smart Label criteria.

8. Test the Smart Label:
    a. Click **Inventory** > **Devices** to display the *Devices* page.
    b. Click the name of a device that matches the criteria, but to which the label has not yet been applied.
    c. On the *Device Detail* page, click **Force Inventory**.

    If the Smart Label is working correctly, the device checks in, and the label is applied to it.

    Force Inventory is available only if the agent messaging protocol connection to an Agent-managed device is active, or for Agentless devices, if the device is reachable.

Assign the Smart Label run order

You can run Smart Labels sequentially by assigning the run order in the Smart Label properties.

Assigning the Smart Label run order can be useful when you want to run a specific Smart Label before other Smart Labels. For example, you might have a Smart Label that identifies a set of devices. If you want to use a second Smart Label to further refine the set of devices based on the first label being applied, you could set the run order so that the first Smart Label runs before the second one. Smart Labels have a default order value of 100, and Smart Labels with lower values run before those with higher values.

1. Go to the *Smart Label* list:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, in the **Home** section, click **Label Management**.
    c. On the Label Management panel, click **Automatic labeling based on advanced search criteria** link under the **Smart Labels** section to display the *Smart Labels* page.
2. In the *Choose Action* menu, in the *Order* section, select the type of label whose run order you want to change.

    The *Order* page appears, showing all Smart Labels of the selected type.
3. To change a Smart Label's order value:
    a. Click the **Edit** button to the right of the *Order* column: .
    b. Enter an order value, then click **Save**.
4. Click **Save**.

Delete Smart Labels

Deleting Smart Label is useful if you need to make extensive changes to Smart Label criteria while preserving labels used in tasks such as Managed Installations.

For example, you could delete all the criteria from a Smart Label, then re-apply new criteria to the container label. In effect, this would create a new Smart Label using the existing container label required for Managed Installations.

Deleting a Smart Label removes the criteria associated with the Smart Label, but it does not delete any other labels associated with the Smart Label.

1. Go to the *Smart Label* list:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, in the **Home** section, click **Label Management**.

c. On the Label Management panel, click **Automatic labeling based on advanced search criteria** link under the **Smart Labels** section to display the *Smart Labels* page.

2. Select the check box next to one or more Smart Labels.
3. Select **Choose Action** > **Delete**, then click **Yes** to confirm.

Managing label groups

You manage label groups in the *Labels* section.

Add, view, or edit label groups

You can add, view, and edit label groups as needed.

1. Go to the *Label Group Detail* page:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, in the **Home** section, click **Label Management**.
   c. On the Label Management panel, click **View and edit master list of labels** link under the **Labels** section to display the *Labels* page.
   d. Display the *Label Group Detail* page by doing one of the following:

   # Click the name of a label group

   # Select **Choose Action** > **New Label Group**

2. Provide the following information:

Option	Description
Name	The name of the label group.
Description	Any additional information you want to provide.
Restrict Label Group Usage To	(Optional) The categories of items to which the label or label group can be applied. If you do not restrict label usage, the label or label group can be applied to any item. However, if you restrict the label or label group to categories such as Applications and Patches, that label or label group can be applied only to Applications and Patches; it cannot be applied to other items, such as Devices.
Meter Software Usage	Select or clear this check box to enable or disable metering for Device labels.
Allow Application Control	Enable Application Control on devices. Software marked as Not Allowed is prevented from running on devices to which the label is applied.
Label Group	(Optional) The label group to which the label is assigned. To assign the label to a label group, click **Edit** next to the *Label Group* field, then select a label group. This is useful if you have a large number of labels and you want to organize them into sub-labels. For example, you could include the labels of your licensed applications in a group label named *Licenses*. In addition, labels inherit any restrictions of the groups to which they belong.

3. Click **Save**.

Related topics

Apply the Application Control label to devices

Assign labels to or remove labels from label groups

Labels can be assigned to groups, and they can be associated with more than one label group. Labels inherit the restrictions of the groups to which they belong.

1. Go to the *Labels* list:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, in the **Home** section, click **Label Management**.
    c. On the Label Management panel, click **View and edit master list of labels** link under the **Labels** section to display the *Labels* page.
2. Select the check boxes next to the labels you want to assign to a group.
3. Select **Choose Action** > **Apply Label Groups**, then select the label group to which you want to assign the label.

    Apply Label Groups appears only if you have label groups on your appliance.

    The name of the label group appears next to the name of the label or labels you selected.
4. Select the check box next to the labels you want to remove from a group.
5. Select **Choose Action** > **Remove Label Groups**, then select the label group from which you want to remove the labels.

    Remove Label Groups appears only if you have label groups on your appliance.

    The name of the label group no longer appears next to the name of the label or labels you selected.

Delete label groups

You can delete label groups only if they do not contain any labels or subgroups.

If a label group contains labels or subgroups, you must remove them from the label group before you can delete the group.

1. Go to the *Labels* list:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, in the **Home** section, click **Label Management**.
    c. On the Label Management panel, click **View and edit master list of labels** link under the **Labels** section to display the *Labels* page.
2. If the label group does not contain any labels or subgroups:
    a. Select the check box next to the group's name
    b. Select **Choose Action** > **Delete**, then click **Yes** to confirm.

        The label group is removed.
3. If the group contains labels or subgroups:
    a. Click the name of the label group to display the *Label Group Detail* page.
    b. In the *Labeled Items* section toward the bottom of the page, click the **Add** button to expand the *Labels* section: .
    c. Click the name of a label or label group to display the detail page for that label or label group.
    d. In the *Label Group* field, click **Edit**.
    e. In the *Assign to Label Group* window, click the **Delete** button next to the label you want to remove: .
    f. Click **OK**, then click **Save**.

g. When you have removed all labels and subgroups from the label group, select the check box next to the label group's name on the *Labels* page.

h. Select **Choose Action** > **Delete**, then click **Yes** to confirm.

Managing LDAP Labels

You manage LDAP Labels in the *Labels* section.

Add or edit LDAP Labels

You can add and edit LDAP Labels as needed. Be sure to test LDAP Labels before you enable them.

1. Go to the *LDAP Label Detail* page:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, in the **Home** section, click **Label Management**.
   c. On the Label Management panel, click **New LDAP Label** link under the **LDAP Labels** section to display the *LDAP Label Detail* page.

      Or

      On the Label Management panel, click Automatic labeling based on LDAP or Active Directory lookup link under the LDAP Labels section to display the *LDAP Labels* **page.**

   d. Display the *LDAP Label Detail* page by doing one of the following:

   # Click the name of an LDAP label.

   # Select **Choose Action** > **New**.

2. Provide the following information:

Option	Description
Enabled	Enable the appliance to run the LDAP Label. **NOTE:** Select the *Enabled* check box only after you have tested the LDAP Label to verify that the LDAP criteria is correct and labels are applied as expected.
Type	The LDAP Label type. There are two types of LDAP Labels: • **Device**: Labels applied to device records. This is useful if you want to automatically group devices by name, description, and other LDAP criteria. When devices are inventoried, this query runs against the LDAP server to determine whether any devices contain LDAP attributes with values that correspond to the LDAP search filter criteria. If a result is returned, the device is assigned the label specified in the *Associated Label Name* field. You must include at least one appliance variable, such as `KBOX_COMPUTER_NAME`, in device labels for the LDAP label to be applied to a device. During LDAP label processing, the variable is used to compare an attribute's value in the LDAP directory to determine whether relationships exists between the LDAP object and an appliance object. See LDAP variables. • **User**: Labels applied to user records. This is useful if you want to automatically group users by domain, location, budget code, or other LDAP criteria. LDAP Labels are applied to or removed from user records when users are imported to the appliance manually or according to a schedule. You can use user variables, such as

Option	Description
	KBOX_USER_NAME, in user labels. During LDAP label processing, the variable is used to compare an attribute's value in the LDAP directory to determine whether relationships exists between the LDAP object and an appliance object. See LDAP variables. **TIP:** To test a label, replace the KBOX_ variables with the appropriate values for your environment, then select **Test**.
Associated Label	The manual label, or container label, to associate with this LDAP Label. Each LDAP Label must have an associated label.
Associated Label Description	Notes from the label selected in the *Associated Label Name* field.
Server	The IP address or the hostname of the LDAP server. If the IP address is not valid, the appliance waits to timeout, resulting in login delays during LDAP authentication. **NOTE:** To connect through SSL, use an IP address or hostname. For example: ldaps://hostname.
Port	The LDAP port number, which is usually 389 (LDAP) or 636 (secure LDAP).

Base DN	The criteria used to search for accounts.
	
	This criteria specifies a location or container in the LDAP or Active Directory structure, and the criteria should include all the users that you want to authenticate. Enter the most specific combination of OUs, DCs, or CNs that match your criteria, ranging from left (most specific) to right (most general). For example, this path leads to the container with users that you need to authenticate:
	
	`OU=end_users,`
	
	`DC=company,DC=com.`

Advanced Search	The search filter. For example:
	
	`(&(sAMAccountName=KBOX_USER_NAME)`
	`(memberOf=CN=financial,DC=example,DC=com))`

Credentials	An LDAP credential of the account the appliance uses to log in to the LDAP server to read accounts. Select from the list or create a new LDAP credential. For more information about LDAP credentials, see Add and edit LDAP User/Password credentials.

If you are unsure of the *Base DN* and *Advanced Search* information, use the LDAP Browser. See Use the LDAP Browser.

NOTE: Negative search filters are formatted as follows: `(!(sAMAccountName=David))`. Any other format using negatives will result in an error.

3. Click the **Test** button to test the new label. Change the label parameters and test again as needed.
4. If the LDAP Label is ready to use, select the *Enabled* check box. Otherwise, save the label without enabling it.
5. Click **Save**.

Related topics

Use the LDAP Browser

Enable LDAP Labels

After you have added and tested an LDAP Label, you can enable it. Device LDAP Labels that are enabled run against the LDAP server when devices check in to the appliance. User LDAP Labels that are enabled run against the LDAP server when users are imported manually or imported according to a schedule.

Add and test an LDAP Label. See Add or edit LDAP Labels.

1. Go to the *LDAP Label Detail* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, in the **Home** section, click **Label Management**.
    c. On the Label Management panel, click **Automatic labeling based on LDAP or Active Directory lookup** link under the **LDAP Labels** section to display the *LDAP Labels* page.
    d. Click the name of an LDAP label.
2. Select the *Enabled* check box.
3. Click **Save**.

Delete LDAP Labels

Deleting an LDAP Label removes the criteria associated with the LDAP Label, but it does not delete any other labels associated with the LDAP Label.

1. Go to the *LDAP Label Detail* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, in the **Home** section, click **Label Management**.
    c. On the Label Management panel, click **LDAP Labels**.
2. Select the check box next to one or more LDAP Labels.
3. Select **Choose Action** > **Delete**, then click **Yes** to confirm.

Use the LDAP Browser

The LDAP Browser enables you to browse and search data located on an LDAP server, such as an Active Directory server.

To use the LDAP Browser, you must have the Bind DN and the LDAP password to log on to the LDAP server.

The LDAP Browser can be useful when you need to enter information in the *Search Base DN* and the *Search Filter* fields for LDAP queries.

1. Go to the *LDAP Browser*:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, in the **Home** section, click **Label Management**.
    c. On the *Label Management* panel, click **Tool to browse or search an LDAP server** link under the **LDAP Browser** section to display the *LDAP Browser* page.
2. Specify *LDAP Server* settings:

Option	Description
IP Address or Hostname	The IP address or the hostname of the LDAP server. If the IP address is not valid, the appliance waits to timeout, resulting in login delays during LDAP authentication.

Option	Description
	NOTE: To connect through SSL, use an IP address or hostname. For example: ldaps://hostname.
Port	The LDAP port number, which is usually 389 (LDAP) or 636 (secure LDAP).

Credentials	The credentials of the account the appliance uses to log in to the LDAP server to read accounts. For example:
	`LDAP Login:CN=service_account,CN=Users,`
	`DC=company,DC=com.`
	If user name and password are not provided, the tree lookup is not performed. Each LDAP Label can connect to a different LDAP or Active Directory server.

3. Click **Test**.

   Upon successful connection to the LDAP server, the Next button becomes active.

   If the operation fails, verify the following:

   # The IP address or hostname is correct.
   # The LDAP server is running.
   # The login credentials are correct.

4. Click **Next**.

   The *Narrow the Search* window appears.

5. Enter a search filter to limit the number of results displayed at the bottom of the screen.

Option	Description
LDAP EasySearch	Type a string that you want to search for.
Search on	Indicate if you want to search for indexed or non-indexed fields by selecting the appropriate option, as required.
Other attributes	Type a comma-separated list of Active Directory fields that you want to search for. **NOTE:** The search does not check if the specified fields actually exist in the Active Directory.

6. Click **Go**.

   The search results appear at the bottom of the screen, on the left panel.

7. Click a child node to view its attributes.

   The attributes appear in the right panel.

Configuring user accounts, LDAP authentication, and SSO

You can configure and manage user accounts, authenticate users with LDAP information, and enable single sign on (SSO) for users.

About user accounts and user authentication

User accounts can be created and managed on the appliance. Users who access the **Administrator Console** and **User Console** using these accounts are referred to as **locally authenticated**.

As an alternative to local authentication, you can set up external authentication through an external LDAP server. See Using an LDAP server for user authentication.

Types of locally authenticated user accounts include:

- **System-level user accounts**. Accounts that enable users to log in to the **System Administration Console** to manage appliance settings, such as the appliance host name and network settings. System-level user accounts include the default **admin** account for the appliance. These accounts also enable access to organization-level components (admiui) and the **User Console**. See Managing System-level user accounts.
- **Organization user accounts**. Accounts that enable users to log in to the **Administrator Console** Organization level (Administrator Console) to manage organization-specific components. These components may include Inventory, Assets, Distribution, Scripting, Security, Service Desk, and **User Console** depending on the user's role. See Managing organization user accounts.

About locale settings

Locale settings determine the language used for text in the interfaces. You can select locale settings for the **Command Line Console**, **Administrator Console**, and **User Console**.

See Configuring locale settings.

Managing System-level user accounts

System-level user accounts enable users to log in to the **System Administration Console** to manage appliance settings, such as the appliance host name and network settings. System-level user accounts authenticate users locally on the appliance.

To use an LDAP server for user authentication, see Using an LDAP server for user authentication.

NOTE: You cannot delete the default **admin** account. You can change the user name of the **admin** account or disable it on the appliance (LDAP or SAML configuration required). You can also change the **admin** account password. See Add or edit System-level user accounts. Additionally, if the Organization component is enabled on your appliance, or if you want to link multiple K-Series appliances, use caution when changing the login and password of the **admin** account. The **admin** account login names and passwords on all linked appliances and organizations must be the same if you want to switch among them using the drop-down list in the top-right corner of the **System Administration Console**. The drop-down list shows only those appliances and organizations whose **admin** account login names and passwords are the same.

NOTE: See Enable fast switching for organizations and linked appliances.

Add or edit System-level user accounts

You can add or edit System-level user accounts as needed. These accounts enable users to log in to the **System Administration Console** to manage appliance settings.

If the Organization component is enabled on your appliance, you can also add or edit organization-specific user accounts. See Managing organization user accounts.

NOTE: You cannot delete the default **admin** account. You can change the user name of the **admin** account or disable it on the appliance (LDAP or SAML configuration required). You can also change the **admin** account password. Additionally, if the Organization component is enabled on your appliance, or if you want to link multiple K-Series appliances, use caution when changing the login and password of the **admin** account. The **admin** account login names and passwords on all linked appliances and organizations must be the same if you want to switch among them using the drop-down list in the top-right corner of the **System Administration Console**. The drop-down list shows only those appliances and organizations whose **admin** account login names and passwords are the same.

NOTE: See Enable fast switching for organizations and linked appliances.

1. Go to the *Administrator Detail* page:
    a. Log in to the appliance System Administration Console, `http://`**appliance_hostname**`/system`, or select **System** from the drop-down list in the top-right corner of the page.
    b. On the left navigation bar, click **Settings**, then click **Administrators**.
    c. Display the *Administrator Detail* page by doing one of the following:
    # Click the name of an administrator
    # Select **Choose Action** > **New**.
2. Enter or change the user information.

Option	Description
Login	(Required) The name the user types in the *Login ID* field on the login page. If you are editing the default *admin* account, you can change the login name, however use caution when changing the login and password of the *admin* account. The *admin* account login names and passwords on all linked appliances and organizations must be the same if you want to switch between them using the drop-down list in the top-right corner of the **System Administration Console**. The drop-down list shows only those appliances and organizations whose *admin* account login names and passwords are the same.
Name	The user's full name.
Primary Email	The user's primary email address.
Additional Emails	Any additional email addresses associated with the user.
Domain	The Active Directory domain associated with the user.
Budget Code	The code of the financial department associated with the user.
Location	The name of the work site or building where the user is located.
Work Phone, Home Phone, Mobile Phone, and Pager Number	The user's telephone numbers.
Custom 1-4	Any additional information about the user or the user's account.
Password and Confirm Password	(Required) The password the user types when logging in. If the Organization component is enabled on your appliance, or if you want to link multiple K-Series appliances, use caution when changing the password of the **admin** account. **Admin** account passwords for the System-level, for organizations, and for linked appliances must be the same if you want to switch among them using the drop-

Option	Description
	down list in the top-right corner of the **Administrator Console**. The drop-down list shows only those organizations and appliances whose admin account passwords are the same.
Role	(Required) Roles are assigned to user accounts to control access to the **Administrator Console** and **User Console**. Default administrator roles include: • **Administrator**: This user can log in to and access all features in the **Administrator Console**. • **Read Only Administrator**: This user can log in but cannot modify any settings in the **Administrator Console**. You cannot change the role of the default admin account.
Make default	Select this option if you want the selected role to become the default role for new users.
Locale	The locale to use for the **Administrator Console** and **User Console** for the user. You cannot change the locale of the default admin account.

3. Click **Save**.

Manage appliance administrator email notifications

Quest notifies appliance administrators of security issues and sales and marketing opportunities using email. You can enable or disable the email notifications for System-level (appliance) administrator accounts.

Email notifications are available only to appliance administrator accounts. Notifications are not available to non-administrator users. If the Organization component is enabled on your appliance, notifications are not available to Admin-level administrator accounts in organizations.

1. Go to the *User Detail* page or the *Administrator Detail* page:

   To go the *User Detail* page:

   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Settings**, then click **Users**.
   c. Display the *User Detail* page by doing one of the following:
   # Click the name of a user.
   # Select **Choose Action** > **New**.

   To go the *Administrator Detail* page:

   a. Log in to the appliance System Administration Console, `http://`**appliance_hostname**`/system`, or select **System** from the drop-down list in the top-right corner of the page.
   b. On the left navigation bar, click **Settings**, then click **Administrators**.
   c. Display the *Administrator Detail* page by doing one of the following:
   # Click the name of an administrator
   # Select **Choose Action** > **New**.

2. Verify the user information, email address, and role.

NOTE: To enable notifications, the user must have an appliance administrator role.

3. Click **Save**.

Delete System-level user accounts

If the Organization component is enabled on your appliance, you can delete user accounts at the System level. This option is available only if the Organization component is enabled on the appliance.

If the Organization component is not enabled on your appliance, follow the instructions in Managing organization user accounts.

NOTE: You cannot delete the default *admin* account.

1. Go to the *Administrators* list:
    a. Log in to the appliance System Administration Console, `http://`**appliance_hostname**`/system`, or select **System** from the drop-down list in the top-right corner of the page.
    b. On the left navigation bar, click **Settings**, then click **Administrators**.
2. Select the check box next to one or more accounts.
3. Select **Choose Action** > **Delete**, then click **Yes** to confirm.

Managing organization user accounts

Organization user accounts provide the credentials that enable users to log in to the **Administrator Console** or **User Console** and access components based on the user role assigned to their account. You can add or edit user roles and user accounts as needed.

Organization user accounts authenticate users locally on the appliance. To use an LDAP server for user authentication, see Using an LDAP server for user authentication.

Add or edit User Roles

User Roles are assigned to user accounts to control access to the **Administrator Console** and **User Console**. You can add or edit User Roles as needed.

However, you cannot edit the predefined roles: Administrator, No Access, Read Only Administrator, and User.

If the Organization component is enabled on your appliance, the permissions available to User Roles depends on the Organization Role assigned to the organization. See Managing Organization Roles and User Roles.

1. Go to the *Role Detail* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Settings**, then click **Roles**.
    c. Display the *Role Detail* page by doing one of the following:
    # Click the name of a role.
    # Select **Choose Action** > **New**.
2. In the *Name* field, provide a name, such as Service Desk Staff.

    You cannot change the name of the predefined roles.
3. If you want this role to be a default role for new roles, select the **Default role for new users** check box.
4. In the *Description* field, provide a brief description of the role, such as Used for Service Desk Administrators.

This description appears on the *Roles* list. You cannot change the description of predefined roles.

5. Set the Administrator Console permissions.
    a. Under *Administrator Console Permissions*, click the **Expand All**.
    b. Set the permissions for each component, as applicable.
6. Set the User Console permissions.
    a. Under *End User Console Permissions*, click **User Console** to expand the list of permissions.
    b. Set the permissions for each component, as applicable.
7. Under *Device Scope*, specify the devices to which you want to grant full access with this role.

    Role-based user access allows administrators to restrict actions to users based on the devices associated with their user role. You can grant access to all devices with a user with a specific role (a *scoped user*), or only to selected devices that are associated with a label.

    TIP: Labels are containers that enable you to organize and categorize items, such as devices, so that you can manage them as a group. For more information about labels, see About labels.

    TIP: When a Smart Label is associated with a role, this is indicated on the *Smart Labels* list, in the *Name* column.

    # To grant access to all devices in the appliance or organization (as applicable), select **Scopes All Devices**.
    # To grant access only to devices associated with a specific label, click **Restrict to Labels**, and select a label, as required.
8. Click **Save**.

The *Roles* page appears. When a user who is assigned to the role logs in, the appliance component bar shows the available features.

Delete User Roles

You can delete User Roles provided that they are not assigned to any users and that they are not predefined User Roles. If the Organization component is enabled on your appliance, you delete User Roles for each organization separately.

NOTE: You cannot delete User Roles that are associated with one or more labels.

1. Go to the *Roles* list:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Settings**, then click **Roles**.
2. Select the check box next to one or more roles.
3. Select **Choose Action** > **Delete**, then click **Yes** to confirm.

Add or edit organization user accounts

You can add or edit user accounts at the organization level. If the Organization component is enabled on your appliance, you add and edit users accounts for each organization separately.

1. Go to the *User Detail* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Settings**, then click **Users**.

c. Display the *User Detail* page by doing one of the following:

Click the name of a user.

Select **Choose Action** > **New**.

NOTE: There can be a maximum of 50 organization in your system. Any attempts to create more organizations result in an error message.

2. Add or edit the following information:

Option	Description
Login	(Required) The name the user types in the *Login ID* field on the login page. If you are editing the default *admin* account, you can change the login name, however use caution when changing the login and password of the *admin* account. The *admin* account login names and passwords on all linked appliances and organizations must be the same if you want to switch between them using the drop-down list in the top-right corner of the **Administrator Console**. The drop-down list shows only those appliances and organizations whose *admin* account login names and passwords are the same.
Name	The user's full name.
Email	The user's primary email address.
Additional Emails	One or more additional emails the user has access to. Separate multiple entries with commas.
Domain	The Active Directory domain associated with the user.
Budget Code	The code of the financial department associated with the user.
Location	The name of the work site or building where the user is located. Click and select a location from the drop-down list that appears.
Work Phone, Home Phone, Mobile Phone, and Pager Number	The user's telephone numbers.
Custom 1-4	Any additional information about the user or the user's account.
Password and Confirm Password	(Required) The password the user types when logging in.

Option	Description
Role	(Required) The role associated with the user. Roles are assigned to user accounts to control access to the **Administrator Console** and **User Console**. Default system roles include: • **Administrator**: This user can log in to and access all features in the **Administrator Console**. • **Read Only Administrator**: This user can log in but cannot modify any settings in the **Administrator Console**. • **Administrator Console only**: This user can log in to the **Administrator Console** only. • **No Access**: The user cannot log in to the **Administrator Console** or the **User Console**. You cannot change the role of the default admin account.
Locale	The locale that is displayed when the user logs in to the **Administrator Console** or the **User Console**.
Assign To Label	The label associated with the user.
Default Queue	The queue used as the default for Service Desk tickets submitted by the user.
Mobile Device Access	Enable or disable Mobile Device Access for the user. Mobile device access enables you to interact with the appliance using the KACE GO app on iOS and Android smart phones and tablets. Administrators can use the app to access Service Desk, inventory, and application deployment features. **NOTE:** This field is available when mobile device access is enabled on the appliance. See Configuring Mobile Device Access.
Service Desk Tickets	(Read only) Links to tickets created by the user.
Associated Assets	(Read only) Assets assigned to the user. For each user, the list shows the asset name, its type (for example, Software or Device), and the asset subtype (if applicable). You can sort the list by any column heading, as needed.
Assigned Devices	Devices assigned to the user. For each user, the list shows the device name, its subtype (if applicable), and an indication of whether a device is a primary user's device. You can sort the list by any column heading, as needed. To assign a device to a user, click +, and select an asset. If you choose a device that is already assigned to another user, the ownership of that device shifts to this user. The first device assigned to the user becomes the primary device by default. When multiple devices are assigned to a user, any device can be set as a primary device.

3. Click **Save**.

Related topics

Add or edit User Roles

Configuring locale settings

About labels

Customize user details

You can modify the custom fields available in user accounts as needed.

Every user account comes with a set of custom fields. You can edit these fields so that they can contain meaningful user-specific information, such as their badge number.

1. Go to the *User Detail* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Settings**, then click **Users**.
    c. Select **Choose Action** > **Customize User Fields** to display the *User Custom Fields* page.
2. On the *User Detail* page, click *Customize Additional Fields*.

    The *User Custom Fields* **page appears.**
3. For each custom field, you can specify the following information:

Option	Description
Field Name	The name of the custom field.
Required	An indicator of whether the field is required.
Default Value	The default value.

4. Manage the collection of custom fields, as needed, using the available controls.
5. Click **Save**.

Archive user accounts

When users are removed from your system, you have an option to archive their accounts prior to deleting them.

In order to archive user accounts, user archival must be enabled on the *General Settings* page. For more information, see Configure Admin-level or organization-specific General Settings.

Archived user accounts are maintained on the appliance in read-only mode. You can delete them, as needed. If you archive a user account, and add it to appliance again, a new user account is created, while the archived account is maintained until being removed. For example, if an employee leaves the organization and its user account becomes archived, if they join the organization again, a new user account is created without any association with the archived account. Similarly, if you archive a user account on the appliance without updating your organization's Active Directory, an LDAP import results in a new user account, that is not associated with the previously archived user.

NOTE: When user archival is enabled, user accounts can only be deleted only if they are marked as archived.

1. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
2. On the left navigation bar, click **Settings** > **Users**.
3. Complete one of the following steps:
   - **On the *Users* list, select one or more user accounts that you want to archive and select Choose Action > Archive.**
   - **On the *Users* list, click the name of the user that you want to archive. On the *User Detail* page that appears, click Archive.**
4. In the dialog box that appears, click **Confirm**.

   The dialog box closes, and the *Users* list refreshes, indicating that the user is in the Archived state ( ).
5. If you want to review the details for an archived user, on the *Users* list, in the *Name* column, click the user name.

   The *User Details* page appears, showing the user details in read-only mode.

Next, you can delete archived user accounts, if needed.

View or edit user profiles

You can view general information about your user profile, and edit some settings, when needed.

The *User Profile* dialog box allows every user to quickly change their password, review the devices and assets assigned to them, and any Service Desk Tickets that they created. Users with administrative-level permissions can also edit some additional parameters, such as their name, email, manager, and locale. They can also quickly go to the *User Detail* page to review additional information about their account, and to make any changes, as needed.

For more information about editing user accounts using the *User Detail* page, see the following topics:

- Add or edit organization user accounts
- Add or edit System-level user accounts

1. Do one of the following:
   - **Log in to the appliance Administrator Console, `https://appliance_hostname/admin`, where appliance_hostname is the host name of your appliance. Or, if *Show organization menu in admin header* is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.**
   - **Log in to the appliance System Administration Console, `https://appliance_hostname/system`, where appliance_hostname is the host name of your appliance, or select System from the drop-down list in the top-right corner of the page.**
   - **Log in to the applianceUser Console, `https://appliance_hostname/user`, where appliance_hostname is the host name of your appliance, or select User Console from the drop-down list in the top-right corner of the page.**
2. From the drop-down list in the top-right corner of the page, select **Manage My Profile**.

   The *User Profile* dialog box appears.
3. Review and edit the information on the *User Profile* dialog box, as needed.

   NOTE: Users without administrative privileges can only update their passwords and view a limited set of information in this dialog box without making any additional changes or accessing the *User Detail* page.

Tab	Option	Description
Profile	**Login**	The name the user types in the *Login ID* field on the login page. **NOTE:** You cannot change the login of the default admin account.
	Name	The user's full name.
	Primary Email	The user's email address.
	Manager	The user's manager.
	Locale	The locale to use for the **Administrator Console** and **User Console** for the user.
Manage Password		The password the user types when logging in. If the Organization component is enabled on your appliance, or if you want to link multiple K-Series appliances, use caution when changing the password of the **admin** account. **Admin** account passwords for the System-level, for organizations, and for linked appliances must be the same if you want to switch among them using the drop-down list in the top-right corner. The drop-down list shows only those organizations and appliances whose admin account passwords are the same.
Devices	**Name**	The device name.
	Subtype	The Asset Subtype for this device, if one is assigned.
	Primary Device	Indicates if the device is the primary device for the selected user.
Assets	**Name**	The asset name.
	Type	The asset type.
	Subtype	The Asset Subtype for this device, if one is assigned.
Service Desk Tickets	**Number**	The number of the Service Desk ticket the user logged.
	Title	The title of the Service Desk ticket the user logged.

Tab	Option	Description
	Status	The status of the Service Desk ticket the user logged.

4. **Optional**. To access the *User Detail* page, in the top-left corner, click **View Full Profile**, and continue reviewing and editing the user profile on that page.

   NOTE: This link only appears if your account has administrative privileges.

5. To save your changes, click **Update**.

Using an LDAP server for user authentication

User authentication can be done locally, using accounts created on the appliance, or externally, using an LDAP server.

If you use external LDAP server authentication, the appliance accesses a directory service to authenticate users. This allows users to log in to the appliance **Administrator Console**, **User Console**, or **System Administration Console** using their domain username and password.

For information about adding user accounts to the appliance for local user authentication, see:

- About user accounts and user authentication
- Managing user accounts for organizations

About the login account on your LDAP server

To set up LDAP user authentication, you need to create a login account for the appliance on your LDAP server. The appliance uses this account to read and import user information from the LDAP server.

The account needs read-only access to the *Search Base DN* field on the LDAP server. The account does not need write access, because the appliance does not write to the LDAP server.

In addition, the account must have a password that never expires. Because the password never expires, make sure it is very secure. The user can change the password (that complies with the appropriate security requirements), however, the password must be updated on the appliance. You can give the account a username, such as KACE_Login, or you can attempt to connect to the LDAP server using an anonymous bind.

Configure and test LDAP user authentication

You can configure and test connections from the appliance to an external LDAP server.

1. Do one of the following:

   - **Log in to the appliance Administrator Console, `https://appliance_hostname/admin`. Or, if *Show organization menu in admin header* is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.**
   - **Log in to the appliance System Administration Console, `https://appliance_hostname/system`, or select System from the drop-down list in the top-right corner of the page.**

   The *Dashboard* or *System Dashboard* page appears.

2. Go to the Admin-level or System-Level *Authentication Settings* page:
   a. On the left navigation bar, click **Settings**, then click **Control Panel**.
   b. On the *Control Panel*, in the *User Authentication* section. click **Configure Trust with LDAP** (Administrator Console only), or **Configure Trust with LDAP** (System Administration Console only).
3. If you want to disable the local admin account, and you are logged in as an administrative-level user through LDAP or SAML, select **Configure Trust with LDAP**.

Disabling the built-in admin account does not affect a tether used by KACE Support, when required. For more information about this feature, see Enable a tether to Quest KACE Support.

4. Select the **LDAP Authentication** option:

Option	Description
Local Authentication	Enable local authentication (the default). If local authentication is enabled, the password is authenticated against the existing entries in the local database at **Settings** > **Users**.
LDAP Authentication	Enable external user authentication using an LDAP server or Active Directory server. If **LDAP Authentication** is enabled, the password is authenticated against the external LDAP server. For assistance with authentication, contact **Quest Support** at https://support.quest.com/contact-support.

5. Click the buttons next to the server names to perform the following actions:

Button	Action
	Schedule a user import for the server.
	Modify the server definition. For information about the fields in this section, see Table 5.
	Remove the server.
	Change the order of the server in the list of servers.

6. **Optional**: Click **New** to add an LDAP server. You can have more than one LDAP server configured.

NOTE: All servers must have a valid IP address or hostname. Otherwise, the operation times out, which results in login delays when using LDAP authentication.

7. To add a server, provide the following information:

Table 5. Server information

Option	Description
Name	The name you want to use to identify the server.
Host Name or IP Address	The IP address or the hostname of the LDAP server. If the IP address is not valid, the appliance waits to timeout, resulting in login delays during LDAP authentication. **NOTE:** To connect through SSL, use an IP address or hostname. For example: ldaps://hostname.
Port	The LDAP port number, which is usually 389 (LDAP) or 636 (secure LDAP).
Base DN	The criteria used to search for accounts. This criteria specifies a location or container in the LDAP or Active Directory structure, and the criteria should include all the users that you want to authenticate. Enter the most specific combination of OUs, DCs, or CNs that match your criteria, ranging from left (most specific) to right (most general). For example, this path leads to the container with users that you need to authenticate:

Option	Description
	`OU=end_users,DC=company,DC=com`. **NOTE:** Domain Users is a special group that is not added to the `memberof` attribute values. For Domain Users members, use this format: (primaryGroupId=513).
Advanced Search	The search filter. For example: `(&(sAMAccountName=KBOX_USERNAME)(memberOf=CN=financial,DC=example,DC=com))`
Login	The credentials of the account the appliance uses to log in to the LDAP server to read accounts. For example: `LDAP Login:CN=service_account,CN=Users,` `DC=company,DC=com`. If user name and password are not provided, the tree lookup is not performed. Each LDAP Label can connect to a different LDAP or Active Directory server.
Password	The password of the account the appliance uses to log in to the LDAP server.
Role	(Required) The user's role: • **Global Administrator**: The user can access the **System Administration Console**, and each organization's **Administrator Console** as an administrator with full read/write permissions. They must first log in to the **System Administration Console**, and then log in to the applicable organization account using the drop-down list in the top-right corner. • **Administrator**: The user can log in to and access all features of the **Administrator Console**, **User Console**, or **System Administration Console**. • **Read Only Administrator**: The user can log in, but cannot modify any settings in the **Administrator Console**, **User Console**, or **System Administration Console**. • **User Console Only**: The user can log in only to the **User Console** . This role is only available in the **Administrator Console**. • **No Access**: The user cannot log in to the **Administrator Console**, **System Administration Console** or **User Console**. **No Access** is the default role. **NOTE:** These roles are predefined and you cannot edit them. However, you can create and edit custom roles as needed.

NOTE: Record the search and filtering criteria you use for filling out this form. You use this same information to import user data, and later to schedule user import on a regular basis.

8. Click **Save**.
9. Test authentication on an external LDAP server as follows:
   a. Select the **LDAP Authentication**.
   b. Click the **Edit** button next to the server on which the user account you are testing is located .
   c. In the *Advanced Search:* box, replace **KBOX_USER** with the username to test. The syntax is `sAMAccountName=username`.
   d. Enter the user's password in the *Password for test* field.
   e. Click **Test**.

If the test is successful, the authentication setup is complete for this user, and other users in the same LDAP container.

Importing users from an LDAP server

You can import user information from LDAP servers to create user accounts on the appliance. This provides administrators, such as Service Desk staff, with a richer set of data to use when working with users.

There are two ways to import user information:

- **Manually:** See Import user information manually
- **According to a schedule:** See Import user information according to a schedule

NOTE: User information is overwritten each time users are imported to the appliance. Password information, however, is not imported. Users must enter their passwords each time they log in to the **Administrator Console** or **User Console**.

Import user information manually

You can import user information manually by specifying criteria to identify the users you want to import.

1. Go to the *Users* page:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Settings**, then click **Users**.
   c. Select **Choose Action** > **Import Users**.
2. Provide the following information:

   NOTE: Use the LDAP Browser to specify the *Search Base DN* and *Search Filter*. See Use the LDAP Browser.

Option	Description
Server	The IP address or the hostname of the LDAP server. If the IP address is not valid, the appliance waits to timeout, resulting in login delays during LDAP authentication. **NOTE:** To connect through SSL, use an IP address or hostname. For example: ldaps://hostname.
Port	The LDAP port number, which is usually 389 (LDAP) or 636 (secure LDAP).
Base DN	The criteria used to search for accounts. This criteria specifies a location or container in the LDAP or Active Directory structure, and the criteria should include all the users that you want to authenticate. Enter the most specific combination of OUs, DCs, or CNs that match your criteria, ranging from left (most specific) to right (most general). For example, this path leads to the container with users that you need to authenticate: `OU=end_users,DC=company,DC=com`. **NOTE:** Use the LDAP Browser to specify the Search Base DN and Search Filter. Use the LDAP Browser.
Advanced Search	The search filter. For example:

Option	Description
	`(&(sAMAccountName=KBOX_USERNAME)(memberOf=CN=financial,DC=example,DC=com))`

Login	The credentials of the account the appliance uses to log in to the LDAP server to read accounts. For example:
	`LDAP Login:CN=service_account,CN=Users,`
	`DC=company,DC=com.`
	If user name and password are not provided, the tree lookup is not performed. Each LDAP Label can connect to a different LDAP or Active Directory server.

Password	The password of the account the appliance uses to log in to the LDAP server.

3. Specify the LDAP attributes to import.

Option	Description
Attributes to retrieve	Specify the LDAP attributes to retrieve. For example: `sAMAccountName, objectguid, mail, memberof, displayname, sn, cn, userPrincipalName, name, description, manager` The LDAP attributes specified in this field can be mapped to appliance User attributes on the next page. If this field is blank, the appliance retrieves all LDAP attributes. Leaving this field blank increases the time required to import attributes and is not recommended. **IMPORTANT: To retrieve the manager object associated with the user, you must add the `manager` attribute to the list, and to specify this mapping in a later step.**
Label Attribute	Enter a label attribute. For example: `memberof`. This setting returns a list of groups this user is a member of. The union of all the label attributes forms the list of labels you can import. If the search filter contains both the label names and user names, the label attribute is not required.
Label Prefix	Enter the label prefix. For example: `ldap_` The label prefix is a string that is added to the beginning of all the labels.
Binary Attributes	Enter the binary attributes. For example: `objectsid`. Binary attributes indicates which attributes should be treated as binary for purposes of storage.
Maximum Number of Rows	Enter the maximum number of rows to retrieve. This limits the result set that is returned in the next step.
Debug Output	Select the check box to view the debug output.

4. Click **Next**.

   The *Define mapping between User attributes and LDAP attributes* page appears.

5. In the drop-down list next each attribute, select the value to use for appliance User attributes during import. Values in the drop-down list are the values specified in the ***Attributes to retrieve*** field on the previous page.

The following attribute mappings are required:

Option	Description
Ldap Uid	The identifier for the user. Recommended value: `objectguid`.
User Name	The name of the user. Recommended value: `name`.
Email	The email address for the user. Recommended value: `mail`.
Manager	The manager of the user. This mapping is mandatory only if you want to retrieve the manager information. Recommended value: `manager`. **IMPORTANT: To retrieve the manager object associated with the user, you must also add the `manager` attribute to the *Attributes to retrieve* box.**

The following attribute mappings are not required, but they are recommended:

Option	Description
Api Enabled	Whether users are enabled to access the appliance using the KACE GO app. Access is enabled if the field contains a numerical value. Access is disabled if the field contains no value. Therefore, to enable access, select an attribute that returns a numerical value. To disable access, select **No Value**.
Ams Id	Not used. Recommended value: **No Value**.

6. **Optional**: In the *Role* drop-down list, select the role for the imported users. See Add or edit User Roles.
7. **Optional**: In the *Labels* drop-down list, select the label to apply to imported users. See About labels.
8. In the *Search Results* section below the attribute mapping drop-down lists, verify that the list of users to import is correct, and the information listed for each user is what you expect. To refine your search, click the **Back** button and revise the search parameters and attributes.

   For example, to change the number of *Search Results*, change the *Maximum Number of Rows* on the *Choose attributes to import* page.
9. Click **Next** to display the *Import Data into the appliance* page.
10. Review the tables of users to ensure that the data is valid and includes the data that you expect.

    Only users with values for the required attributes, *Ldap Uid*, *User Name*, *Email*, and *Manager* are imported. Records that do not have these values are listed in the *Users with invalid data* section.
11. Click **Import Now** to start the import.

The *Users* page appears, and the imported users appear on the list. The imported users can access the features of the **Administrator Console**, **User Console** based on the role to which they are assigned.

Import user information according to a schedule

To keep user data current, schedule regular user data imports from your LDAP server.

1. Go to the Admin-level *Authentication Settings* page:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Settings**, then click **Control Panel**.
   c. On the *Control Panel*, in the *User Authentication* section. click **Configure Trust with LDAP** (Administrator Console only), or **Configure Trust with LDAP** (System Administration Console only).
2. Select **LDAP Authentication**, then click the **Schedule** button next to the server name in the list of servers to schedule a user import:

The *User Import: Schedule – Choose attributes to import* page appears.

The following *Read Only Administrator Server Details* are displayed:

Option	Description
Server	The IP address or the hostname of the LDAP server. If the IP address is not valid, the appliance waits to timeout, resulting in login delays during LDAP authentication. **NOTE:** To connect through SSL, use an IP address or hostname. For example: ldaps://hostname.
Port	The LDAP port number, which is usually 389 (LDAP) or 636 (secure LDAP).
Base DN	The criteria used to search for accounts. This criteria specifies a location or container in the LDAP or Active Directory structure, and the criteria should include all the users that you want to authenticate. Enter the most specific combination of OUs, DCs, or CNs that match your criteria, ranging from left (most specific) to right (most general). For example, this path leads to the container with users that you need to authenticate: `OU=end_users,DC=company,DC=com.` **NOTE:** Use the LDAP Browser to specify the Search Base DN and Search Filter. Use the LDAP Browser.

Advanced Search	The search filter. For example:
	`(&(sAMAccountName=KBOX_USERNAME)`
	`(memberOf=CN=financial,DC=example,DC=com))`

Login	The credentials of the account the appliance uses to log in to the LDAP server to read accounts. For example:
	`LDAP Login:CN=service_account,CN=Users,`
	`DC=company,DC=com.`
	If user name and password are not provided, the tree lookup is not performed. Each LDAP Label can connect to a different LDAP or Active Directory server.

Password	The password of the account the appliance uses to log in to the LDAP server.

3. Specify the LDAP attributes to import.

Option	Description
Attributes to retrieve	Specify the LDAP attributes to retrieve. For example: `sAMAccountName, objectguid, mail, memberof, displayname, sn, cn, userPrincipalName, name, description, manager` The LDAP attributes specified in this field can be mapped to appliance User attributes on the next page. If this field is blank, the appliance retrieves all LDAP attributes. Leaving this field blank increases the time required to import attributes and is not recommended. **IMPORTANT: To retrieve the manager object associated with the user, you must add the `manager` attribute to the list, and to specify this mapping in a later step.**
Label Attribute	Enter a label attribute. For example: `memberof`.

Option	Description
	This setting returns a list of groups this user is a member of. The union of all the label attributes forms the list of labels you can import. If the search filter contains both the label names and user names, the label attribute is not required.
Label Prefix	Enter the label prefix. For example: `ldap_` The label prefix is a string that is added to the beginning of all the labels.
Binary Attributes	Enter the binary attributes. For example: `objectsid`. Binary attributes indicates which attributes should be treated as binary for purposes of storage.
Maximum Number of Rows	Enter the maximum number of rows to retrieve. This limits the result set that is returned in the next step.
Debug Output	Select the check box to view the debug output.

4. In the *Email Recipients* section, click the **Edit** button to enter the recipient's email address .
5. Select users in the *Recipients* drop-down list.
6. In the *Schedule* section, specify schedule options:

Option	Description
None	Run in combination with an event rather than on a specific date or at a specific time. This option is useful if you want to patch servers manually, or perform patch actions that you do not want to run on a schedule.
Every _ hours	Run at a specified interval.
Every day/specific day at HH:MM	Run daily at a specified time, or run on a designated day of the week at a specified time.
Run on the nth **of every month/ specific month at HH:MM**	Run on the **n**th day every month, (for example, the first or the second) day of every month, or a specific month, at the specified time.
Run on the nth weekday of every month/specific month at HH:MM	Run on the specific weekday of every month, or a specific month, at the specified time.

Custom	Run according to a custom schedule.
	Use standard 5-field cron format (extended cron format is not supported):
	`* * * * *`
	`| | | | +————————day of week (0-6)(Sun=0)`
	`| | | +————————month (1-12)`
	`| | +————————day of month (1-31)`
	`| +————————hour (0-23)`
	`+————————minute (0-59)`

Option	Description
	Use the following when specifying values: • **Spaces ( )**: Separate each field with a space. • **Asterisks (*)**: Include the entire range of values in a field with an asterisk. For example, an asterisk in the hour field indicates every hour. • **Commas (,)**: Separate multiple values in a field with a comma. For example, `0,6` in the day of the week field indicates Sunday and Saturday. • **Hyphens (-)**: Indicate a range of values in a field with a hyphen. For example, `1-5` in the day of the week field is equivalent to `1,2,3,4,5`, which indicates Monday through Friday. • **Slashes (*/*)**: Specify the intervals at which to repeat an action with a slash. For example, `*/3` in the hour field is equivalent to `0,3,6,9,12,15,18,21`. The asterisk (`*`) specifies every hour, but `/3` restricts this to hours divisible by 3. Examples: • `15 * * * * Run 15 minutes after every hour every day` • `0 22 * * * Run at 22:00 every day` • `0 0 1 1,6 * Run at 00:00 on January 1 and June 1` • `30 8,12 * * 1-5 Run weekdays at 08:30 and 12:30` • `0 2 */2 * * Run every other day at 02:00`
View Task Schedule	Click to view the task schedule. The *Task Schedule* dialog box displays a list of scheduled. Click a task to review the task details. For more information, see View task schedules.

7. Click **Next** to display the *User Import: Schedule - Define mapping between User attributes and LDAP Attributes* page.
8. In the drop-down list next each attribute, select the value to use for appliance User attributes during import. Values in the drop-down list are the values specified in the *Attributes to retrieve* field on the previous page.

The following attribute mappings are required:

Option	Description
Ldap Uid	The identifier for the user. Recommended value: `objectguid`.
User Name	The name of the user. Recommended value: `name`.
Email	The email address for the user. Recommended value: `mail`.
Manager	The manager of the user. This mapping is mandatory only if you want to retrieve the manager information. Recommended value: `manager`. **IMPORTANT: To retrieve the manager object associated with the user, you must also add the `manager` attribute to the *Attributes to retrieve* box.**

The following attribute mappings are not required, but they are recommended:

Option	Description
Api Enabled	Whether users are enabled to access the appliance using the KACE GO app. Access is enabled if the field contains a numerical value. Access is disabled if the field

Option	Description
	contains no value. Therefore, to enable access, select an attribute that returns a numerical value. To disable access, select **No Value**.
Ams Id	Not used. Recommended value: **No Value**.

9. **Optional**: In the *Role* drop-down list, select the role for the imported users. See Add or edit User Roles.
10. If you want the selected role to be a default role for new roles, select the **Make default** check box.
11. **Optional**: In the *Labels* drop-down list, select the label to apply to imported users. See About labels.
12. In the *Search Results* section below the attribute mapping drop-down lists, verify that the list of users to import is correct, and the information listed for each user is what you expect. To refine your search, click the **Back** button and revise the search parameters and attributes.

    For example, to change the number of *Search Results*, **change the** *Maximum Number of Rows* **on the** *Choose attributes to import* **page.**
13. Click **Next** to display the *Import Data into the appliance* page.
14. Review the tables of users to ensure that the data is valid and includes the data that you expect.

    Only users with values for the required attributes, *Ldap Uid*, *User Name*, *Email*, **and** *Manager*, **are imported. Records that do not have these values are listed in the** *Users with invalid data* **section.**
15. Do one of the following:

    - **Click Back to change settings.**
    - **Click Import to save the schedule and import user information immediately. The import begins, and the schedule is set to run according to the options selected in** *Scheduling* **section.**
    - **Click Finish to save the schedule without importing user information. The schedule is set to run according to the options selected in the** *Scheduling* **section.**

    User information is imported according to the specified schedule.

About single sign on (SSO)

Single sign on enables users who are logged on to the domain, or authenticated through a third-party, to access the appliance **Administrator Console** and **User Console** without having to re-enter their credentials on the appliance login page.

You can use Active Directory for single sign on.

Single sign on is available for:

- **One domain only**: If you have multiple domains, only one can be enabled for single sign on. This is true even if the Organization component is enabled on the appliance, and you have multiple organizations that are on different domains. Single sign on is a System-level configuration, and organizations cannot be configured independently for single sign on.
- **Microsoft Active Directory servers**: You can enable single sign on using Microsoft Active Directory servers with 2003 R2 or higher schema versions. Earlier schema versions cannot be used. If the Organization component is enabled on your appliance, the Active Directory single sign on method can be used with multiple organizations.

Using external LDAP or Active Directory servers for single sign on

When using Active Directory for authentication for single sign on, the external LDAP or Active Directory server must have the same entries as the Active Directory server specified for single sign on. The appliance matches user credentials on the joined domain, and then it uses the external LDAP configuration to determine user roles and privileges.

To authenticate users by using local accounts on the appliance, you need to either import accounts from an LDAP or Active Directory server to the appliance, or manually create accounts on the appliance. See:

- Importing users from an LDAP server
- Managing System-level user accounts
- Managing organization user accounts

Enabling and disabling single sign on

You can enable or disable single sign on in the appliance security settings.

Enable single sign on

To enable single sign on, you need to configure the appliance Security Settings to establish a connection between an Active Directory server and the appliance.

- To configure single sign on for Active Directory, see Configure Active Directory as the single sign on method

1. Go to the appliance *Control Panel*:
   - **If the Organization component is not enabled on the appliance, log in to the appliance Administrator Console, `https://appliance_hostname/admin`, then select Settings > Control Panel.**
   - **If the Organization component is enabled on the appliance, log in to the appliance System Administration Console, `https://appliance_hostname/system`, or select System in the drop-down list in the top-right corner of the page, then select Settings > Control Panel.**
2. Click **Security Settings** to display the *Security Settings* page.
3. In the *Single Sign On* tab, select a single sign on method.

- Configure Active Directory as the single sign on method

Disable single sign on

You can disable single sign on without removing the appliance from the domain.

1. Go to the appliance *Control Panel*:
   - **If the Organization component is not enabled on the appliance, log in to the appliance Administrator Console, `https://appliance_hostname/admin`, then select Settings > Control Panel.**
   - **If the Organization component is enabled on the appliance, log in to the appliance System Administration Console, `https://appliance_hostname/system`, or select System in the drop-down list in the top-right corner of the page, then select Settings > Control Panel.**
2. Click **Security Settings** to display the *Security Settings* page.
3. In the *Single Sign On* section, select **Disable**.

   Single sign on is disabled. Users who are currently logged in to the Administrator Console or User Console remain logged in until their sessions end. The next time they attempt to access the Administrator Console or User Console, however, they are required to enter their credentials.

Using Active Directory for single sign on

When single sign on is configured to use Active Directory, authenticated users can access the **Administrator Console** or the **User Console** without having to enter login credentials.

To do so, users must type the hostname of the appliance in the browser address field. If users enter an IP address, they are directed to the appliance login page, instead of being signed on automatically, and they must enter their credentials to log in.

If you use Active Directory for single sign on, you must configure Microsoft Edge and Mozilla Firefox browsers to use the appropriate security settings.

Configure Active Directory as the single sign on method

Active Directory single sign on enables users who are logged on to the domain to access the appliance **Administrator Console** and **User Console** without having to re-enter their logon credentials each time.

Before you connect the appliance to an Active Directory server, verify that:

- Network and DNS settings are configured to enable the appliance to access the Active Directory server. See Change appliance network settings.
- The time settings on the Active Directory server match the time settings on the appliance. For information on setting the time on the appliance, see Configure appliance date and time settings.

1. Go to the appliance *Control Panel*:
   - **If the Organization component is not enabled on the appliance, log in to the appliance Administrator Console, `https://appliance_hostname/admin`, then select Settings > Control Panel.**
   - **If the Organization component is enabled on the appliance, log in to the appliance System Administration Console, `https://appliance_hostname/system`, or select System in the drop-down list in the top-right corner of the page, then select Settings > Control Panel.**
2. In the *Single Sign On* tab of the *Security Settings* page, select **Active Directory**, then provide the following information:

Option	Description
Domain	The host name of the domain of your Active Directory® server, such as example.com.
Username	The user name of the administrator account on the Active Directory server. For example, username@example.com.
Password	The password of the administrator account on the Active Directory server.
Computer Object Container	The name of the computer object container of the administrator account on the Active Directory server.
Computer Object Name	The name of the computer object container of the administrator account on the Active Directory server.
Service Account Container	The name of the service account container of the administrator account on the Active Directory server.

3. Click **Join**.

The appliance performs the following tests, which require read-only permission, to determine whether the domain is configured correctly to allow the appliance to join the domain:

```
#   Check for supported operating system and correct operating system patches
#   Check for sufficient disk space to install QAS
#   Check that the hostname of the system is not 'localhost'
#   Check if the name service is configured to use DNS
#   Check resolv.conf for proper formatting of name service entries and that
    the host can be resolved
#   Check for a name server that has the appropriate DNS SRV records for Active
    Directory
#   Detect a writable domain controller with UDP port 389 open
#   Detect Active Directory site if available
#   Check if TCP port 464 is open for Kerberos kpasswd
#   Check if UDP port 88 and TCP port 88 are open for Kerberos traffic
#   Check if TCP port 389 is open for LDAP
#   Check for a global catalog server and if TCP port 3268 is open for
    communication with global catalog servers
#   Check for a valid time skew against Active Directory
#   Check for the QAS application configuration in Active Directory
#   Check if TCP port 445 is open for Microsoft CIFS traffic
```

These tests do not need write access and they do not check for permission to write to any directory. In addition, these tests do not verify username and password credentials. If the credentials are incorrect, the appliance might not be able to join the domain even if the tests are successful.

A message appears stating the results of the test. To view errors, if any, click **Logs**, then in the *Log* drop-down list, select **Server Errors**.

4. **Optional**: Select **Force Join** to join the server to ignore errors and join the domain.
5. Click **Save**.

When users are logged in to devices that are joined to the Active Directory domain, they can access the appliance **User Console** without having to re-enter their credentials. If users are on devices that are not joined to the Active Directory domain, the login window appears and they can log in using a local appliance user account. See Add or edit System-level user accounts.

NOTE: To use single sign on with Microsoft Edge and Firefox browsers, users must configure their browser settings to use the appropriate authentication. See Configuring browser settings for single sign on.

Configuring browser settings for single sign on

To use Active Directory single sign on with Microsoft Edge™ and Firefox® browsers, users must configure their browser settings to use the appropriate authentication. The Chrome™ browser does not require any special configuration.

Configure Microsoft Edge browser settings

To use Active Directory single sign on with the Microsoft Edge, you must configure the Windows security settings.

1. In the Windows Control Panel, click **Internet OptionsTools** > **Internet Options** > **Security**.
2. In the *Internet Properties* dialog box that appears, on the *Security* tab, select the appropriate security policy:
   - **If the appliance is available on the Internet select Trusted Sites.**
   - **If the appliance is not available on the Internet, select local intranet.**
3. Click **Custom level**, then scroll to the bottom of the list.
4. Select **Automatic logon with current username and password**. If this option is not selected, Microsoft Edge cannot automatically log in to the Administrator Console or User Console even if single sign on is enabled on the appliance.

Configure Firefox browser settings

To use Active Directory single sign on with Firefox, you must configure the browser's authentication settings.

1. In the Firefox browser, type about:config in the address bar.
2. In the *Search* field type the following network.negotiate-auth.trusted-uris.
3. In the search results, double-click the name of the preference.
4. In the string value box, enter the URL of the appliance. For example, http://kace_sma.example.com, then click **OK**.

Use Active Directory single sign on to access the Administrator Console or User Console

When Active Directory single sign on is enabled on the appliance, users who are logged in to the domain can access the **Administrator Console** or **User Console** without entering their credentials on the appliance login page.

Single sign on must be enabled through Active Directory. See Enable single sign on.

1. Log in to the domain.
2. In a web browser, type the hostname of the appliance in the browser address field. To identify the host name, see Change appliance network settings.

   TIP: If you enter the appliance IP address, you are directed to the appliance login page instead of being signed on automatically.

   The Administrator Console or User Console appears, depending on user account privileges.

Unjoin the domain and disable Active Directory single sign on

You can remove the appliance from the Active Directory domain. Removing the appliance from the domain automatically disables single sign on as well.

1. Go to the appliance *Control Panel*:
   - **If the Organization component is not enabled on the appliance, log in to the appliance Administrator Console, `https://appliance_hostname/admin`, then select Settings > Control Panel.**
   - **If the Organization component is enabled on the appliance, log in to the appliance System Administration Console, `https://appliance_hostname/system`, or select System in the drop-down list in the top-right corner of the page, then select Settings > Control Panel.**
2. Click **Security Settings** to display the *Security Settings* page.
3. In the *Single Sign On* tab, click **Unjoin Domain**.

NOTE: Users who are currently logged in to the **User Console** or **Administrator Console** remain logged in until their session ends. The next time they attempt to access the **User Console** or **Administrator Console**, however, they are required to enter their credentials.

Configure SAML for single sign on

You can configure the appliance to authenticate users without providing their credentials on the *Welcome* page using a third-party authentication tool.

Security Assertion Markup Language (SAML) is an XML-based protocol that uses security tokens between identity and service providers. The security tokens contain assertion elements that provide information about the user's identity.

When SAML is enabled and configured on the appliance, and the user logs in using this single sign-on method, the appliance sends an authorization request to your Identity Provider (IdP). The identity provider then confirms the user's identity and sends an authentication response to the appliance. Next, the appliance logs the user in to the **Administrator Console** (or **User Console**) and establishes the user session. When a SAML user logs out of the appliance, they are logged out of their IdP account. If you want to continue to be logged into your IdP account after using the appliance, simply close the **Administrator Console** browser window without signing out. If a SAML user's session times out, and they are still logged into their IdP account, the appliance automatically starts a new session for that user.

If you have multiple organizations, you can configure SAML in each organization that uses this method of authentication, and keep the local login method for other organizations.

1. Ensure that your IdP has valid identity information for logging you in to the appliance.
2. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
3. Go the *SAML Settings* page:
    a. On the left navigation bar, click **Settings**, then click **SAML Configuration > Configure Single Sign On with SAML**.
    b. On the *SAML Settings* page, under *Security Assertion Markup Language (SAML)*, select the **Enable SAML Service Provider** check box.
4. If you want to allow users to only use SAML to access this appliance, select **Require SAML login**.

    This option causes all local logins to the appliance to be disabled, with the exception of the local admin user and the KACE Support account (available only with an active Support tether).
5. In the *Remote Identity Provider (IdP) Settings* section, specify your IdP metadata to authenticate users by completing one of the following steps.
    - **Recommended. If your IdP provides an URL to the XML page containing the IdP metadata (suggested option), click Get Metadata From IdP. In the *IdP Metadata URL* field that appears, type that URL, and click Import IdP Metadata.**
    - **To use your IdP metadata XML file, click Enter XML Metadata, and in the *IdP Metadata XML* field that appears, copy and paste the contents of the XML file. Then click Import IdP Metadata. The appliance parses the provided XML content and populates the settings required to establish a connection with the IdP.**

    The *Remote Identity Provider (IdP) Settings* section refreshes, showing the details of your IdP configuration. The listed options specify the appliance page redirects during SAML authentication. For more information, visit https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security.

NOTE: To review this information anytime during your SAML configuration, click **View Metadata** in this section.

6. In the *IdP Attribute Mappings* tab, select the option that you want to use to grant the SAML user access to the appliance.
   - **Use Local User Table: Relies on the user list stored locally on the appliance.**
   - **Use LDAP Lookup: Imports user information from an external LDAP server. For more information, see Using an LDAP server for user authentication.**
   - **Use SAML: Uses the values specified on this page to map to the fields used by your IdP to the appliance user records, such as name, email address, and so on. For example, if the IdP uses LDAP to authenticate users, you can set *UID* and *Login* to `objectGUID` and `cn`, respectively. For more information, see your IdP documentation.**
7. If you selected **Use SAML**, indicate if you want to create a new user on the appliance for authenticated SAML users that do not have accounts on the appliance. To do that, select **Create new SMA user if authenticated SAML user does not exist on SMA**.
8. If you selected **Use SAML**, specify the roles that you want to grant to the SAML-authenticated user. Under *Role Mapping*, specify the conditions that you want to check when granting the roles.

   For example, you can grant the *Administrator* role to the members of an LDAP group whose name contains a specific text string (such as `admin`), set the Administrator role as follows:

   Administrator `memberOf` *Contains* `admin`

   The roles are listed in the order of priority. You can change the role priority by dragging and dropping them, as needed. If there are multiple matches, the appliance grants the role with the highest priority to the SAML user.

   Role mapping is optional. If no matches are found, the appliance assigns the default role. To specify the default role, click Default Role for Unmatched Users, and choose a role from the available options, as applicable: *Administrator*, *No Access*, *Read Only Administrator*, or *User Console Only*.
9. **Optional**. To view the appliance-specific SAML settings on the appliance, in the *Local Service Provider (SP) Settings* section, click **View Metadata**, and review the options that appear.

   These fields contain default values and in most cases you do not need to make any changes.
10. Click **Save**.
11. Test your SAML configuration.
    a. Log out of the appliance.
    b. Ensure you are logged in to your IdP account.
    c. Open the Administrator Console or User Console Welcome page.
    d. Without specifying your user credentials, click **Login**.

    TIP: When SAML is enabled on the appliance, click **Local Sign On**, and specify your user credentials.

    The Administrator Console or User Console page appears.

Example: Using Microsoft Active Directory in Azure as a SAML Identity Provider

When you use Active Directory in Azure as a SAML Identity Provider (IdP), some additional steps are required. This topic describes the process of configuring SAML with Active Directory as an IdP.

1. Ensure that your IdP has valid identity information for logging you in to the appliance.
2. Complete the following steps:
   a. Enable SSL for the appliance. This step is required because Microsoft Azure can successfully communicate only with SSL clients. For instructions, see Configure security settings for the appliance.

b. Log in to https://portal.azure.com and select **Azure Active Directory**.

c. Under **App Registrations**, create a new registration, leaving the *Redirect URI* settings cleared.

d. In the newly created App Registration, on the *Endpoints* page, copy the contents of the *Federation metadata document* field.

3. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
4. Go the *SAML Settings* page:

   a. On the left navigation bar, click **Settings**, then click **SAML Configuration > Configure Single Sign On with SAML**.

   b. On the *SAML Settings* page, under *Security Assertion Markup Language (SAML)*, select the **Enable SAML Service Provider** check box.
5. In the *Remote Identity Provider (IdP) Settings* section, specify your IdP metadata to authenticate users by completing the following steps.

   a. Click **Get Metadata From IdP**.

   b. In the *IdP Metadata URL* field that appears, enter the contents from the *Federation metadata document* field that you recorded in 2.d, and click **Import IdP Metadata**.

   The *Remote Identity Provider (IdP) Settings* section refreshes, showing the details of your IdP configuration. The listed options specify the appliance page redirects during SAML authentication. For more information, visit https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security.

   NOTE: To review this information anytime during your SAML configuration, click **View Metadata** in this section.
6. In the *Security Assertion Markup Language (SAML)* tab, ensure the **IdP Does Not Support Passive Authentication** check box is selected.
7. In the *IdP Attribute Mappings* tab, select the option that you want to use to grant the SAML user access to the appliance.

   - **Use Local User Table: Relies on the user list stored locally on the appliance.**
   - **Use LDAP Lookup: Imports user information from an external LDAP server. For more information, see Using an LDAP server for user authentication.**
   - **Select Use SAML, and set the following options:**

   # **UID**: http://schemas.microsoft.com/identity/claims/objectidentifier

   # **Login**: http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name

   # **Name**: http://schemas.microsoft.com/identity/claims/displayname

   # **Primary Email**: http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name
8. If you selected the **Use SAML** option, under *Role Mapping*, specify the following condition for the role that you want to grant to SAML-authenticated users (for example, the *Administrator* role):

   `http://schemas.microsoft.com/ws/2008/06/identity/claims/groups` *equals* **`<Object ID>`**

   Where `<Object ID>` is the object ID of the group.
9. **Optional**. To view the appliance-specific SAML settings on the appliance, in the *Local Service Provider (SP) Settings* section, click **View Metadata**, and review the options that appear.

   These fields contain default values and in most cases you do not need to make any changes.
10. Complete the following steps:

    a. In the *Local Service Provider (SP) Settings* section, click **View Metadata**

    b. In the Microsoft Azure Portal, locate the newly created App Registration.

    c. On the App Registration page, click **Add a Redirect URI**.

d. In the *Redirect URIs* section, select **Web** and set it to the *SP Assertion Consumer Service (url)* value from the *SAML Settings* page, under *Local Service Provider (SP) Settings*.

e. In the *Advanced settings*, set the *Logout URL* field to the *SP SLO Endpoint (url)* value from the *Local Service Provider (SP) Settings* section.

f. In Azure, click **Expose an API**, and click **Set** next to *Application ID URI*. Set this field to the *SP Entity Identifier (uri)* value from the *Local Service Provider (SP) Settings* section.

g. In Azure, click **Manifest**, and in the editor that appears on the right, add or update the `"groupMembershipClaims"` attribute and set its value to `"SecurityGroup"` or `"All"`.

For example: `"groupMembershipClaims": "SecurityGroup",`

11. Click **Save**.
12. Test your SAML configuration.
    a. Log out of the appliance.
    b. Ensure you are logged in to your IdP account.
    c. Open the Administrator Console or User Console Welcome page.
    d. Without specifying your user credentials, click **Login**.

TIP: When SAML is enabled on the appliance, click **Local Sign On**, and specify your user credentials.

The Administrator Console or User Console page appears.

Reviewing user sessions

The appliance keeps track of user sessions. You can review a list of the most recent sessions, or see all sessions for the appliance.

To allow the appliance to display the location associated with the logged-in user's public IP address, you must install a location database. See Install and configure the location database.

You can see all sessions on the *Recent Sessions* page. For a quick list of the latest sessions associated with your user account, use the *My Recent Sessions* pane. See View a list of user sessions.

Install and configure the location database

User session details include the IP address of the currently logged-in user. This information is displayed on the *Recent Sessions* page. For public IP addresses you can also display the geographical location associated with a specific IP address, however this requires a location database to be installed on the appliance. You can install the MaxMind *Geolocation* database free of charge and display user locations for any public IP address.

MaxMind offers country and city databases. A city database is typically larger in size and takes longer to install. A country database provides only the name of the country associated with each public IP address, while a city database allows the appliance to display the city, state (if applicable), and the country.

You can periodically refresh the location database by installing an updated version. While it is possible to install multiple databases over time, the most recently installed database overwrites the contents of the previous version. For example, if a country database is already installed, and you install a city database on the appliance, the *Location* column on the *Recent Sessions* page reflects the information from the newly installed city database.

For complete information about MaxMind Geolocation databases, visit https://www.maxmind.com/.

NOTE: Locations cannot be displayed when a private IP address is used to access the appliance.

1. Download a location database from https://www.maxmind.com/.

NOTE: To download a database file from MaxMind, start by creating a user profile. You must download a file that uses the `MMDB` format, not a `CSV` file.

2. Do one of the following:
   - **If the Organization component is not enabled on the appliance, log in to the appliance Administrator Console, `https://appliance_hostname/admin`, then select Settings > Control Panel.**
   - **If the Organization component is enabled on the appliance, log in to the appliance System Administration Console, `https://appliance_hostname/system`, or select System in the drop-down list in the top-right corner of the page, then select Settings > Control Panel.**
3. On the *General Settings* page that appears, in the *Geolocation Lookup Database* section, point to the downloaded ZIP file.

   To do that, under *MaxMind Geolocation Database*, click Choose file and navigate to the newly downloaded file.
4. Click **Save**.

   It may take a few minutes for the database installation to complete, depending on the type of database being installed. When the installation is complete, the *Database Type* and *Database Version* fields provide the relevant details.

NOTE: A city database typically takes longer to install and update than a country database due to its file size.

Next, you can go to the *Recent Sessions* page and review the location data for the current user. See View a list of user sessions.

View a list of user sessions

You can review user sessions on the appliance. Use the *My Recent Sessions* pane to see the latest sessions associated with your account. You can also review all sessions that are currently active on the appliance on the *Recent Sessions* page.

In case the appliance detects multiple sessions for the current user, the icon displays a red exclamation point.

1. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
2. In the top-right corner, click the Recent Sessions icon.

   NOTE: If there are multiple active sessions associated with your user account, an exclamation mark appears on the Recent Sessions icon.
3. In the *My Recent Sessions* pane that appears, review the list of your latest user sessions.

   Each entry identifies your browser, IP address, session duration, the date and time of the most recent activity, and any applicable actions.

   NOTE: You can delete duplicated sessions by clicking the Delete icon in the *Actions* column, as needed.
4. To see all sessions that are currently active on the appliance, in the *My Recent Sessions* pane, click *View All Recent Sessions*.

   On the *Recent Sessions* page that appears, each entry displays the user name, the browser used, the operating system, IP address, the session duration, the date and time of the last activity, and any applicable actions. For users with a public IP address, if you have a location database installed, it also shows their location. See Install and configure the location database.

Deploying the KACE Agent to managed devices

The KACE Agent is an application that can be installed on devices to enable inventory reporting and other device management features. KACE Agents installed on managed devices communicate with the appliance through an agent messaging protocol. Agents perform scheduled tasks, such as collecting inventory information from, and distributing software to, managed devices.

You can deploy the KACE Agent to managed devices using one of the following methods.

TIP: Only authenticated KACE Agents can establish a successful connection with the appliance. For more information, see Registering KACE Agent with the appliance.

- **Provisioning the KACE Agent**: You can use the Agent Provisioning Assistant to perform provisioning for devices with Windows, Mac OS X, and Linux operating systems. Within the Assistant, you can choose between using the appliance GPO Provisioning Tool for deploying the Agent to Windows devices, or using Onboard Provisioning for deploying the Agent to Windows, Mac OS X, or Linux devices. See Provisioning the KACE Agent.
- **Manually deploying the KACE Agent**: Use manual deployment is useful when automated Agent provisioning is not practical or when you want to deploy the KACE Agent using email, logon scripts, GPO (Group Policy Objects), or Active Directory. The appliance includes KACE Agent installers for different OS platforms. Each platforms offers one or more ways to deploy the KACE agent. To get started, visit the following sections and their sub-topics:
  - # Manually deploying the KACE Agent on Windows devices
  - # Manually deploying and upgrading the KACE Agent on Linux devices
  - # Manually deploying and upgrading the KACE Agent on Mac devices

Using Replication Shares

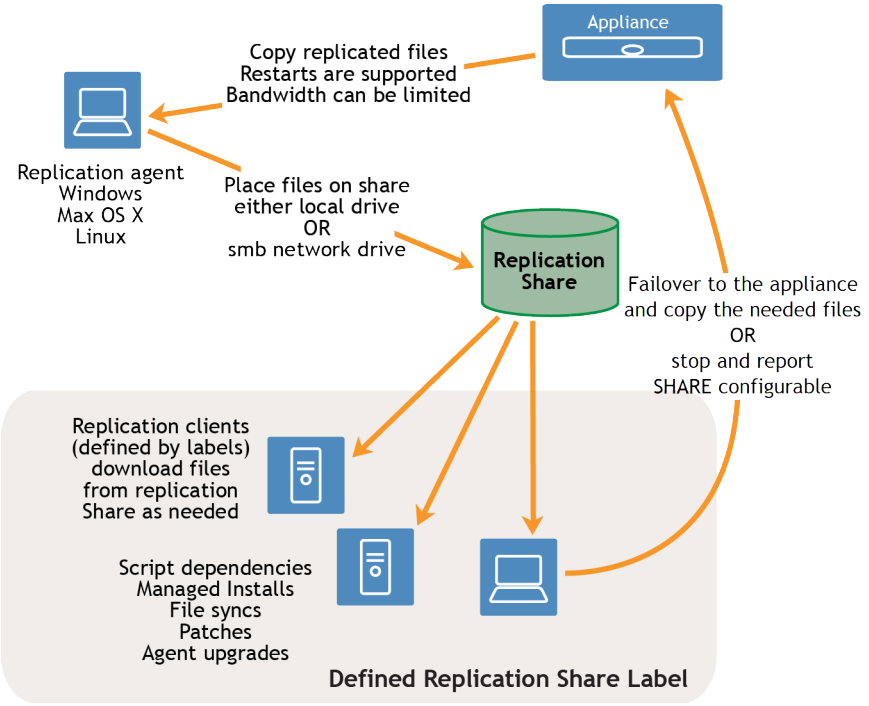
Replication Shares are devices that keep copies of files for distribution, and they are especially useful if your managed devices are deployed across multiple geographic locations.

For example, using a Replication Share, a device in New York could download files from another device at the same office, rather than downloading those files from a appliance in Los Angeles. A Replication Share is a full replication of all digital assets and is managed automatically by the appliance. Whenever a Replication Share is specified for a label, devices in that label go to the Replication Share to get files.

In addition, you can use Replication Shares to deploy of Managed Installations, patches, or Dell Updates where network bandwidth and speed are issues. Replication Shares are good alternatives to downloading directly from an appliance.

Replication Shares enable an appliance to replicate application installers, patches, upgrades, and script dependencies to a shared folder on a device. If any replication item is deleted from the appliance, it is marked for deletion in the Replication Share and deleted in the replication task cycle. The figure shows a Replication Share configuration and task flow.

Figure 9. Replication Share configuration



To create a Replication Share, identify one device at each remote location to act as a **Replication Device**. The appliance copies all the replication items to the Replication Device at the specified destination path. The replication process automatically restarts if it is stopped due to a network failure or replication schedule. If stopped, the replication process restarts at the point it was stopped.

Sneaker net share: You can create a folder and copy the contents of an existing replication folder to it. You can then specify this folder as the new replication folder in the appliance. The appliance determines whether the new folder has all the replication items present and replicates only the new ones, which conserves bandwidth. You can manually copy the contents of replication folder to a new folder. The replication folder created in a device follows following hierarchy:

```
\\machinename\foldername\repl2\replicationitems folder
```

The device name and folder name is user defined while `repl2` is automatically created by appliance. The replication items folder includes the folder for patches, kbots, upgrade files, and applications.

All the replication items are first listed in the replication queue and then copied one at a time to the destination path. Any new replication item is first listed in the replication queue and then copied after an interval of 10 minutes.

Replication items are copied in this order:

1. Script dependencies
2. Applications
3. Agent upgrades
4. Patches

Create Replication Shares

You can create Replication Shares on managed devices.

To create a Replication Share you must:

- Have **write** permission on the destination path to write the software files.
- Install the KACE Agent on the Replication Share.
- Create a label for your devices before starting the process.

Replication Shares can be created only on devices that appear on the *Devices* list in Inventory. If the device you want to use is not on the *Devices* list, you need to create an inventory record for the device before you can use it as a Replication Share.

See Managing inventory information.

1. Go to the *Replication Schedule Detail* page:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Distribution**, then click **Replication**.
   c. Select **Choose Action** > **New**.
2. In the *Configure* tab, select the **Enabled** check box.
3. **Optional**: Select **Failover To Appliance** to use the appliance when the Replication Share is not available.

   NOTE: Enable **Failover To Appliance** only after testing the Replication Share.
4. In the *Device* drop-down list, select the device to use as a Replication Share.

   The Replication Share can be created by two methods:

   - **Locally**
   - **On a shared network drive**
5. Select the **Operating System** and **Locales** of the patches to replicate. The lists are populated based on the operating systems and locales selected in the patch subscription.
6. Select the **Include Application Patches**, **Include Windows Feature Updates**and **Include Dell Updates** check boxes to copy the patch and update files to the Replication Share.
7. Specify the settings in the *Destination Share* tab:

Option	Description
Path	The path the Replication device uses for the Replication Share. Applications are copied from the appliance to this location. For a local drive, use local drive syntax, for example: `C:\`**kace_sma_share** For a network drive, use UNC format, for example: `\\`**kaceRep**`\`**kace_sma_share**`\` **NOTE:** **$** notation, for example `\\`**KaceRep**`\e$`, is not supported.
Share Type	Select whether to use a Local Share or UNC.
Credentials	The details of the service account required to connect to the device and run commands. Select existing credentials from the drop-down list, or select **Add credential** to add credentials not already listed. See Add and edit User/Password credentials.
Label	The label of the devices using the Replication Share. Verify that the selected label does not have KACE_ALT_LOCATION specified. KACE_ALT_LOCATION takes precedence over the Replication Share for downloading files to devices.

8. Specify settings in the *Download Share* tab :

Option	Description
Path	The path used by devices in the replication label to copy items from the replication drive. For example, a UNC path: `\\fileservername\directory\kace_sma\` Other devices need **read** permission to copy replication items from this shared folder.
Credentials	The details of the service account required to connect to the device and run commands. Select existing credentials from the drop-down list, or select **Add credential** to add credentials not already listed. See Add and edit User/Password credentials.

9. Specify the following settings in the *Schedule* tab:

Option	Description
High Bandwidth	The maximum bandwidth to use for replication. If this field is blank, the maximum bandwidth available for replication is used. This field is specified in bytes per second.
Low Bandwidth	The restricted bandwidth to use for replication. If this field is blank, the maximum bandwidth available for replication is used. This field is specified in bytes per second.
Schedule table	The bandwidth used for each hour of the day (24-hour clock format) and each day of the week. • To change the bandwidth selection, click in a square. • To select hours (columns), click the hour number. • To select days (rows), click the day of the week. Bandwidth is color-coded: • **White**: Replication is off • **Grey**: Replication is on with low bandwidth • **Blue**: Replication is on with high bandwidth
Schedule	Select an existing Replication Schedule in the drop-down list to replicate items according to that schedule.
Notes	Any additional information you want to provide.

10. Click **Save**.

    The *Replication* page appears.

11. **Optional**: After you have tested the Replication Share, return to 3 and enable **Failover To Appliance**.

Related topics

Add or edit manual labels

About patch management

View Replication Share details

You can view details of devices used as Replication Shares.

1. Go to the *Replication* list:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Distribution**, then click **Replication**.

    This page displays a list of the Replication Shares that are available on the appliance. For each Replication Share, a default view shows its *Status*, replication *Task*, associated *Device*, *Destination Path*, KACE *Agent Version*, *Label*, an indication if the Replication Share is *Enabled*, and the number of files remaining to be copied along with the total size of files remaining to be copied (in the *ToDo* column). The information appearing in the *ToDo* column allows you to review the state of replication process for each Replications Share in this list, instead of reviewing individual shares to find out if their replication process is complete.
2. In the *Device* column, click the name of a Replication Share to display the *Replication Schedule Detail* page.

    On this page you can:

    # **View the Replication queue**: To view items that are queued for replication, click **Show Replication Queue** below the configuration information. This view is displayed by default when you access the page.
    # **View the Replication inventory**: To view items that have been replicated to the share, click **Show Share Inventory** below the configuration information.
    # **Delete the Replication queue**: To view replication items that are marked for deletion, click **Show Delete Queue** below the configuration information.

Managing credentials

The appliance enables you to manage the usernames and passwords required for logging in to other systems, such as managed computers and servers, and the information required for Google or SNMP authentication, from a central location.

Credentials that have been added to the appliance's *Credentials Management* page are available for selection on drop-down lists in the *Inventory* (Discovery, Provisioning, and Agentless device management), *Distribution* (Managed Installations, File Synchronizations, and Replication), and *Scripting* (Configuration Policies and Security Policies) sections.

In addition, credentials that are updated on the *Credentials Management* page are automatically updated wherever they are used in the various appliance components. You do not need to independently update each item that uses the credentials.

However, the credentials you add to the appliance must match the credentials on the target systems. If you change the credentials on target systems, you must change them on the appliance's *Credentials Management* page as well.

If the Organization component is enabled on your appliance, you manage credentials for each organization separately.

NOTE: The Credentials Management drop-down list is not available on LDAP configuration pages, and the feature is not used to manage user credentials for accessing the appliance **Administrator Console** or **User Console**, which use single sign on and LDAP authentication. See About user accounts and user authentication.

Tracking changes to Credentials Management settings

If History subscriptions are configured to retain information, you can view the details of the changes made to settings, assets, and objects. This information includes the date the item was created, changed, or deleted, and the user who performed the action, which can be useful during troubleshooting.

See About history settings.

Add and edit Secret Key credentials

To streamline the management of Secret Key credentials used in Inventory, Distribution, and Scripting, add those credentials to the *Credentials Management* page. Secret Key credentials can be created for devices managed using the KACE Cloud Mobile Device Manager.

- You have the secret key from the KACE Cloud Mobile Device Manager.
- You have administrator privileges in the **Administrator Console**.

After you add credentials, you can select them on configuration pages instead of entering the credentials manually each time. In addition, you can add credentials from any of the configuration pages that use them. Credentials added on configuration pages are automatically added to the *Credentials Management* page.

1. Go to the *Credentials Management* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Settings**, then click **Credentials**.
2. Select **Choose Action** > **New**.
3. On the *Add Credential* form, specify credential properties:

    NOTE: You can also access this form from pages that use credentials, such as the *Discovery Schedule Detail* page. Credentials added on these pages are automatically added to the *Credentials Management* list.

Option	Description
Name	A unique name for the credential. This name appears on the *Credentials Management* list and in the credential selection drop-down lists in component sections, such as Scripting. This name is used for identification in **Administrator Console**, and it is not part of the actual credential on the target device.
Type	The classification of the credential. Select **Secret Key** to specify credentials that contain secret keys from the KACE Cloud Mobile Device Manager.
Secret	The secret key of the KACE Cloud Mobile Device Manager environment.
Show typing	Show the characters in the *Password* field on the *Add Credential* form. This option is available only when you are adding credentials. If you are editing existing credentials, the password characters cannot be displayed.
Notes	Any additional information you want to provide about the credential.

4. Click **Save**.

The credential appears on the *Credentials Management* list and it is available for selection in components that use credentials.

Add and edit User/Password credentials

To streamline the management of username and password credentials used in Inventory, Distribution, and Scripting, add those credentials to the *Credentials Management* page. User/Password credentials can be created for Mac, Windows, and Linux operating systems as well as VMware ESXi hosts and vCenter Servers.

- You have the usernames and passwords of the credentials you want to manage.
- You have administrator privileges in the **Administrator Console**.

After you add credentials, you can select them on configuration pages instead of entering the credentials manually each time. In addition, you can add credentials from any of the configuration pages that use them. Credentials added on configuration pages are automatically added to the *Credentials Management* page.

1. Go to the *Credentials Management* page:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Settings**, then click **Credentials**.
2. Select **Choose Action** > **New**.
3. On the *Add Credential* form, specify credential properties:

NOTE: You can also access this form from pages that use credentials, such as the *Discovery Schedule Detail* page. Credentials added on these pages are automatically added to the *Credentials Management* list.

Option	Description
Name	A unique name for the credential. This name appears on the *Credentials Management* list and in the credential selection drop-down lists in component sections, such as Scripting. This name is used for identification in **Administrator Console**, and it is not part of the actual credential on the target device.
Type	The classification of the credential. Select **User/Password** to specify credentials that have usernames and passwords.
User or Domain \User	The username required for the credential. **TIP:** The `Domain\User` format might be required for some Windows configurations.
Password	The password required for the credential.
Show typing	Show the characters in the *Password* field on the *Add Credential* form. This option is available only when you are adding credentials. If you are editing existing credentials, the password characters cannot be displayed.
Targets	The device types on which the credential can be used. **TIP:** You can select multiple device types, or operating systems, if the specified credentials can be used for authentication on multiple operating systems.

Option	Description
Notes	Any additional information you want to provide about the credential.

4. Click **Save**.

   The credential appears on the *Credentials Management* list and it is available for selection in components that use credentials.

Add and edit LDAP User/Password credentials

To easily manage and password LDAP credentials, add those credentials to the *Credentials Management* page. LDAP User/Password credentials can be created for Mac, Windows, and Linux operating systems.

- You have the LDAP user names and passwords of the credentials you want to manage.
- You have administrator privileges in the **Administrator Console**.

After you add credentials, you can select them on configuration pages instead of entering the credentials manually each time. In addition, you can add credentials from any of the configuration pages that use them. Credentials added on configuration pages are automatically added to the *Credentials Management* page.

1. Go to the *Credentials Management* page:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Settings**, then click **Credentials**.
2. Select **Choose Action** > **New**.
3. On the *Add Credential* form, specify credential properties:

   NOTE: You can also access this form from pages that use credentials, such as the *Discovery Schedule Detail* page. Credentials added on these pages are automatically added to the *Credentials Management* list.

Option	Description
Name	A unique name for the credential. This name appears on the *Credentials Management* list and in the credential selection drop-down lists on the *LDAP Label Detail* page. This name is used for identification in **Administrator Console**, and it is not part of the actual credential on the target device.
Type	The classification of the credential. Select **LDAP User/Password** to specify LDAP credentials that include user names and passwords.
User or Domain \User	The user name required for the credential. **TIP:** The `Domain\User` format is sometimes required for some Windows configurations.
Password	The password required for the credential.
Show typing	Show the characters in the *Password* field on the *Add Credential* form. This option is available only when you are adding credentials. If you are editing existing credentials, the password characters cannot be displayed.
Notes	Any additional information you want to provide about the credential.

4. Click **Save**.

The credential appears on the *Credentials Management* list and it is available for selection in components that use credentials.

Add and edit Google Workspace credentials

To streamline the management of Google Workspace credentials used in Inventory, Distribution, Scripting, and Service Desk, add the applicable credentials to the *Credentials Management* page.

The appliance can obtain access to a Google Workspace Domain using the Google APIs. The following appliance-managed components can be authenticated through Google API:

- **Google Workspace Device Discovery and Inventory**: This includes both Chromebooks and mobile devices that are managed by a Google Workspace Domain (formerly G Suite). This type of authentication requires the following:
  # You have a Google Workspace Domain with Chrome Device Management support.
  # You have a Google User admin account that is a member of the domain. The account must be assigned the Super User role.
  # You have a Google account that can be used as your developer account in this procedure. This account does not have to be the same as the Admin account, nor does it have to be a member of the business or education domain.
- **Service Desk Queue Inboud Email**: This includes email accounts that are part of a Google Workspace or a public Gmail account. This type of authentication requires the following:
  # You have a Gmail account.
  # The following applies to your Service Account:
    # The Gmail account belongs to a Google Workspace Domain.
    # You have a Google User admin account that is a member of the domain, The account must be assigned the Super Admin role.
  # You have a Google account that can be used as your developer account in this procedure. This account does not have to be the same as the admin account, nor does it have to be a member of the business or education domain.

For each of these component types, the appliance supports the following methods authentication by a Google API. The method you choose depends on the components using the Google Workspace credential and the preference or role of the appliance administrator.

- **Service Account authentication** consists of a Service Account Key that is associated with a unique Client ID. A Google Workspace Super Admin can use the Client ID to grant the Service Account Domain Wide Access to a resource.
  # **This is a preferred method for Chromebook and Mobile Device Discovery and Inventory.**
  # It requires a configuration step using the Google Workspace Console by a Super Admin.
  # It grants domain-wide access to a specific resource type. In the case of Service Desk Queue emails, this means the service account is granted access to any email inbox. It is up to the administrator to ensure that it is only used with the desired Service Desk email.
- **OAuth Client authentication** consists of a OAuth Client ID that is used along with a Client Secret to request and grant access to a particular Google resource using a browser-based workflow.
  # **This is a preferred method for Service Desk Queue Inboud Email integration.**
  # It requires that the browser used to configure the credential in the **Administrator Console** connects to the appliance using a host name that is considered public (no private domains).
  # It can be used with public Gmail accounts.

Start by creating one or more Google Workspace Service Account or OAuth credentials, as applicable. After you add credentials, you can select them on configuration pages instead of entering them manually each time. In addition, you

can add credentials from any of the configuration pages that use them. Credentials added on configuration pages are automatically added to the *Credentials Management* page. The appliance does not validate stored Google OAuth credentials as you enter them, but attempting to save any changes using invalid credentials result in an error.

1. Create and configure a Google Cloud Platform project.
    a. Sign in to your developer account at https://console.cloud.google.com.
    b. Assign a new name and ID to the project.
    c. Enable the desired Admin SDK API and/or Gmail API, as applicable.
2. **Service Account credentials only.**
    a. While still logged in to the Google Cloud console, select *IAM & Admin*.
    b. Create a Service Account with a desired name and description.
    c. Add a Service Account Key and save the JSON key file.
    d. Record the OAuth 2 Client ID of the Service Account for later use.
3. **OAuth credentials only.**
    a. While still logged in to the Google Cloud console, select *APIs & Services*, and go to the *OAuth consent screen*.
    b. If the developer account is part of the same Google Workspace domain as the resources being accessed, select *Internal* otherwise choose *External*.
    c. Create an app and specify its name, Support email address, and Developer contact email address.
    d. Add the following scopes:
    # **Device Discovery and Inventory only:**
        - https://www.googleapis.com/auth/admin.directory.device.chromeos
        - https://www.googleapis.com/auth/admin.directory.device.mobile
        - https://www.googleapis.com/auth/admin.directory.user
    # **Service Desk Queue email only:**
        - https://www.googleapis.com/auth/gmail.modify
    e. Create a credential and select OAuth Client ID.
    f. Choose *Web Application* as the Application type.
    g. Assign a name to the client.
    h. Provide the following URI: `https://<appliance_hostname>/common/authorize.php`, where `appliance_hostname` is the host name of the appliance Administrator Console.
    i. Record the Client ID and Client Secret for later use.
4. **Service Account credentials only (optional).** Delegate a domain-wide authority to a Service Account. This step requires Super Admin access to the Google Workspace Admin console.

    NOTE: When authorizing the Gmail modify scope to a Service Account, access is granted to that service account for all mailboxes on the domain. Ensure that the Service Account Key credentials are protected accordingly.

    a. Sign in to the Google Admin console at https://admin.google.com/.
    b. Under **Security** > **Access and data control** > **API Controls** > **Manage Domain Wide Delegation**, create a new delegation and provide the Client ID of the Service Account that you created in 2.
    c. Add the following scopes:
    # **Device Discovery and Inventory only:**
        - https://www.googleapis.com/auth/admin.directory.device.chromeos
        - https://www.googleapis.com/auth/admin.directory.device.mobile
        - https://www.googleapis.com/auth/admin.directory.user
    # **Service Desk Queue email only:**

- https://www.googleapis.com/auth/gmail.modify

5. Go to the *Credentials Management* page:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Settings**, then click **Credentials**.
6. Select **Choose Action** > **New**.
7. On the *Add Credential* form, specify credential properties:

Option	Description
Name	A unique name for the credential. This name appears on the *Credentials Management* list and in the credential selection drop-down lists in component sections, such as Scripting. This name is used for identification in **Administrator Console**, and it is not part of the actual credential.
Type	The classification of the credential. Select **Google Workspace** or **GMail**, as applicable.

8. **Service Account credentials only.** While still on the *Add Credential* form, specify the credential properties:

Option	Description
Service Account	Select this option.
Impersonation Account	• **Device Discovery and Inventory only:** The email address of an administrator that has access to the devices in the Google Admin console. • **Service Desk Queue email only:** The email address from which you can receive inbound email.
Service Account Key	Navigate to the JSON file obtained in 2.
Notes	Any additional information you want to provide about the credential.

9. **OAuth credentials only.** While still on the *Add Credential* form, specify the credential properties:

Option	Description
OAuth	Select this option.
Client ID	Your Google developer API Client ID obtained in 3.
Client Secret	Your Google developer API Client Secret obtained in 3.
Show typing	Show the characters in the *Client Secret* field on the *Add Credential* form. This option is available only when you are adding credentials. If you are editing existing credentials, the characters in the *Client Secret* field cannot be displayed.

Option	Description
Authorize Credential	Click, log in, and grant access to the desired Google account on the page that appears. • **Device Discovery and Inventory only:** The account of an administrator that has access to the devices in the Google Admin console. • **Service Desk Queue email only:** The email address from which you can receive inbound email.
Notes	Any additional information you want to provide about the credential.

10. Click **Save**.

    The credential is available for selection in components that use credentials.

Add and edit SNMP credentials

To streamline the management of SNMP credentials used in Inventory, Distribution, and Scripting, add those credentials to the *Credentials Management* page.

- You have the information required for SNMP authentication.
- You have administrator privileges in the **Administrator Console**

After you add credentials, you can select them on configuration pages instead of entering them manually each time. In addition, you can add credentials from any of the configuration pages that use them. Credentials added on configuration pages are automatically added to the *Credentials Management* page.

1. Go to the *Credentials Management* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Settings**, then click **Credentials**.
2. Select **Choose Action** > **New**.
3. On the *Add Credential* form, provide the following information:

Option	Description
Name	A unique name for the credential. This name appears on the *Credentials Management* list and in the credential selection drop-down lists in component sections, such as Scripting. This name is used for identification in **Administrator Console**, and it is not part of the actual credential.
Type	The classification of the credential. Select **SNMP** to specify SNMP credentials.

4. For SNMP v1 or v2c, provide the following information:

Option	Description
SNMP v1 or v2c	SNMP credentials that do not use authentication or encryption.
Community String	For SNMP v1 or v2c, the community string to query. The default is **Public**. The Public String is required for SNMP v1 or v2c.
Notes	Any additional information you want to provide about the credential.

5. For SNMP v3, provide the following information:

Option	Description
SNMP v3	SNMP credentials that require authentication and encryption algorithms to increase security.
Security Name	For SNMP v3, the name of the USM (user-based security model) user account. This account, and any passwords required for authentication and encryption, must be set up on target devices.
Security Level	For SNMP v3, the level of security. Security levels include: • **authPriv**: The highest level of SNMP v3 security, which uses both authentication and encryption. To use this level, you must specify all the SNMP V3 Authentication and Privacy settings. • **authNoPriv**: The mid-range of SNMP v3 security, which uses authentication only. Communications are not encrypted. To use this level, you must specify the Authentication settings. • **noAuthNoPriv**: The lowest level of SNMP v3 security. Communications are not encrypted.
Authentication Password	For SNMP v3, the password used to authenticate communications when **authPriv** or **authNoPriv** security levels are selected. This password is associated with the USM user and must be set up on target devices.
Protocol	For SNMP v3, the protocol used for communications. Protocols include: • **SHA**: Secure hash algorithm, SHA-1. • **MD5**: Message Digest 5. Faster than SHA, but considered to be less secure.
Privacy Password	For SNMP v3, the password used to authenticate communications when the **authPriv** security level is selected. This password is associated with the USM user and must be set up on target devices.
Protocol	For SNMP v3, the protocol used for the privacy password. Protocols include: • **DES**: Data Encryption Standard. This algorithm has a 56-bit key size and is considered to be less secure than AES. • **AES**: Advanced Encryption Standard. The appliance supports the 128-bit key size.
Notes	Any additional information you want to provide about the credential.

6. Click **Save**.

   The credential is available for selection in components that use credentials.

Add and edit Microsoft Office 365 OAuth credentials

To easily use Office 365 credentials used in Service Desk email communication, add them to the *Credentials Management* page.

- You have an Office 365 account, and have created a Microsoft Active Directory app in Microsoft Azure with a Client ID and Client Secret. For more information, visit https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-create-service-principal-portal.
- You have administrator privileges in the **Administrator Console**.

After you add credentials, you can select them in configuration pages instead of entering them manually each time. In addition, you can add credentials from any of the configuration pages that use them. Credentials added on configuration pages are automatically added to the *Credentials Management* page. The appliance does not validate stored Office 365 credentials as you enter them, but attempting to save any changes using invalid credentials result in an error.

NOTE: This feature is only available when SSL (secure) access to the appliance is enabled. For more information, see Configure security settings for the appliance.

1. Go to the *Credentials Management* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Settings**, then click **Credentials**.
2. Select **Choose Action** > **New**.
3. On the *Add Credential* form, specify credential properties:

Option	Description
Name	A unique name for the credential. This name appears on the *Credentials Management* list and in the credential selection drop-down lists in component sections, such as Service Desk email settings. This name is used for identification in **Administrator Console**, and it is not part of the actual credential.
Type	The classification of the credential. Select **Office365 OAuth** to specify credentials for Office 365.
Client ID	Your Office 365 Client ID.
Client Secret	Your Office 365 Client Secret.
Show typing	Show the characters in the *Client Secret* field on the *Add Credential* form. This option is available only when you are adding credentials. If you are editing existing credentials, the characters in the *Client Secret* field cannot be displayed.
Azure AD Tenant Type	Select your Azure AD tenant type from the available options. The tenant type must match the one selected when registering your Azure AD application in the Azure AD admin portal. • **Multitenant & Personal Microsoft Accounts - Default**: Use this option to grant access to the widest range of Microsoft identities and to enable multi-tenancy. All users with a work or school, or personal Microsoft account can access your application or API using this credential. It applies to schools and businesses that use Office 365 as

Option	Description
	well as personal accounts that are used to sign in to services like Xbox or Skype. This is the default setting. • **Azure AD directory - Multitenant**: Use this option to grant access to business or educational users, and to enable multitenancy. All users with a work or school account from Microsoft can use your application or API. This includes schools and businesses that use Office 365. • **Personal Microsoft Accounts only**: Use this option to grant access to personal accounts that are used to sign in to services like Xbox or Skype. • **Organizational directory only (Single tenant)**: Use this option to grant access to the users associated with your organization.
Authorize Credential	Click, log in, and grant access to the desired Office 365 account on the page that appears.
Azure AD Endpoint URL	Use this option to select required azure portal URL according to the region.
Azure AD Endpoint URL - Share the Azure URL	Use this option to select required azure portal URL according to the region.
Notes	Any additional information you want to provide about the credential.

4. Click **Save**.

   The credential is available for selection in components that use credentials.

View credential usage

You can view credential usage on the *Credentials Management* page.

- Credentials have been added to the *Credentials Management* page. See Managing credentials.
- You have administrator privileges in the **Administrator Console**.

1. Go to the *Credentials Management* page:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Settings**, then click **Credentials**.

   The *In Use* column shows the components using the credentials.
2. To sort the list, select a **Type** from the *View By* drop-down list above the table.

Create reports from the Credentials Management list

If history subscriptions are configured to retain credential information, you can generate reports that show when credentials were created, edited, and deleted.

- Credentials have been added to the appliance, and they appear on the *Credentials Management* page.
- History subscriptions are configured to retain credential information. See Configure object history.

When you create reports from the *Credentials Management* page, you can include information about the credentials, such as the name, type, creation date, and usage information. Authentication details, however, such as the password or client secret, are not included in reports.

NOTE: If the Organization component is enabled on your appliance, you create credential reports for each organization separately.

1. Go to the *Credentials Management* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Settings**, then click **Credentials**.
2. Select **Choose Action** > **Create Report**.
3. On the *Report Detail* page, provide a name for the report.
4. Select additional report settings, then click **Save**. See Create reports from list pages.

    The report appears on the Reports list.
5. To generate the report, select a format in the *Generate Report* column.

Export credentials information

You can export the list of credentials, or selected credentials, that appear on the *Credentials Management* page.

Credentials have been added to the appliance, and they appear on the *Credentials Management* page.

You can export information about the credentials, such as the name, type, the date the credential was last modified, and usage information. Authentication details, such as the password or Client Secret, cannot be exported.

NOTE: If the Organization component is enabled on your appliance, you export credential information for each organization separately.

1. Go to the *Credentials Management* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Settings**, then click **Credentials**.
2. Select **Choose Action** > **Export**, then select whether to export all credentials or only the selected credentials, and select the format for the exported information.
3. Open or save the exported file.

Delete credentials

You can delete credentials provided that they are not being used in any components, such as Inventory, Distribution, or Scripting.

- Credentials have been removed from any components that are using them. See View credential usage.
- You have administrator privileges in the **Administrator Console**

1. Go to the *Credentials Management* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Settings**, then click **Credentials**.
2. Select the check box next to the credentials you want to delete.

    NOTE: If any of the selected credentials are in use, an error message appears. You cannot delete groups of credentials if any of the selected credentials are in use.

3. Select **Choose Action** > **Delete**, then click **Yes** to confirm.

Configuring assets

You can configure assets and Asset Types as needed.

About the Asset Management component

The Asset Management component includes assets and Asset Types (templates). It enables you to manage assets added automatically through inventory and assets you add manually.

Default Asset Types include: Device, Cost Center, Department, License, Location, Software, and Vendor. You can create custom Asset Types as needed. See Customizing Asset Types.

Using the Asset Management component you can:

- **Manage items throughout their lifecycle**. Track software and other items from procurement to deployment, usage, and end of life. Or, track peripherals such as printers, network devices, and phones. See Identifying the assets to track.
- **Manage software License Compliance**. Track the licenses you own, as well as the number of copies of applications installed on devices. Options for managing License Compliance differ for items in the *Software Catalog* inventory and the *Software* page inventory. See Setting up License Compliance.
- **Track data**. Track purchase orders (POs) by entering each PO as an asset and linking it to the items purchased, received, and distributed. See Add License assets for Software page inventory.
- **Track physical assets**. Track physical assets, such as device hardware and software, as well as other physical assets, such as office furniture. You can track the use of these items as well as the status of their warranties. See Managing physical and logical assets.
- **Track logical assets**. Track logical assets, such as geographic locations, cost centers, departments, vendors, and so on. Logical assets are normally used as the basis for reporting. For example, logical assets answer questions such

as “how many devices does this department have?” and “when do the licenses we bought from a software vendor expire?” See Managing physical and logical assets.

- **Create and track relationships between assets**. Create peer-to-peer and parent-child relationships between assets. These relationships enable you to track assets by PO (purchase order), location, department, project, and other criteria. See Establishing relationships between asset fields.

Using the Asset Management Dashboard

The Asset Management Dashboard provides an overview of managed assets for the selected organization (if applicable), or the appliance.

If the Organization component is enabled on the appliance, and you are logged in to the Administrator Console (`http://`**appliance_hostname**`/admin`), the Asset Management Dashboard shows information for the selected organization. When you are logged in to the System Administration Console (`http://`**appliance_hostname**`/system`), the Asset Management Dashboard shows information for the appliance, including all organizations.

TIP: The appliance updates the summary widgets periodically. To update most of the widgets any time, click the icon and then the **Force Refresh** button. To update an individual widget, hover over the widget, then click the **Refresh** button above the widget. Some widgets may require additional steps.

About the Asset Management Dashboard widgets

Asset Management Dashboard widgets provide overviews of managed assets for the organization or appliance, as selected.

This section describes the widgets available on the *Asset Management Dashboard*. If the Organization component is enabled on your appliance, widgets show the information for the selected organization at the Admin level and for the appliance at the System level.

This dashboard provides a high-level overview of your asset usage. Use it to quickly review the state of your assets and look for any indicators that can improve your asset configuration. For example, you can focus on how your software licenses are used and identify which software titles need to have their license renewed.

Widget	Description
Assets By Type	This widget shows a donut chart, where each section of the chart indicates the percentage of your assets by their asset type, such as device, software, location, license, and others. Hovering over each section of the chart displays the percentage of the assets of the selected type.
Assets By Status	This widget shows a donut chart, where each section of the chart indicates the percentage of your assets by their status, such as Active, Disposed, Missing, or other. Hovering over each section of the chart displays the percentage of the assets in the selected status.
Cost ($) of Unused Licenses By Product	This widget shows a bar chart, where each bar represents the cost of unused licenses for each product. You can use this information to reassign or cancel unused licenses, and to redirect your resource where they are most needed.
License Compliance	If you have created License assets for software, this widget shows the number of Agent-managed devices that have a particular licensed software installed, and the number of licenses available. If the Organization component is enabled on your appliance, the widget shows the information for the selected organization. License assets can be created for applications listed on the *Software* page and the *Software Catalog* page, and the license mode for applications must be *Unit License* or *Enterprise* for license information to appear on this widget. Applications with other

Widget	Description
	license modes, such as *Shareware*, *Freeware*, or *Not Specified*, are not displayed on this widget. This widget is for information only, and the appliance does not enforce license compliance. For example, the appliance does not prevent software from being installed on Agent-managed devices if a license is expired or otherwise out of compliance. The following colors indicate threshold levels: • **Red**: Usage is at or above the critical threshold setting. • **Orange**: Usage is at or above the warning threshold setting but below the critical threshold setting. • **Green**: Usage is below the warning threshold setting. To change the threshold levels, see Configure appliance General Settings without the Organization component. For information about managing License assets, see Managing inventory.
Software Titles	This widget displays the software titles defined in the Software Catalog, with the highest number of installations on managed devices. If the Organization component is enabled on your appliance, the widget shows the information for the selected organization.
Software Publishers	This widget displays the publishers defined in the Software Catalog, with the highest number of software titles installed on managed devices. If the Organization component is enabled on your appliance, the widget shows the information for the selected organization.
Assets by Location	This widget shows a donut chart, where each section of the chart indicates the percentage of your assets by their location. Hovering over each section of the chart displays the percentage of the assets in the selected location.
Software Installed But Not Used in 60 Days	This widget shows a bar chart, where each bar represents a software title and the corresponding number of instances of that product that have not been in use in the last 60 days. You can use this information to further investigate whether these titles are needed, to reassign or uninstall unused software, and to redirect your resource where they are most needed.
Expiring Software License Maintenance	This widget shows a vertical bar chart, where each bar represents the number of software licenses that are about expire in the given time period.
Expired Software License Maintenance	This widget shows a donut chart representing the ration of expired and current licenses. Hovering over each section of the chart displays the percentage of the software licenses that are either expired or current, as selected.
Expiring Contracts	This widget shows a vertical bar chart, where each bar represents the number of contracts that are about expire in the given time period.
Expired Contracts	This widget shows a donut chart representing the ration of expired and current contracts. Hovering over each section of the chart displays the percentage of the contracts that are either expired or current, as selected.

Widget	Description
Software License Configuration	If you set up License assets for software, and specify the license type, such as site, subscription, or unit, that information is displayed in this widget. If the Organization component is enabled on your appliance, the widget shows the information for the selected organization.

Customize the Asset Management Dashboard

You can customize the Asset Management Dashboard to show or hide widgets as needed.

1. Go to the *Asset Management Dashboard*.
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Asset Management**, then click **Dashboard**.
2. Hover over the widget, then use any of the following buttons:
   # : Refresh the information in the widget.
   # : Display information about the widget.
   # : Edit the widget.
   # : Remove the widget.
   # : Resize the widget.
   # : Drag the widget to a different position on the page.
3. The widgets are editable, allowing you to filter the information that they display. To edit a widget, click and in the dialog box that appears, provide the required information. You can edit the chart type. Based on the chart type you select here from the drop down list, the relevant fields populate.
4. Click the button in the top-right corner of the page to view the list of available widgets.

   For information on how to add widgets to the dashboard refer Adding Widget to Asset Management Dashboard

Work with Asset Management Dashboard

When you click the icon, the dashboard settings panel displays. You get to see the following options:

Dashboard Name	Description
Dashboard Settings	You can customize the look and feel of the widgets. For more information, refer to Setting an Asset Management Dashboard
Add Widget	You can add a new widget. For more information, refer to Adding Widget to Asset Management Dashboard
Email Dashboard	You can share a dashboard snapshot through email. For more information, refer to Emailing an Asset Management Dashboard

Force Refresh	You can refresh all the widget data on the dashboard. For more information, refer to Refreshing Asset Management Dashboard Data Manually

Adding Widget to Asset Management Dashboard

You can add widgets to the Dashboard.

There is a list of widgets in the panel. You can enter a keyword in the Search text box to refine the list, then click on your selection.

To add widgets to the dashboard,

1. Click the icon to open the **Add Widget** panel.
2. Search for the desired widget in the following ways:
   - **In the Sort By drop-down, select the widget by title or newest.**
   - **In the Search field, enter a keyword to refine the list.**

   The refined result displays.
3. Click the desired widget.

   The widget gets added to the dashboard.

Setting an Asset Management Dashboard

You can customize the look and feel of the widgets and the dashboards.

You can change the color used in the dashboard charts, edit the dashboard name and its description, change the display of the widgets.

To customize a dashboard,

1. Click the icon to open the Dashboard Settings panel.
2. Make changes to the fields as required:

Fields	Description
Name	Add/Edit name for the dashboard. This is displayed on the dashboard.
Description	Add/Edit description of the dashboard. This describes the dashboard.
Choose Your Colors	Click on the color selector to choose your dashboard chart colors. Drag and drop the colors to arrange them in the desired order. The colors at the top of the list will be used first by each chart.
Layout	Chose one of the layout options. The widgets and other elements are displayed in the selected layout.

3. Click **Save**.

   The changes gets reflected on the dashboard.

Emailing an Asset Management Dashboard

You can share a dashboard snapshot through email, send it to multiple users, and configure the frequency of email.

To email a dashboard,

1. Click the icon to open the dashboard settings panel.
2. Click the Email Dashboard option to open the Email Dashboard panel.
3. Select appropriate option from the given options:
    a. **Send Now**: You can send an email immediately.
    b. **Schedule**: You can set the frequency of sending a snapshot of dashboard through email.

The detailed steps for each option are given below:

Send email now

To send email immediately,

1. Click **Send Now** to open the Email Dashboard dialog.
2. Enter details in the Email Address, Subject, and Message fields.
3. Choose the layout in which you want the widgets to appear.
4. Click Send.

The dashboard is sent through email.

Schedule

To set the frequency of sending a snapshot of dashboard through email,

1. Click **Schedule** to open the Schedule dialog.
2. Enter details in the Subject and **Message** fields.
3. Choose the layout in which you want the widgets to appear.
4. To add recipients, select the names from the **Select user to add drop down list**.

    NOTE: You can add multiple recipients from the list.

5. Select the frequency from the drop down list.
6. In the **Next Run** field that appears after you select the **Frequency**, set the date, month, and time for the next email delivery.
7. Click Save. The dashboard is sent through email according to the set schedule.

Refreshing Asset Management Dashboard Data Manually

You can refresh the widgets data to show the latest results on the dashboard.

To update the widgets,

1. Click the icon to open the dashboard settings panel.
2. Click **Force Refresh** to open the Confirm dialog box.
3. Click Yes to confirm refresh all widget data on the dashboard.

About managing assets

Assets are the entities that contain information about the devices, software, licenses, and other items you want to manage. Assets are based on Asset Types, which are templates used to create assets.

How asset information differs from inventory information

Asset and inventory information differ in the ways that the information is collected and managed.

The following table compares asset information and inventory information:

Item	Asset Component	Inventory Component
Where information appears	In the *Assets* section.	In the *Inventory* section.
The type of information managed	Asset information includes details about devices, software, licenses, physical assets, logical assets, and the relationships between them.	Inventory information includes details about devices and the software, processes, startup programs, and services on managed devices. The Software Catalog provides additional information about applications that are categorized as *Discovered* or *Not Discovered*.
How the information is managed	Asset information is static and changes only when you import data or change it manually. Device assets are exceptions to this rule, because Device assets are updated whenever managed devices report inventory. For License assets, however, the number of installations or seats is updated when managed devices report data to the appliance. Asset history is stored on the appliance and displayed in the **Administrator Console**; it remains with the asset until the asset is deleted.	Inventory information is automatically generated and overwritten each time managed devices report data to the appliance.
How licenses are tracked	The Asset Management component enables you to manage software License Compliance as well as physical and logical assets.	On the *Software* page, inventory information includes the number of Software assets, but it does not show the number of licenses. On the *Software Catalog* page, license information is displayed if License assets are associated with applications.

Identifying the assets to track

One of the first tasks in setting up Asset Management is identifying the assets to track.

Spreadsheets often contain asset details, such as purchasing data, vendor contact information, product keys, license details, and device information. These details are candidates for asset tracking.

You can import asset information into the Asset Management component to create assets that can be managed and tracked by the appliance. In addition, you can set up relationships among the imported assets to make the information more useful. For example, you can create License and Vendor assets, associate them with devices, and quickly identify devices related to a license or vendor. For information on importing asset information, see Importing license data in CSV files.

View assets and search for asset information

You can view assets and search for asset information as needed.

1. Go to the *Assets* list:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.

b. On the left navigation bar, click **Asset Management**, then click **Assets**.

2. To search across all Asset Types using the advanced search:
   a. In the *View By* drop-down list, select **All Items**.
   b. Click the **Filter** tab above the list to display the *Filter* panel.
   c. Specify the search criteria.

      For example, to search for all assets whose Vendor is Smith, specify the following criteria:

      ```
      Vendor | contains | Smith
      ```

   d. Click **Search**.

      Assets of any type, including Device, License, Software, or Vendor, that match the criteria appear.

   NOTE: You can save the search criteria applied. Click the **Save Filter** button, and then add filter name in the **Save Filter As** dialog box.

3. To search for an asset across all Asset Types using the simple search, in the **Search List** field, type full or partial contents of the field contained in the asset that you want to search for. For example, if you want to find an asset whose barcode contains zz, type it in the field, and press Enter.

   Assets that match the criteria appear.

4. To search a single Asset Type:
   a. In the *View By* drop-down list, select **Asset Type** > **Asset Type**.
   b. Click the **Filter** tab above the list on the right to display the *Filter* panel.
   c. Specify the search criteria.

      For example, to search for License assets that are scheduled to expire within the next two months, select the License Asset Type in the *View By* drop-down list, then specify the following criteria:

      ```
      Expiration Date | is within next | 2 months
      ```

   d. Click **Search**.

      License assets whose expiration date is within the next two months appear.

   NOTE: You can save the search criteria applied. Click the **Save Filter** button, and then add filter name in the **Save Filter As** dialog box.

Add barcodes to assets

You can view assets and search for asset information as needed.

Specify one or more barcode tags for the type of the asset for which you want to specify barcodes. For more information, see Add or customize Asset Types.

1. Go to the *Asset Detail* page:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Asset Management**, then click **Assets**.
   c. Click the name of an asset.

2. Under *Barcodes*, click +, and provide the following information:

Option	Description
Barcode Data	The barcode number. Barcode numbers are always unique, they cannot be shared between multiple assets. However, it is possible for an active asset to share a barcode with an archived asset.
Barcode Name	The barcode tag associated with this asset type. There can be only one barcode of the same type per asset.
Barcode Format	The barcode format. For example, UPC-A, Code 11, or UPC-E.

You can add as many barcodes as needed.

3. Optional. To see additional information about each barcode tag, such as its first or last scanned date, in the *Barcodes* area, click **Show all columns**. To return to the previous view with fewer columns per barcode, click **Show less columns**.
4. Click **Save**.

Change device owners

You can change asset and device owners as needed.

This topic describes the process of changing device owners using the Assets list. You can also change device owners using the *Asset Detail* or *Device Detail* page.

1. Go to the *Assets* list:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Asset Management**, then click **Assets**.
2. In the *View By* drop-down list, select **Asset Type > Device > All Device Subtypes**.
3. In the *Assets* list, select one or more devices that you want to assign to a specific owner.
4. Select **Choose Action** > **Assign to**.
5. In the *Assign To* dialog box that appears, click *Unassigned*, and select a user account that you want to assign as an owner of the selected assets.

The list that appears displays the full name, account name, and email address for each user.

6. Click **Save**.

The *Assign To* **dialog box closes and the** *Assets* **list refreshes, showing the asset owner name in the** *Assignee Name* **column.**

7. Add more owner-related columns to the *Assets* list.
    a. In the *Assets* list, click ⚙.
    b. Select any of the following options, as required, to view these columns in the *Assets* list: **Assignee Login**, **Assignee Email**, **Assignee Domain**, **Assignee Budget Code**, **Assignee Location**, **Assignee Role**, or **Assignee Locale**.

The selected columns appear in the *Assets* **list.**

8. If you changed the owner for a device, you can observe this change on the *Devices* list.
    a. On the left navigation bar, click **Inventory**, then click **Devices**.
    b. In the *Devices* list, observe the *Assignee Name* column of the row containing the device whose owner you changed.

The *Assignee Name* **column displays the name of the device owner**

TIP: Alternatively, you can change the asset or device owner on the *Asset Detail* or *Device Detail* page.

View and configure asset lifecycle settings

With the exception of locations, each asset type can have a status indicating its use or purpose, such as Active, Disposed, Expired, or others.

In order to configure applicable asset lifecycle settings, your user role must be granted a write-level *Asset Lifecycle* permission. To view asset lifecycle settings, a read-level permission is sufficient. For more information about user roles, see Managing Organization Roles and User Roles.

Use the *Asset Lifecycle Settings* page to view the list of existing asset status entries, and to add new ones, as required.

1. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
2. Complete one of the following steps:
   - **On the left navigation bar, click Asset Management, then click Assets.**
   - **On the left navigation bar, click Asset Management, then click Contracts.**
   - **On the left navigation bar, click Asset Management, then click Licenses.**
3. On the list page that appears, click **Choose Action** > **Configure Lifecycle Settings**.

   TIP: You can quickly change an asset status by selecting the asset on the list page, clicking **Choose Action** > **Change Asset Status**, and selecting the appropriate status in the *Change Asset Status* dialog box. Access to this command requires a write-level *Assets*, *Contracts*, or *Licenses* permission, as applicable. For more information about user roles, see Managing Organization Roles and User Roles.

   The *Asset Lifecycle Settings* page appears.
4. On the *Asset Lifecycle Settings* page, under *Asset Status*, review the list of default asset statuses.

   The following default asset statuses are available:

   # **Active**: Any asset that is deployed, active, or in use.
   # **Disposed**: An asset that is no longer available for use.
   # **Expired**: A software license or contract asset that has expired.
   # **In Stock**: A recently received asset.
   # **Missing**: Any asset that cannot be located.
   # **Repair**: An asset that is being repaired.
   # **Reserved**: An asset that is set aside for a specific person or use.
   # **Retired**: Any asset that reached its end-of-life state, or is no longer in use.
   # **Stolen**: An asset that has been reported as stolen.
5. Add, delete, or edit a custom asset status.

TIP: Default asset statuses cannot be modified or deleted.

- To add a new asset status, click +, specify the *Name* and *Description* for the asset status, and click **Add**.
- To delete a custom asset status, in the row containing the asset status, click .
- To edit a custom asset status, in the row containing the asset status, click , and edit the *Name* and/or *Description* of the asset status, as applicable.

6. If you made any changes to the *Asset Lifecycle Settings* page, click **Save**. Otherwise, click **Cancel** to return to the previous page.

Adding and customizing Asset Types and maintaining asset information

You can add or customize Asset Types as needed. You can also maintain real-time information on assets by scanning your network at regularly scheduled intervals.

In addition, you can add subtypes to your Asset Types. Asset Subtypes enable you to track asset properties, such as toner or ink levels of printers.

About Asset Types

Asset Types are templates for creating assets. Asset Types contain the fields and other information that define assets.

Default Asset Types include: Device, Cost Center, Department, License, Contract, Location, Purchase, Software, and Vendor, and you can add custom Asset Types as needed.

In addition, you can add Asset Subtypes and custom fields for any Asset Type. This is especially useful for collecting additional information about non-computer Device assets, such as printers. See About Asset Subtypes, custom fields, and device detail preferences.

Customizing Asset Types

You can rename fields, create fields, and delete fields in Asset Types as needed. Customizations to Asset Types are preserved during appliance updates.

About renaming fields and changing field types in Asset Types

When you rename a field in an Asset Type, the field is renamed in all assets that are based on the Asset Type. Values for the renamed field are retained.

However, if you change the **Type** to a type that does not support the data already entered in a field, that data is lost. For example, you might have a field named *Model Number* that is of the *Type*, *Text*, and that contains the value A123. If you change the *Type* from *Text* to *Number*, the system cannot convert A123 to a valid number. The value for the *Model Number* field is set to 0.

About adding and deleting asset fields

When you add a field to an Asset Type, the field is available to all assets of that type. Similarly, if you delete a custom asset field, that field, and any values entered in that field, are removed from all assets of that type.

For example, if you created a custom field named *BIOS Serial Number* in the Device Asset Type, that field would be available to all Device Asset Types. However, if you delete the *BIOS Serial Number* custom asset, that field, and any values entered in the field, are removed from all Device Asset Types.

If you delete an asset field, the asset association is removed from any assets that point to the deleted field.

Add or customize Asset Types

You can have as many custom Asset Types as you need. In addition, you can create custom fields in any Asset Type. When you create a custom field in an Asset Type, that field becomes available to all assets that are based on that Asset Type.

If the Organization component is enabled on your appliance, you add and customize Asset Types for each organization separately.

1. Go to the *Asset Type Detail* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Asset Management**, then click **Asset Types**.
    c. Display the *Asset Type Detail* page by doing one of the following:
    # Click the name of an Asset Type.
    # Select **Choose Action** > **New**.
2. In the *Name* field, in the General tab, add or change the name as needed.

    TIP: Additional options are available for Device and License Asset Types. See About customizing the Device Asset Type and Customize the License Asset Type.

3. **All asset types except Locations**. In the *Defaut Asset Status* field, under the *General* tab, enter a default asset status, or a custom one (if they exist).

    A default installation of the appliance includes the following asset statuses:

    # **Active**: Any asset that is deployed, active, or in use.
    # **Disposed**: An asset that is no longer available for use.
    # **Expired**: A software license or contract asset that has expired.
    # **In Stock**: A recently received asset.
    # **Missing**: Any asset that cannot be located.
    # **Repair**: An asset that is being repaired.
    # **Reserved**: An asset that is set aside for a specific person or use.
    # **Retired**: Any asset that reached its end-of-life state, or is no longer in use.
    # **Stolen**: An asset that has been reported as stolen.
4. If you want to allow users who do not have the Administrator role to delete assets of this type, select **Restrict Delete to built-in Administrator Role**. This option is turned off by default. Only administrators can configure this option. For other types of users, this field appears on the page, but it is disabled.

    For more information on user roles, see Add or edit User Roles.

5. If you want assets of this type to display the asset location in the asset details, select **Show Location settings**. This option is turned off by default.
6. **Asset Fields**. In the *Defaut Archive Asset Status* field, enter an asset status that you want to automatically assign to a device when it becomes archived.
7. If you want the instances of this asset type to use barcodes, specify one or more tags in the *Barcode Tags* tab.

    Any assets of this type that you create will have the barcode tags available for configuration. For example, if you specify a Corporate Tag and a Dell Asset Tag, barcodes identified with these two tags will be available for selection in on the *Asset Detail* page, when you create or edit an asset of this asset type.

To add a barcode, click +, type the barcode name, and click Save.

8. In the *Asset Fields* tab, click +.

   A new line appears.

9. Provide the following information:

Item	Description
Name	The name of the custom asset field, such as Asset Code, Purchase Date, or Building Address Line 1. This name appears on the form used to create assets of the selected Asset Type.
Available Values	The values that appear in fields that contain lists of values. This field is enabled when you select **Single Select** or **Multiple Select** from the *Type* drop-down list. If you select **Single Select** or **Multiple Select**, you must enter at least one value in this field. To use multiple values, separate each value with a comma.
Default Values	The value that appears in the field by default. If you select **Single Select** or **Multiple Select** from the *Type* drop-down list, you must type one of the values given in the *Available Values* field.
Required	Whether the field is mandatory or optional. If this check box is selected, users must enter a value in the field when creating assets of the selected type.
Type	The type of field. Field types include: • **Attachment**: Enables users to add attachments to the asset. • **Currency**: Used for monetary values. • **Software Catalog**: Enables users to associate the asset with an application in the Software Catalog. • **Publisher**: Enables user to associate the publisher info of an application to the asset. • **Date**: Used for calendar information. • **Label**: Enables users to associate a label with the asset. • **Link**: Used for Internet links. Links must be valid URLs, such as **http://quest.com**. • **Locale** : Enables user to associate the locale with an asset. • **Multiple Select**: Displays a list where multiple values can be selected. The maximum length for each value is 255 characters. • **Notes**: Used for additional information. • **Number**: Used for numerical values expressed as whole numbers. • **Parent**: Enables the asset to point to the same type of asset in a parent-child relationship. For example, you might allow Location types to have a Parent connection,

Item	Description
	allowing New York to point to a North America location. This can then be used in the reporting system to show all assets in North America. • **Single Select**: Displays a value list where only a single value can be selected. The maximum length for each value is 255 characters. • **Text**: Used for additional text. The maximum length is 255 characters. • **Timestamp**: Used to add a day and time to the record. • **User**: Used to associate user records with an asset. • **Assets Asset Type**: Used to specify relationships among Asset Types.
Multiselect	Whether the asset field points to other assets. A check box is enabled when you select **Assets Asset Type** from the *Type* drop-down list. Select the check box to allow this custom field to point to multiple records. For example, you might want a field to point to multiple devices that are approved for a particular license. In that case, you would select the check box. To create a single relationship field, such as a printer that is used by only one department, clear the check box. **NOTE:** When you create an asset, this field is populated with the available assets of the specified Asset Type. The field is empty if there are no assets of the specified type.
Section	**License assets only**. The tab on which this field appears on the *License Detail* page: *General*, *Purchase*, *Maintenance*, *Related*, *Custom*, or *Notes*. For more information about the tabs appearing on the *License Detail* page, see Add or edit licenses.
Device Section	**Device assets only**. The location, on the *Device Detail* page, where the field is reported. For example, if you are creating a printer Asset Subtype, with a field named *Toner Level*, you might select *Hardware* because that field is related to printer hardware. However, you can choose any section in the drop-down list for any field.

10. Click **Save** at the end of the row, then click **Save** at the bottom of the page.

Optional: Add Asset Subtypes for Asset Types. See Add Asset Subtypes and select Device Detail page preferences.

About customizing the Device Asset Type

Almost all Device asset data, whether displayed in the *Assets* or *Inventory* sections, originates from the *Assets* section.

The only device inventory or asset information that comes from the *Inventory* section is data for the *Mapped Inventory Field* and the *Matching Asset Field*. The values for those fields are collected each time devices are inventoried. During the inventory process, the appliance determines whether devices already have mapped assets. If no asset is found, the appliance creates one.

The default data type for *Mapped Inventory Field* is **System Name**, and the default data type for *Matching Asset Field* is **Name**. However, if you re-image your systems, the information under the old system name is lost to the Asset Management component. To prevent this loss, consider using BIOS serial numbers, IP addresses, MAC addresses, or something similar for tracking.

You can import Device asset data or change it manually in the *Assets section* any time.

CAUTION: If you change the default Asset Type, you lose the asset history prior to the change because the appliance automatically creates assets with the new information. Therefore, it is important to decide whether you want to change the default values as early as possible in the setup process.

Example: Add custom fields to the Device Asset Type

This example shows how to add fields to the Device Asset Type and select them in the *Mapped Inventory Field* and the *Matching Asset Field*.

1. Go to the *Asset Type Detail* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Asset Management**, then click **Asset Types**.
    c. Click the **Device** Asset Type.
2. In the **Asset Fields** tab, click the **Add** button on the right side of the page: +.

    A new line appears.
3. Provide the following information:
    a. In the *Name* field, enter BIOS Serial Number.
    b. In the *Type* drop-down list, select **Text**.
4. Click **Save** at the end of the row, then add a row:
    a. Click the **Add** button: +.

        A new line appears.
    b. Provide the following information for the new line:

        In the *Name* field, enter Serial Number.

    In the *Type* drop-down list, select **Text**. Reserve the **Number** *Type* for fields on which you perform calculations. Using the **Number** *Type* might strip leading zeros in a serial number.
5. Click **Save** at the end of the row, then add a row:
    a. Click the **Add** button: +.

        A new line appears.
    b. Provide the following information for the new line:

        In the *Name* field, enter Purchase Date.

    In the *Type* drop-down list, select **Text**.
6. Click **Save** at the end of the row, then add a row:
    a. Click the **Add** button: +.

        A new line appears.
    b. Provide the following information for the new line:

        In the *Name* field, enter Location.

    In the *Type* drop-down list, select **Asset Location**.
7. Click **Save** at the end of the row.
8. In the **General** tab, in the *Mapped Inventory Field* drop-down list, change the value to **BIOS Serial Number**.
9. In the *Matching Asset Field*, select **Serial Number**.
10. Click **Save** at the bottom of the page.

Establishing relationships between asset fields

You can edit Asset Types to establish relationships among assets and track them together.

These relationships can be:

- Peer-to-peer, such as printer and device.
- Parent-child, such as a cost center and the devices associated with it.

Example: Add fields to the Location Asset Type shows how to make a parent-child relationship with locations by adding a field to the Location Asset Type.

Example: Add fields to the Location Asset Type

You can add fields to the Location Asset Type as needed.

1. Go to the *Asset Type Detail* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Asset Management**, then click **Asset Types**.
    c. Click the **Location** Asset Type.
2. In the **Asset Fields** tab, click the **Add** button on the right side of the page: +.

    A new line appears.
3. In the *Name* field, enter Parent Location.
4. In the *Type* drop-down list, select **Parent**.
5. Click **Save** at the end of the row, then click **Save** at the bottom of the page.

When you open a Location asset, the *Parent Relationship* field is shown on the *Asset Detail* page.

Add parent relationships to Location assets

Parent-child relationships can be useful when managing assets, such as Location assets.

Add *Parent Location* custom fields as described in Example: Add fields to the Location Asset Type.

When adding parent relationships, start with the highest level (parent level) in the relationship.

1. Go to the *Assets* list:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Asset Management**, then click **Assets**.
2. **Optional**: In the *View By* drop-down list, which appears above the table on the right, select **Asset Type** > **Location**.

    The view is restricted to Location assets.
3. If the highest level (parent level) Location asset does not exist, create it:
    a. Select **Choose Action** > **New** > **Location** to display the *Location Asset Detail* page.
    b. Enter the name for the new field. For example, Western Division.
    c. Leave the *Parent Location* **Unassigned**, then click **Save** to display the *Assets* page.

    NOTE: The *Parent Location* field is a user-created custom field.
4. If the second-level asset exists, select it. If the second-level asset does not exist, create it:
    a. Select **Choose Action** > **New** > **Location** to display the *Location Asset Detail* page.
    b. Enter the name for the new asset. For example, San Jose.
    c. For this example, select **Western Division** for the *Parent Location*. If you have many Location assets, enter the first characters in the *Filter* field to limit the choices available in the *Parent Location* field.
5. Click **Save**.
6. Create additional Location assets as needed.

For example, you could create Location assets for each building on a campus or each rack in a data center.

Delete Asset Types

You can delete Asset Types, provided that no assets are assigned to those types.

You have Asset Types that do not have any assets assigned to them.

1. Go to the *Asset Types* list:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Asset Management**, then click **Asset Types**.
2. Click the check box next to an Asset Type.
3. Select **Choose Action** > **Delete**, then click **Yes** to confirm.

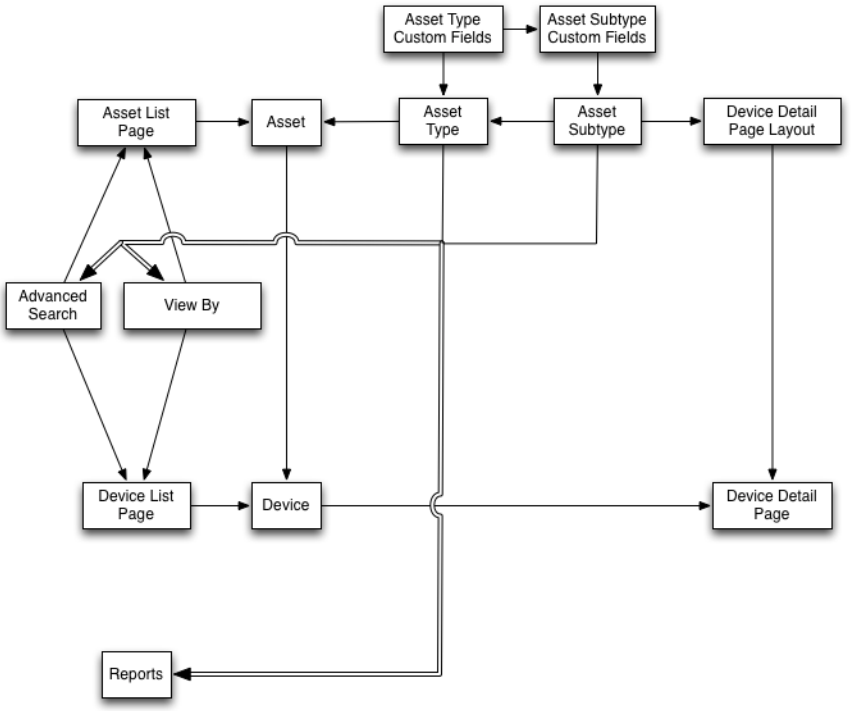
About Asset Subtypes, custom fields, and device detail preferences

Asset Subtypes are subcategories of assets that you can add to any Asset Type, including custom Asset Types. This enables you to identify and manage subtypes of assets, such as Device assets that are computers, printers, or routers, and Software assets that run on Windows, Mac, or Linux systems in the appliance inventory.

Asset Subtypes inherit the fields from the Asset Type, and you can add custom fields to enable the appliance inventory process to collect relevant information about the Asset Subtype. For example, you could add the Asset Subtype **Printer** to the **Device** Asset Type. You could then add a custom field for the **Printer** subtype, such as *Toner*. The *Toner* field would then be available to Device Assets with the subtype *Printer*.

NOTE: To enable the appliance to populate Asset Subtype fields from Agentless devices, you must assign the appropriate Asset Subtype when the device is configured, you must obtain the appropriate object identifier (OID), and you must map that identifier to the subtype field on the *SNMP Inventory Configuration Detail* page. You cannot add or change SNMP device subtypes after they have been configured. See Obtain a list of object identifiers (OIDs) using the Administrator Console.

In addition, you can choose whether to show or hide the details that appear for each Device Asset Subtype on the *Device Detail* page. For example, you can hide information that is irrelevant to printers, such as *Installed Programs*, *Discovered Software*, and *Metered Software*, from the *Device Detail* page of assets with the subtype **Printer**.



Workflow for using Asset Subtypes with SNMP devices

To use Asset Subtypes, you need to add them, and any custom fields you want to use, to your Asset Types. To populate the fields with data from SNMP (Simple Network Management Protocol) devices, you can also add object identifiers (OIDs) to the custom fields.

The workflow for using Asset Subtypes with SNMP devices includes these tasks:

1. Add a Device Asset Subtype to the Asset Type, and add custom fields to the subtype. See Add Asset Subtypes and select Device Detail page preferences.
2. Add assets that use the Asset Type and Asset Subtype. See Assign or change Device Asset Subtypes from the Devices page.

   IMPORTANT: You must assign the appropriate Asset Subtype when the device is configured. You cannot add or change SNMP device subtypes after they have been configured.

3. **Optional**: Populate the fields:

   # To enable the system to populate fields with data from SNMP devices, obtain the object identifiers (OIDs) to use for the custom fields, then add the field for Agentless devices on the *SNMP Inventory Configuration Detail* page, select the Asset Subtype, then add the OID information for the fields. See Obtain a list of object identifiers (OIDs) using the Administrator Console.

   # Manually update the fields as needed. See Update custom asset fields manually.

Add Asset Subtypes and select Device Detail page preferences

You can add Asset Subtypes to any Asset Type, including custom Asset Types, and you can add custom fields for each Asset Subtype.

In addition, you can choose which fields to display on the *Device Detail* page, and the sections where you want those fields to appear. This enables you to customize the *Device Detail* page and emphasize the most important information.

NOTE: If the Organization component is enabled on your appliance, you manage Asset Subtypes for each organization separately.

1. Go to the *Asset Type Detail* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Asset Management**, then click **Asset Types**.
    c. Display the *Asset Type Detail* page by doing one of the following:
    # Click the name of an Asset Type.
    # Select **Choose Action** > **New**.
2. In the *Subtypes* tab, click **Add Subtype**.

    NOTE: In a default installation, Device Assets include two Asset Subtypes for printer devices: *Laser Printer: Color* and *Laser Printer: Monochrome*. Each of these subtypes provides a common set of fields that apply to most printers. The appliance also comes with a set of printer templates for typical SNMP-enabled printer models, based on these Asset Subtypes. You can edit these templates or add new ones, as needed. When you apply a printer template to a device, the data defined in the template, such as toner levels or descriptions, is collected for the printer in the next inventory cycle. For more information, see About printer templates.

    The *Asset Subtype Detail* page appears. The *Inherited Fields* section shows fields that are available to the Asset Subtype because they have been added to the Asset Type. The *Inherited Fields* are hidden by default. You must click the *Inherited Fields* link to display the field.
3. In the top section, provide the following information and choose whether to make the Asset Subtype the default:

Option	Description
Name	The name of the Asset Subtype. This name appears in the list on the *Asset Type Detail* page.
Default	Whether to use the Asset Subtype as the default for new assets of the selected type. If you select this check box, new assets of the selected type are automatically assigned to this Asset Subtype. You can change this setting any time.

4. In the *Subtype Fields* section, click the **Add** button in the heading row on the right side of the table: +.
5. Provide the following information:

Item	Description
Name	The name of the Asset Subtype. This name identifies the Asset Subtype on the *Asset Detail* page.
Available Values	The values that appear in fields that contain lists of values. This field is enabled when you select **Single Select** or **Multiple Select** from the *Type* drop-down list. If you select **Single Select** or **Multiple Select**, you must enter at least one value in this field. To use multiple values, separate each value with a comma.
Default Values	The value that appears in the field by default. If you select **Single Select** or **Multiple Select** from the *Type* drop-down list, you must type one of the values given in the *Available Values* field.
Required	Whether the field is mandatory or optional. If this check box is selected, users must enter a value in the field when creating assets of the selected type.

Item	Description
Type	The type of field. Field types include: • **Attachment**: Enables users to add attachments to the asset. • **Currency**: Used for monetary values. • **Software Catalog**: Enables users to associate the asset with an application in the Software Catalog. • **Publisher**: Enables user to associate the publisher info of an application to the asset. • **Date**: Used for calendar information. • **Label**: Enables users to associate a label with the asset. • **Locale** : Enables user to associate the locale with an asset. • **Link**: Used for Internet links. Links must be valid URLs, such as **http://quest.com**. • **Multiple Select**: Displays a list where multiple values can be selected. The maximum length for each value is 255 characters. • **Notes**: Used for additional information. • **Number**: Used for numerical values expressed as whole numbers. • **Parent**: Enables the asset to point to the same type of asset in a parent-child relationship. For example, you might allow Location types to have a Parent connection, allowing New York to point to a North America location. This can then be used in the reporting system to show all assets in North America. • **Single Select**: Displays a value list where only a single value can be selected. The maximum length for each value is 255 characters. • **Text**: Used for additional text. The maximum length is 255 characters. • **Timestamp**: Used to add a day and time to the record. • **User**: Used to associate user records with an asset. • **Assets Asset Type**: Used to specify relationships among Asset Types.
Multiselect	Whether the asset field points to other assets. A check box is enabled when you select **Assets Asset Type** from the *Type* drop-down list. Select the check box to allow this custom field to point to multiple records. For example, you might want a field to point to multiple devices that are approved for a particular license. In that case, you would select the check box. To create a single relationship field, such as a printer that is used by only one department, clear the check box. **NOTE:** When you create an asset, this field is populated with the available assets of the specified Asset Type. The field is empty if there are no assets of the specified type.
Device Section	The location, on the *Device Detail* page, where the field is reported. For example, if you are creating a printer Asset Subtype, with a field named *Toner Level*, you might select *Hardware* because that field is related to printer hardware. However, you can choose any section in the drop-down list for any field.

6. Click **Save** at the end of the row.
7. For Device Asset Subtypes, choose the information you want to show or hide on the *Device Detail* page:
    a. Scroll down to *Subtype, Device Details: Show/Hide sections*.

b. Select the check boxes next to the items you want to show.

For a printer subtype, you might want to show *Inventory Information* **such as** *Hardware*, *Printers*, *Network Interfaces*, **and** *SNMP Data*.

c. Clear the check boxes next to the items you want to hide.

For a printer subtype, you might want to hide the *Software* **and** *Dell Command | Monitor* **sections because they are not relevant to printers.**

8. Click **Save** at the bottom of the page.

To enable the system to automatically populate custom fields with data on the *Device Detail* page, you must obtain the appropriate object identifiers and map the fields OIDs. See:

- Map Object Identifiers to fields in the inventory table
- Obtain a list of object identifiers (OIDs) using the Administrator Console

To manually update custom fields, go to the *Asset Detail* page. See Update custom asset fields manually.

Edit Asset Subtypes

You can edit Asset Subtypes as needed. If the Organization component is enabled for your appliance, you edit Asset Subtypes for each organization separately.

1. Go to the *Asset Type Detail* page:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Asset Management**, then click **Asset Types**.
   c. Click the name of an Asset Type to display the *Asset Type Detail* page.
2. In the *Subtypes* tab click the **Edit** button next to the subtype you want to edit: .

   The *Asset Subtype Detail* **page appears. For information on the options available to Asset Subtypes, see Add Asset Subtypes and select Device Detail page preferences.**
3. Click **Save** at the end of the row, then click **Save** at the bottom of the page.

Set an Asset Subtype as the default

To automatically assign new assets to a subtype, you can mark an Asset Subtype as the default.

1. Go to the *Asset Type Detail* page:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Asset Management**, then click **Asset Types**.
   c. Display the *Asset Type Detail* page by doing one of the following:
   # Click the name of an Asset Type.
   # Select **Choose Action** > **New**.
2. In the *Subtypes* tab click the **Edit** button next to the subtype you want to edit: .

   The *Asset Subtype Detail* **page appears.**
3. In the top section, select the check box next to *Default*.
4. Click **Save** at the end of the row, then click **Save** at the bottom of the page.

   The Asset Subtype is marked as the default subtype for the Asset Type. New assets of the selected type are automatically assigned to this Asset Subtype.

View subtypes available to Asset Types

You can view the Asset Subtypes that are available to the Asset Types you manage. If the Organization component is enabled for your appliance, you view and manage Asset Subtypes for each organization separately.

- Go to the *Asset Type Detail* page:

    1. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    2. On the left navigation bar, click **Asset Management**, then click **Asset Types**.
    3. Display the *Asset Type Detail* page by doing one of the following:

    # Click the name of an Asset Type.

    # Select **Choose Action** > **New**.

    The subtypes available to the Asset Type are listed in the *Subtypes* table.

View Asset Subtypes on the Assets page

You can use the *View By* menu to sort the *Assets* page by subtypes.

1. Go to the *Assets* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Asset Management**, then click **Assets**.

    The *Subtypes* column shows the subtype assignments for assets. None indicates that the asset is not assigned to a subtype.
2. To view the subtypes assigned to a specific Asset Type, go to the *View By* menu in the upper right and select an Asset Type.
3. To view a single subtype for an Asset Type, go to the *View By* menu, select an Asset Type, then select a subtype.

    Fields related to the subtype, such as *Ink Level* for a *Printer* subtype, appear as columns on the *Assets* page.

Assign or change Device Asset Subtypes from the Devices page

If you have existing Device assets that are not assigned to subtypes, you can assign them to subtypes or change their subtype assignments, from the *Devices* page, provided that those devices are not SNMP (Simple Network Management Protocol) devices. Subtypes for SNMP devices must be assigned when the devices are initially configured.

You have existing device assets in appliance inventory and you have created subtypes for the Device Asset Type. See Add Asset Subtypes and select Device Detail page preferences.

IMPORTANT: For SNMP devices, you must assign the appropriate Asset Subtype when the device is configured. You cannot add or change SNMP Asset Subtypes after they have been configured.

1. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
2. Select **Inventory** > **Devices** to display the *Devices* page.
3. To filter the list to show only those devices that are assigned to a subtype:
    a. Click the **Filter** tab above the list on the right to display the *Filter* panel.
    b. Specify the criteria required to find devices.
    c. Click **Search**.

TIP: You can also use the *View By* drop-down list to identify devices that belong to a specific Asset Subtype.

4. Select the check boxes next to the devices you want to assign to a subtype. To select all devices, click the check box next to *Name* at the top of the table.
5. Select **Choose Action** > **Change Subtype to**.

   The subtype is selected, and the change is reflected on the *Device Detail* page the next time inventory is reported for the device.

Assign assets to subtypes or change subtype assignments from the Assets page

If you have existing assets that are not assigned to Asset Subtypes, you can assign them to subtypes or change their subtypes, from the *Assets* page, provided that those devices are not SNMP (Simple Network Management Protocol) devices. Subtypes for SNMP devices must be assigned when devices are initially configured.

You have existing assets in appliance inventory and you have created subtypes for Asset Types. See Add Asset Subtypes and select Device Detail page preferences.

IMPORTANT: For SNMP devices, you must assign the appropriate Asset Subtype when the device is configured. You cannot add or change SNMP Asset Subtypes after they have been configured.

1. Go to the *Assets* list:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Asset Management**, then click **Assets**.
2. To filter the list to show only those assets that are assigned to a subtype:
   a. Click the **Filter** tab above the list on the right to display the *Filter* panel.
   b. Specify the criteria required to find the assets whose subtypes you want to assign or change.
   c. Click **Search**.

   TIP: You can also use the *View By* drop-down list to identify assets that belong to a specific Asset Subtype.
3. Select the check boxes next to the assets you want to assign to a subtype. To select all assets, click the check box next to *Name* at the top of the table.
4. Select **View By** > **Asset Type** > **Device**, and select one of the available entries in the list. For example, to display all device assets, select **All Device Subtypes**.
5. Select **Choose Action** > **Change Subtype to**.

   The selected assets are assigned to the selected subtype.

Update custom asset fields manually

You can update custom asset fields manually as needed. This is useful when you have asset information that cannot be collected automatically, or supplemental information you want to track with an asset.

You have added custom Asset Subtypes or custom asset fields.

TIP: As an alternative to manually updating custom assets fields, you can import information from spreadsheets. See Importing license data in CSV files.

1. Go to the *Asset Detail* page:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Asset Management**, then click **Assets**.

c. Click the name of the asset you want to update.

2. Modify the custom asset fields as needed.
3. Click **Save**.

Delete Asset Subtypes

You can delete Asset Subtypes provided that no assets are assigned to those subtypes.

You have Asset Subtypes that do not have any assets assigned to them.

1. Go to the *Asset Type Detail* page:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Asset Management**, then click **Asset Types**.
   c. Click the name of an Asset Type to display the *Asset Type Detail* page:
2. In the *Subtypes* section click the **Delete** button next to the subtype you want to edit: .
3. In the dialog window, click **Yes**.

   The Asset Subtype is deleted from the Asset Type, and any related fields are removed immediately.

Managing Software assets

You can customize the Software Asset Type, and add Software assets for applications in the *Software* page inventory as needed.

Software assets can be added for *Software* page inventory only. Software assets are not required for applications in the Software Catalog inventory.

Customize the Software Asset Type

You can add, change, or delete the fields available to the Software Asset Type as needed. The Software Asset Type is the template that determines the fields available when you add Software assets.

If the Organization component is enabled on your appliance, you customize the Software Asset Type for each organization separately.

1. Go to the *Asset Type Detail* page:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Asset Management**, then click **Asset Types**.
   c. In the **Name** column, click **Software**.
2. **Optional**: Modify fields or values on the *Asset Fields* table.
   a. Click the **Edit** button at the end of a row: .
   b. Change the field information as needed, then click **Save** at the end of the row.
   c. To add a field, click the **Add** button in the table heading: +. Add field information, then click **Save** at the end of the row.
   d. To change the order of fields, click the **Reorder** button at the end of the row: .
   e. To remove a field, click the **Delete** button: .
3. Click **Save** at the bottom of the page.

Adding Software assets

Software assets enable you to track information about applications in the *Software* page inventory. For example, after you add Software assets for applications, you can associate those assets with License assets to track license information.

You can create Software assets for applications that have been added to the appliance automatically or manually.

NOTE: Software assets are not required to set up License Compliance for applications in the *Software Catalog* inventory. See About License Compliance for Software Catalog applications.

If the Organization component is enabled on your appliance, you create Software assets for each organization separately.

Add Software assets on the Software list

You can add Software assets for one or more applications at once by selecting applications on the *Software* list.

Software assets can be added for *Software* list inventory only. Software assets are not required for applications in the Software Catalog inventory.

1. Go to the *Software* list:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Inventory**, then click **Software**.
2. Select the check box next to one or more applications.
3. Select **Choose Action** > **Create Asset**.

The assets are created, and they appear on the *Assets* list.

Add Software assets in the Assets section

You can create Software assets one-at-a-time in the *Assets* section.

Software assets can be added for *Software* list inventory only. Software assets are not required for applications in the Software Catalog inventory.

1. Go to the *Software Asset Detail* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Asset Management**, then click **Assets**.
    c. Select **Choose Action** > **New** > **Software**.
2. Complete the asset fields as follows:

Option	Description
Name	The asset name. For example, Office Pro SW Asset.
Subtype	The asset subtype, if applicable.
Asset Status	The asset status, if applicable. You can select a default asset status, or a custom one (if they exist).

Option	Description
	A default installation of the appliance includes the following asset statuses: • **Active**: Any asset that is deployed, active, or in use. • **Disposed**: An asset that is no longer available for use. • **Expired**: A software license or contract asset that has expired. • **In Stock**: A recently received asset. • **Missing**: Any asset that cannot be located. • **Repair**: An asset that is being repaired. • **Reserved**: An asset that is set aside for a specific person or use. • **Retired**: Any asset that reached its end-of-life state, or is no longer in use. • **Stolen**: An asset that has been reported as stolen. For more information, see View and configure asset lifecycle settings.
Location	Select the location for this asset from the drop-down list. The values in this list contain all locations defined on the appliance. See Managing locations **TIP:** Locations can be defined for all default asset types, including Cost Centers, Departments, Devices, Licenses, Software, and Vendors.
Software	The name of the application to associate with the asset. To search for items, begin typing in the field.
Software Label	Select a label from the drop-down list. The list is empty unless you have created a Smart Label. You can type in the box to look for specific labels.
Barcode Data	Review or add barcodes that you want to associate with this asset. See Add barcodes to assets.
Barcode Name	
Barcode Format	

a. In the *Name* field, enter a name for the asset. For example, Office Pro SW Asset.
b. **Optional**: In the *Software* field, select the name of the application to associate with the asset. To search for items, begin typing in the field.
c. **Optional**: In the *Software Label* field, select a label in the *Select label* drop-down list. The list is empty unless you have created a Smart Label. To filter the labels list, enter a few characters of the label name in the *Filter* field.

3. Click **Save**.

The new asset appears on the *Assets* list.

Managing physical and logical assets

Physical assets include device hardware and software, as well as other physical assets, such as office furniture. Logical assets include locations, cost centers, and vendors.

The appliance Inventory component automatically provides the Asset Management component with information about physical assets, such as devices, that report software and hardware inventory to the appliance. For physical and logical assets that do not report inventory to the appliance, however, information is added and updated manually. See Update custom asset fields manually.

Managing logical assets enables you to:

- Identify and protect logical assets.
- Establish relationships between logical assets and use them in reports. For example, geographical relationships or the relationships of business entities.

You can also add custom logical assets, such as support contracts, to track additional metadata about those objects.

Add physical Asset Types

You can add physical Asset Types as needed.

1. Go to the *Asset Type Detail* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Asset Management**, then click **Asset Types**.
    c. Select **Choose Action** > **New**.
2. In the *Name* field, under the *General* tab, enter a descriptive name for the asset, such as Laptop.
3. In the *Defaut Asset Status* field, under the *General* tab, enter a default asset status, or a custom one (if they exist).

    A default installation of the appliance includes the following asset statuses:

    # **Active**: Any asset that is deployed, active, or in use.
    # **Disposed**: An asset that is no longer available for use.
    # **Expired**: A software license or contract asset that has expired.
    # **In Stock**: A recently received asset.
    # **Missing**: Any asset that cannot be located.
    # **Repair**: An asset that is being repaired.
    # **Reserved**: An asset that is set aside for a specific person or use.
    # **Retired**: Any asset that reached its end-of-life state, or is no longer in use.
    # **Stolen**: An asset that has been reported as stolen.
4. If you want to allow users who do not have the Administrator role to delete assets of this type, select **Restrict Delete to built-in Administrator Role**. This option is turned off by default. Only administrators can configure this option. For other types of users, this field appears on the page, but it is disabled.

    For more information on user roles, see Add or edit User Roles.
5. If you want assets of this type to display the asset location in the asset details, select **Show Location settings**. This option is turned off by default.
6. Under *Barcodes*, click +, and provide the following information:

Option	Description
Barcode Data	The barcode number. Barcode numbers are always unique, they cannot be shared between multiple assets. However, it is possible for an active asset to share a barcode with an archived asset.
Barcode Name	The barcode tag associated with this asset type. There can be only one barcode of the same type per asset.
Barcode Format	The barcode format. For example, UPC-A, Code 11, or UPC-E.

You can add as many barcodes as needed.

7. Click the **Add** button on the right side of the page: +.

   A new line appears.
8. Provide the following information in the new line. For example:
   a. In the *Name* field, enter Brand.
   b. In the *Required* column, select the check box to make the field required.
   c. In the *Type* drop-down list, select **Single Select**.

      The *Available Values* field is enabled.
   d. Go back to the *Available Values* field and enter the brands you use. These will appear in the select list. Separate each brand with a comma.

      For example: Apple, Dell, IBM. This ensures that brand names, such as IBM, are referred to consistently instead of using variations, such as IBM and International Business Machines.
9. Click **Save** at the end of the row, then add a row:
   a. Click the **Add** button: +.
   b. Provide additional information in the new line.

   For example:

   # In the *Name* field, enter Serial Number.
   # In the *Type* drop-down list, select **Text**.
10. Click **Save** at the end of the row, then add a row:
    a. Click the **Add** button: +.
    b. Provide additional information in the new line.

       For example:

    # In the *Name* field, enter Location.
    # In the *Type* drop-down list, select **Asset Location**.
11. Click **Save** at the end of the row, then add a row:
    a. Click the **Add** button: +.
    b. Provide additional information in the new line.

       For example:

    # In the *Name* field, enter Department, and in the *Type* drop-down list select **Asset Department**.
    # In the *Name* field, enter Cost Center, and in the *Type* drop-down list select **Asset Cost Center**.
12. Click **Save** at the end of the row, then add a row:
    a. Click the **Add** button: +.

b. Provide additional information in the new line.

For example:

In the *Name* field, enter Warranty Expiration.

In the *Type* drop-down list, select **Date**. The format is **yyyy-mm-dd**. The supported range is 1000-01-01 to 9999-12-31.

13. Click **Save** at the end of the row, then click **Save** at the bottom of the page.

Archive device Assets

You can archive device Assets as needed.

Appliance administrators can archive device Assets that are no longer in use. When you archive a device Asset, that device is no longer included in the node license count for the appliance. Devices marked for archiving are archived after a pre-defined number of days, as specified in the General Settings. The default period is three days. This allows administrators to revert the device from being marked from archiving, if needed.

For more information about changing the length of time during which device Assets are marked for archiving, see Configure Admin-level or organization-specific General Settings

Once a device is archived, its record is deleted, and it can no longer be reverted to the previous active state. You can review the device details for an archived device Asset, if required.

1. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
2. On the left navigation bar, click **Assets**.
3. Complete one of the following steps:
   - **On the *Assets* list, select a device Asset. Select Choose Action > Archive.**
   - **On the *Assets* list, click the name of a device Asset. On the *Asset Detail* page that appears, click Archive.**
4. In the *Archive Asset* dialog box that appears, in the *Archive Reason* field, type the reason for this action, and click **Save**.

   The *Archive Asset* dialog box closes, and the *Assets* list refreshes, indicating that the device Asset is in the Pending Archive state ( ). When the Pending Archive period expires, the appliance archives the device Asset, and it enters the Archived state ( ).
5. If you want to remove a device Asset from the Pending Archive state:
   a. On the *Assets* list, click the name of a device Asset that is in the Pending Archive state.
   b. On the *Asset Detail* page that appears, click **Undo Pending Archive**.

   The *Asset Detail* page closes, and the *Assets* list refreshes, indicating that the device Asset is no longer in the Pending Archive state.
6. If you want to review the device details for an archived device Asset, on the *Assets* list, in the *Name* column, click the device name enclosed in brackets.

   The *Device Details* page appears. This page contains a subset of the information typically shown for a non-archived device Asset. For more information about the fields appearing on this page, see Groups and sections of items in device details.

Maintaining and using manual asset information

For assets that do not report inventory to the appliance automatically, you can manually add asset information. This is useful for logical assets such as locations, cost centers, and vendors, and physical assets, such as office furniture and equipment. Asset information that is imported or added manually must be updated manually when that information changes.

There are two ways to keep manual asset information up to date:

- Manage the information in spreadsheets and re-import them to the appliance periodically.
- Maintain the information manually in the Asset Management component.

Whichever method you choose, use it consistently to ensure that data remains current.

Creating an asset administrator role

You can create an asset administrator role to permit other users to update assets in the appliance.

For information on creating roles, see Setting up roles for user accounts.

Scheduling regular imports

To maintain asset information efficiently, you can continue updating source spreadsheets. Each time you import, the Asset Management component determines whether to import or update records based on what was designated as the primary key (PK) when the asset was created:

- If the primary key matches an existing record, the Asset Management component compares the data and updates the existing record.
- If there is no matching primary key in the row, a new record is generated.

See Importing license data in CSV files.

TIP: Before importing new data, consider running a report to export the current data. That way you can return to the original data if there is anything wrong with the structure of the new data.

Using asset data in reports

You can export data from the Asset Management component in standard reports.

Some standard reports are:

- **Unapproved Software Installation**: Software found on devices where no license has been approved.
- **Software Compliance Simple**: License counts, such as those found on the *Assets* list.
- **Software License Compliance Complete**: A list of software and devices that are impacted by each license.

In addition, you can create your own reports. See About reports.

Managing locations

A location entity represents a physical site that contains one or more of your assets.

You can add, move, or delete location entities, as needed.

Manage locations

Locations represents physical sites containing one or more of your assets. They are based on location types.

You can add, move, or delete location entities, or export location details into a file, as needed.

1. Go to the *Locations* list:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Asset Management**, then click **Locations**.
2. To add a location, select **Choose Action** > **New**.

    See Add or edit locations for more information.
3. To delete a location:
    a. Select the row containing the location that you want to delete.
    b. Select **Choose Action** > **Delete**.
    c. **Optional**. In the *Delete location* dialog box that appears, specify the replacement location to which you want to move all the assets associated with the location you are about to delete.
    d. Click **Confirm**.

    NOTE: Deleting a parent location does not remove its child locations from the system.
4. To move a location:
    a. Select the row containing the location that you want to move.
    b. Select **Choose Action** > **Move**.
    c. In the *Move location* dialog box that appears, specify the parent location to which you want to move the location.
    d. Click **Confirm**.

    The *Locations* list refreshes, no longer showing the newly moved locations. To view child locations associated with the specific parent, in the row containing the parent location, click ▸ on the right of the location name.
5. In the *Name* field, add or change the name as needed.

    TIP: Additional options are available for Device and License Asset Types. See About customizing the Device Asset Type and Customize the License Asset Type.
6. To export one or more locations to a file:
    a. Select the rows containing the locations that you want to export.
    b. Select **Choose Action** > **Export**, and then choose the appropriate option.

        For example, to export all locations to a CSV file, select them in the list, and then select Choose ActionExportExport All To CSV Format.

    You can import location information from a file using the *Import Assets* wizard. For more information, see Importing asset data using CSV files.

Add or edit locations

The *Location Detail* page shows the details of the selected location.

Location information is static and changes only when you import data or change it manually.

1. Go to the *Location Detail* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Asset Management**, then click **Locations**.

c. Display the *Location Detail* page by doing one of the following:

Click the name of a location.

Select **Choose Action** > **New**.

2. Provide the following information about the location: **Subtype**, **Name** (required), **Description**, **Web site**, **Address**, **Locale**, and **Phone Number**.
3. When you are editing an en existing location, to associate it with a device, in the *Assigned Devices* section, click +, select a device, and click **Add**.

   The selected device appears in the list below.
4. When you are editing an en existing location, to associate it with an asset, in the *Assigned Assets* section, click +, select an asset, and click **Add**.

   The selected asset appears in the list below.
5. Click **Save**.

Customize location fields

You can rename, create, and delete fields on the *Location Detail* page, as needed.

1. Go to the *Location Detail* page:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Asset Management**, then click **Locations**.
   c. Display the *Location Detail* page by doing one of the following:

   # Click the name of a location.

   # Select **Choose Action** > **New**.
2. Specify location subtypes, if needed.
   a. In the *Subtypes* section, click **Add Subtype**.

      The *Location Asset Subtype Detail* **page appears. The** *Inherited Fields* **section shows fields that are available to the Asset Subtype because they have been added to the Asset Type.**
   b. On the *Location Asset Subtype Detail* page that appears, review, and edit the following options, as needed:

Options	Description
Name	The name of the Location Subtype. This name appears in the list on the *Location Detail* page.
Default	Indicates whether to use the Location Subtype as the default for new locations. If you select this check box, new locations are automatically assigned to this Asset Subtype. You can change this setting any time.
Inherited Fields	This section displays the default location fields. You cannot make any changes to this section.
Subtype Fields	Add any fields that are specific to this Subtype, as needed. To add a field, click +, and specify the required information.

   c. Click **Save**.
3. If you want the locations to use barcodes, specify one or more tags in the *Barcode Tags* area.

Any locations that you create going forward will have the barcode tags available for configuration. For example, if you specify a Corporate Tag and a Dell Location Tag, barcodes identified with these two tags will be available for selection in on the *Location Detail* page, when you create or edit a location.

To add a barcode, click +, type the barcode name, and click Save.

4. Specify additional location fields, as needed.
    a. To add a field, in the *Asset Fields* area, click +.
    b. Provide the following information for each new field:

Option	Description
Name	The field name.
Available Values	The values that appear in fields that contain lists of values. This field is enabled when you select **Single Select** or **Multiple Select** from the *Type* drop-down list. If you select **Single Select** or **Multiple Select**, you must enter at least one value in this field. To use multiple values, separate each value with a comma.
Required	Indicates whether the field is mandatory or optional. If this check box is selected, users must enter a value in the field when creating assets of the selected type.
Type	The type of field. Field types include: • **Attachment**: Enables users to add attachments to the asset. • **Currency**: Used for monetary values. • **Software Catalog**: Enables users to associate the asset with an application in the Software Catalog. • **Publisher**: Enables user to associate the publisher info of an application to the asset. • **Date**: Used for calendar information. • **Label**: Enables users to associate a label with the asset. • **Locale** : Enables user to associate the locale with an asset. • **Link**: Used for Internet links. Links must be valid URLs, such as **http://quest.com**. • **Multiple Select**: Displays a list where multiple values can be selected. The maximum length for each value is 255 characters. • **Notes**: Used for additional information. • **Number**: Used for numerical values expressed as whole numbers. • **Parent**: Enables the asset to point to the same type of asset in a parent-child relationship. For example, you might allow Location types to have a Parent connection,

Option	Description
	allowing New York to point to a North America location. This can then be used in the reporting system to show all assets in North America. • **Publisher**: Allows you to select from the current list of publishers available in the Software Catalog. • **Single Select**: Displays a value list where only a single value can be selected. The maximum length for each value is 255 characters. • **Text**: Used for additional text. The maximum length is 255 characters. • **Timestamp**: Used to add a day and time to the record. • **User**: Used to associate user records with an asset. • **Assets Asset Type**: Used to specify relationships among Asset Types.

c. Click **Save**.

5. Click **Save**.

Managing contracts

A contract is a form of purchase agreement between the vendor and the end user, that describes the usage terms. Contracts can be associated with software and hardware items your business uses, and also for physical items such as office furniture or coffee machines.

You can add, edit, or delete contracts, as needed.

Manage contracts

Contracts represent purchase or service agreements for hardware and software items your business uses, and also for any physical products or services, such as office chairs or coffee suppliers.

You can add, edit, or delete contracts, or export contract details into a file, as needed.

1. Go to the *Contracts* list:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Asset Management**, then click **Contracts**.
2. To add a contract, select **Choose Action** > **New**.

   See Add or edit contracts for more information.
3. To delete a contract:
   a. Select the row containing the contract that you want to delete.
   b. Select **Choose Action** > **Delete**.
4. To export one or more contract entries to a file:
   a. Select the rows containing the contracts that you want to export.
   b. Select **Choose Action** > **Export**, and then choose the appropriate option.

      For example, to export all contracts to a CSV file, select them in the list, and then select Choose Action > Export > Export All To CSV Format.

   You can import contract information from a file using the *Import Assets* wizard. For more information, see Importing asset data using CSV files.

Add or edit contracts

The *Contract Detail* page shows the details of the selected contract.

Use this page to add or edit contracts, as needed.

1. Go to the *Contract Detail* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Asset Management**, then click **Contracts**.
    c. Display the *Contract Detail* page by doing one of the following:
    # Click the name of a contract.
    # Select **Choose Action** > **New** > **Contract-Hardware**.
    # Select **Choose Action** > **New** > **Contract-Software**.
    # Select **Choose Action** > **New** > **Contract-Other**.
2. Provide general information about the contract.

    Contracts are a form of asset types, and apart from the *Name* field which is always required, the collection of the fields available with each contract type can be changed to suit your needs. For more information about Asset Types, see About Asset Types

    The following fields typically appear on a contract record:

Option	Description
Subtype	The subtype assignment for this contract asset, if applicable. *None* indicates that the asset is not assigned to a subtype. You can specify the contract subtypes in the applicable contract Asset Subtype (**Contract-Software**, **Contract-Hardware**, or **Contract-Other**). For more information about asset subtypes, see About Asset Subtypes, custom fields, and device detail preferences.
Asset Status	The contract status, if applicable. You can select a default asset status, or a custom one (if they exist). A default installation of the appliance includes the following asset statuses: • **Active**: Any asset that is deployed, active, or in use. • **Disposed**: An asset that is no longer available for use. • **Expired**: A software license or contract asset that has expired. • **In Stock**: A recently received asset. • **Missing**: Any asset that cannot be located. • **Repair**: An asset that is being repaired. • **Reserved**: An asset that is set aside for a specific person or use. • **Retired**: Any asset that reached its end-of-life state, or is no longer in use. • **Stolen**: An asset that has been reported as stolen. For more information, see View and configure asset lifecycle settings.
Location	The location of this asset.

Option	Description
Name	The name of the contract.
Contract Number	The contract number.
Contract Description	Additional information about the contract.
Contract Start Date	The date when the contract is activated.
Contract End Date	The date when the contract ends.
Anniversary	**Software and hardware contracts only**. An indicator of when the contract is up for renewal.
Publisher	**Software and hardware contracts only**. The contract publisher.
Publisher Program	**Software contracts only**. The entries available for selection are populated from the Software Catalog, depending on what you set in the *Publisher* field. When you select a Publisher, the entries available for selection in this field are populated with the program entries associated with the selected Publisher, that exist in your Software Catalog.
Vendor	The name of the vendor associated with the contract. You can select from the available vendor entries.
Vendor Agreement Number	The number of the vendor agreement associated with the contract.
Manufacturer	**Hardware contracts only**. The manufacturer of the device associated with this contract.
Hardware Type	**Hardware contracts only**. The type of the hardware device associated with this contract, such as laptop or server.
Hardware Series	**Hardware contracts only**. The series of the hardware device associated with this contract.
Hardware Model	**Hardware contracts only**. The model number of the hardware device associated with this contract.
Purchase Order Number	The number of the purchase order associated with the contract.
Purchase Order Date	The date of the purchase order associated with the contract.
Linked Contract	Another contract that is associated with this contract entry.
Contact Name	The contact name associated with the contract.
Contact Email	The contact email address associated with the contract.
Contact Phone	The contact phone number associated with the contract.

Option	Description
Notes	Additional information about this contract.
Attachment 1, **Attachment 2**	Any file attachments associated with the contract.

3. **Optional**. Add one or more barcodes to the contract, as needed.
    a. Under *Barcodes*, click +, and provide the following information:

Option	Description
Barcode Data	The barcode number. Barcode numbers are always unique, they cannot be shared between multiple assets. However, it is possible for an active asset to share a barcode with an archived asset.
Barcode Name	The barcode tag associated with this asset type. There can be only one barcode of the same type per asset.
Barcode Format	The barcode format. For example, UPC-A, Code 11, or UPC-E.

4. Review the information in the *Service Desk* section. If you are editing an existing contract associated with one or more Service Desk tickets, they are listed in this section.
5. Review the information in the *Related Assets* section. If you are editing an existing contract associated with one or more licenses, they are listed in this section.
6. Click **Save**.

Managing licenses

A license agreement allows you to use a logical or physical asset, such as software or hardware.

You can add, edit, or delete licenses, as needed, and associate them with your physical or logical assets.

Manage licenses

Licenses allow you to use your logical or physical assets, such as software or hardware that your business uses.

You can add, edit, or delete licenses, or export license details into a file, as needed.

1. Go to the *Licenses* list:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Asset Management**, then click **Licenses**.
2. To add a license, select **Choose Action** > **New**.

    See Add or edit licenses for more information.
3. To delete a license:
    a. Select the row containing the license that you want to delete.
    b. Select **Choose Action** > **Delete**.
4. To export one or more license entries to a file:
    a. Select the rows containing the licenses that you want to export.
    b. Select **Choose Action** > **Export**, and then choose the appropriate option.

For example, to export all licenses to a CSV file, select them in the list, and then select Choose Action > Export > Export All To CSV Format.

You can import license information from a file using the *Import Assets* wizard. For more information, see Importing asset data using CSV files.

Add or edit licenses

The *License Detail* page shows the details of the selected license.

Use this page to add or edit licenses, as needed. Licenses are a form of asset types, and apart from the license name which is always required, the collection of the fields available with a license record can be changed to suit your needs. For more information about Asset Types, seeAbout Asset Types.

1. Go to the *License Detail* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Asset Management**, then click **Licenses**.
    c. Display the *License Detail* page by doing one of the following:
    # Click the name of a license.
    # Select **Choose Action** > **New**.
2. On the *License Detail* page, on the *General* tab, provide the following information:

Option	Description
Name	The name of the license, such as **Office Professional PO #1234**. This is the name that you use to find the asset. If you plan to have multiple licenses associated with an application, provide the purchase order number or purchase date in the fields below to differentiate the licenses.
License Subtype	The Asset Subtype to associate with the license. See About Asset Subtypes, custom fields, and device detail preferences.
Asset Status	The license status, if applicable. You can select a default asset status, or a custom one (if they exist). A default installation of the appliance includes the following asset statuses: • **Active**: Any asset that is deployed, active, or in use. • **Disposed**: An asset that is no longer available for use. • **Expired**: A software license or contract asset that has expired. • **In Stock**: A recently received asset. • **Missing**: Any asset that cannot be located. • **Repair**: An asset that is being repaired. • **Reserved**: An asset that is set aside for a specific person or use. • **Retired**: Any asset that reached its end-of-life state, or is no longer in use. • **Stolen**: An asset that has been reported as stolen. For more information, see View and configure asset lifecycle settings.
Location	The name of the location where the asset is located. See Managing locations.

Option	Description
License Count	The number of installations or seats the license allows. For example, 50.
Applies to Cataloged Software	Applications in the Software Catalog inventory to which the license applies. You can associate License assets with multiple applications in the Software Catalog if necessary. However, it is not necessary to associate a License asset with multiple versions of the same application because the appliance does this automatically to support upgrades and downgrades. You can simply associate the current version with the License asset when you add the license information. In addition, if you assign applications from different publishers, such as Microsoft Office and Adobe Acrobat, to the same License asset, the total number of seats specified in the License asset is assigned to each application. For example, if the License asset has 100 seats, both Microsoft Office and Adobe Acrobat are assigned 100 seats.
Applies to Software	Leave this field blank. A software license cannot be associated with applications from the *Software Catalog* inventory and the *Software* page inventory at the same time. For more information on how to create license assets for cataloged software, see Add License assets for Software page inventory.
License Mode	The mode of the License asset. For applications that require licenses, and to display license usage information on the *License Compliance* page, select either *Enterprise* or *Unit License*. **NOTE:** Most modes, including *Not Specified*, *Client License*, *Subscription*, *Shareware*, *Freeware*, *OpenSource*, *No Licensing*, and *Site License*, are not used for License Compliance. The license mode is used in these sections of the **Administrator Console**: • The *License Compliance* list. See View License Compliance information for Software Catalog applications. • The License Compliance chart that is displayed on the *Dashboard*. Values that are marked as ignored on the *Asset Detail* page are shown with a usage level of 100 percent. See About Dashboard widgets.

3. On the *License Detail* page, on the *Purchase* tab, provide the following information:

Option	Description
Contract	The contract asset associated with the license.
Product Key	The product key associated with the license. You can modify and edit the default information, which can be captured for a License Asset Type.
Unit Cost	The unit cost associated with the license. You can modify and edit the default information, which can be captured for a License Asset Type.
Vendor	The name of the Vendor asset you want to associate with the application. the *Vendor* drop-down list is empty unless you have added a Vendor asset. To search for a vendor, begin typing in the list. **NOTE:** Assigning multiple vendors to a single software License asset is not recommended because it can result in inaccurate License Compliance information.

Option	Description
Purchase Order Number	The purchase order number associated with the license.
Purchase Date	The date the purchase was made. Click in the field, then select a date on the calendar.
Purchase	Select one or more purchase records associated with this license. See Managing purchase records.

4. On the *License Detail* page, on the *Maintenance* tab, provide the following information:

Option	Description
Includes Upgrade Rights	Indicates if the license includes upgrade rights. Upgrade rights refer to the ability to upgrade to a newer version of the licensed software, when such versions become available. For more information, see About license upgrades. Select one of the following options: • **Yes**: Upgrade rights are calculated by comparing the number of existing licenses for the selected software with the counts of available licenses for newer versions of the same software. • **Yes - Select from list**: Choose one or more software versions for which you want to grant upgrade rights. Under *Upgrade Software list*, click **Select cataloged software to add**. The list that appears is populated with higher versions of the selected software to which the license can be upgraded. When you click an entry in the list, your selection appears in the *Upgrade Software list* box. You can add one or more versions, as needed. To delete an item from the list, select it in the *Upgrade Software list* box, and click **Remove**. • **No**: If you do not want to grant upgrade rights to the selected software, select this option.
Includes Maintenance	Whether the license entitles users to upgrade the installed version of the application. See About License Compliance for Software Catalog applications.
Expiration Date	If the license includes maintenance, the expiration date of the maintenance period. The appliance License Compliance feature leverages Software Catalog information, such as application release dates. If new application versions are released during the maintenance period, they are automatically covered by this License asset.
Includes Downgrade Rights	Indicates if the license includes downgrade rights. Downgrade rights refer to the ability to apply licenses for newer software versions to older versions of the same software. For more information, see About license downgrades. Select one of the following options: • **Yes**: Downgrade rights are calculated by comparing the number of existing licenses for the selected software with the counts of available licenses for older versions of the same software. • **Yes - Select from list**: Choose one or more software versions for which you want to grant downgrade rights. Under *Downgrade Software list*, click **Select cataloged software to add**. The list that appears is populated with lower versions of the selected software to which the license can be downgraded. When you click an entry in the list, your selection appears in the *Downgrade Software list* box. You can add one or

Option	Description
	more versions, as needed. To delete an item from the list, select it in the *Downgrade Software list* box, and click **Remove**. • **No**: If you do not want to grant downgrade rights to the selected software, select this option.

5. Click **Next**.
6. On the *License Detail* page, on the *Related* tab, provide the following information:

Option	Description
Department	The business group or department that owns the application.
Cost Center	The cost center associated with the department that owns the application.
Approved for Device	The devices that are approved to use the license. This information is used in License Compliance reporting. For example, if devices have the application installed, but are not on the list of approved devices, the devices are listed in the report titled, *Unapproved Software Installation*. However, the appliance does not enforce license compliance. For example, the appliance does not prevent applications from being installed on managed devices if a license is expired or otherwise out of compliance.
Barcodes	Add or edit barcodes associated with this license, as required. For more information, see Add barcodes to assets.

7. Click **Next**.
8. On the *License Detail* page, on the *Custom* tab, provide additional custom data. You can modify the License Asset Type to include as many additional fields as necessary to meet your business objectives. For more information, see Add or customize Asset Types.
9. Click **Next**.
10. On the *License Detail* page, on the *Notes* tab, provide the following information:

Option	Description
Notes	Any additional information you want to provide.
License Text	Any supplemental information about the license, such as a license number.

11. Click **Save**.

Managing purchase records

Purchase records document the acquisition of any physical and software products for your organization. Your administrators can keep track of individual purchase records and associate them with related license agreements. A license agreement for a specific asset can be associated with one or more purchase record. For example, your organization may have one license agreement for Adobe Acrobat, and multiple purchase record for that software license, one for each group in the organization.

You can add, edit, or delete purchase records, as needed, and associate them with applicable license agreements.

Manage purchase records

Your administrators can keep track of individual purchase records used to acquire physical and software products for your organization.

You can add, edit, or delete purchase records, or export purchase record details into a file, as needed.

1. Go to the *Purchases* list:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Asset Management**, then click **Purchases**.
2. To add a purchase record, select **Choose Action** > **New**.

    See Add or edit purchase records for more information.
3. To delete a purchase record:
    a. Select the row containing the purchase record that you want to delete.
    b. Select **Choose Action** > **Delete**.
4. To export one or more purchase records to a file:
    a. Select the rows containing the purchase records that you want to export.
    b. Select **Choose Action** > **Export**, and then choose the appropriate option.

        For example, to export all purchase record to a CSV file, select them in the list, and then select Choose Action > Export > Export All To CSV Format.

Add or edit purchase records

The *Purchase Detail* page shows the details of the selected purchase record.

Use this page to add or edit purchase records, as needed. Licenses are a form of asset types, and apart from the purchase record name and unit quantity which are always required, the collection of the fields available with a license record can be changed to suit your needs. For more information about Asset Types, seeAbout Asset Types.

1. Go to the *License Detail* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Asset Management**, then click **Purchases**.
    c. Display the *Purchase Detail* page by doing one of the following:

    # Click the name of a purchase record.

    # Select **Choose Action** > **New**.
2. On the *Purchase Detail* page, provide the following information:

Option	Description
Purchase Subtype	The Asset Subtype to associate with the purchase record. You can create purchase records for *Hardware* or *Software* items. See About Asset Subtypes, custom fields, and device detail preferences.

Option	Description
Asset Status	The purchase record status, if applicable. You can select a default asset status, or a custom one (if they exist). A default installation of the appliance includes the following asset statuses: • **Active**: Any asset that is deployed, active, or in use. • **Disposed**: An asset that is no longer available for use. • **Expired**: A software license or contract asset that has expired. • **In Stock**: A recently received asset. • **Missing**: Any asset that cannot be located. • **Repair**: An asset that is being repaired. • **Reserved**: An asset that is set aside for a specific person or use. • **Retired**: Any asset that reached its end-of-life state, or is no longer in use. • **Stolen**: An asset that has been reported as stolen. For more information, see View and configure asset lifecycle settings.
Location	The name of the location where the asset obtained with this purchase is located. See Managing locations.
Name	The name of the purchase record, such as **Office Professional PO #1234**. This is the name that you use to associate this purchase order with a license agreement, as applicable.
Description	The description of the purchase order.
Purchase Order Number	The number of the purchase order issued by your organization.
Purchase Order Date	The date on which your organization issued the purchase order.
Quantity	The number of units purchased.
Unit Cost	The cost of an individual unit purchased.
Vendor	The name of the vendor that the unit is purchased from.
Vendor Order Number	The number of the purchase order issued by the vendor.
Vendor Order Date	The date on which the vendor issued the purchase order.
Proof of Purchase	An image containing the photo of the purchase record.
Notes	Any additional information you want to provide.

Option	Description
Software Title	**Software only**. The name of the purchased software.
Publisher	**Software only**. The publisher of the purchased software.
Contract	**Software only**. The contract associated with the software purchase.
Product Key	**Software only**. The product key of the purchased software.
Maintenance Expiration Date	**Software only**. The date on which the maintenance for the purchased software ends.
Proof of Maintenance	**Software only**. An image containing the photo of the maintenance agreement.
Manufacturer	**Hardware only**. The manufacturer of the purchased hardware item.
Model	**Hardware only**. The model name of the purchased hardware item.
Specifications	**Hardware only**. Any specifications for the purchased hardware item, as applicable.
Serial Number	**Hardware only**. The serial number of the purchased hardware item.
Contract	**Hardware only**. The contract associated with the purchased hardware item.
Warranty Start Date	**Hardware only**. The date on which manufacturer's warranty for purchased hardware item starts.
Warranty End Date	**Hardware only**. The date on which manufacturer's warranty for purchased hardware item ends.
Support End Date	**Hardware only**. The date on which the support for the purchased hardware item ends.
Barcodes	Add or edit barcodes associated the items acquired with this purchase order, as required. For more information, see Add barcodes to assets.

Setting up License Compliance

To track License Compliance information for applications, you need to create License assets. License assets can be associated either with applications in the Software Catalog inventory or the *Software* page inventory. License assets cannot be associated with both inventory types at the same time.

The options for tracking licenses, and the requirements for setting up License Compliance, differ for Software Catalog inventory and for *Software* page inventory.

About License Compliance for Software Catalog applications

The appliance enables you to view License Compliance information for applications in the Software Catalog inventory. This information appears on the *License Compliance* page and in the License Compliance Dashboard widget.

After you configure License assets for applications in the Software Catalog inventory, you can view the number of seats installed on Agent-managed devices, the number of seats available, the type of licenses applied, and, if metering is enabled for the application, usage information. In addition, the appliance leverages information in the Software Catalog to automatically apply the correct licenses to application versions that are classified as upgraded or downgraded.

To set up License Compliance for applications in the Software Catalog inventory:

- (Optional) Customize the License Asset Type to meet your information management requirements. See Customize the License Asset Type.
- (Optional) Enable metering for Software Catalog applications. When metering is enabled, the License Compliance page shows whether applications have or have not been used in the past 30, 60, and 90 days. See About software metering.
- Create License assets and associate them with applications in the Software Catalog inventory. See Add License assets for Software Catalog inventory.
- (Optional) Set the threshold levels for License Compliance used on the Dashboard widget. The default *Warning Threshold* is 90. The default *Critical Threshold* is 100. See Customize license usage warning thresholds.

About license upgrades

Application maintenance plans often enable users to upgrade to newer versions of applications when those versions become available, and the *License Compliance* page shows the number of installations that are considered to be upgrades.

To track upgrades, the appliance uses the information in the Software Catalog and the license details to determine whether to associate new versions of applications with existing licenses. For example, if a License asset was created for the 1.0 version of an application, and the maintenance plan entitles users to upgrade, the 2.0 version of the application is automatically covered by the License asset when it is released. In this example, the License asset must be configured as follows:

- The *Includes Maintenance* field must be set to *Yes*.
- The *Maintenance Expiration Date* must be later than the version 2.0 GA (General Availability) date in the Software Catalog.
- The *License Mode* must be *Enterprise* or *Unit License*.
- The *Include Upgrade Rights* must be set to *Yes* or *Yes - Select from list*.

For more information about these settings, see Add License assets for Software Catalog inventory.

About license downgrades

Vendors often allow users to apply licenses for newer versions of applications to older versions, and these types of installations are referred to as downgrades. The *License Compliance* page shows the number of installations that are considered to be downgrades.

License seats are first allocated to installations of the latest version of the application. If additional seats are available, and if the vendor allows downgrades, the seats are automatically allocated to installations that are considered downgrades.

Licenses for upgrades are always allocated before licenses for downgrades.

Customize the License Asset Type

You can add, change, or delete the fields available to the License Asset Type as needed. The License Asset Type is the template that determines the fields available when you add License assets.

If the Organization component is enabled on your appliance, you customize the License Asset Type for each organization separately.

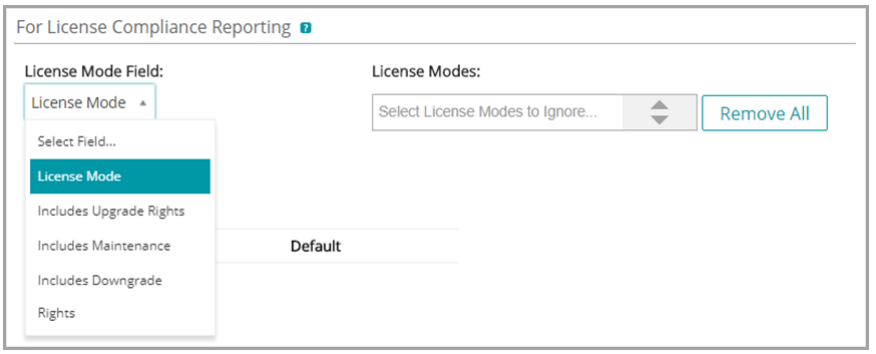
1. Go to the *Asset Types* list:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Asset Management**, then click **Asset Types**.
2. In the *Name* column, click **License** to display the *Asset Type Detail* page.
3. In the *Default Asset Status* field, enter a default asset status, or a custom one (if they exist).

    A default installation of the appliance includes the following asset statuses:

    # **Active**: Any asset that is deployed, active, or in use.
    # **Disposed**: An asset that is no longer available for use.
    # **Expired**: A software license or contract asset that has expired.
    # **In Stock**: A recently received asset.
    # **Missing**: Any asset that cannot be located.
    # **Repair**: An asset that is being repaired.
    # **Reserved**: An asset that is set aside for a specific person or use.
    # **Retired**: Any asset that reached its end-of-life state, or is no longer in use.
    # **Stolen**: An asset that has been reported as stolen.
4. In the *Name* field, type the name of the Asset Type.

    The default for this type of asset is *License*.
5. **Optional**: In the *For License Compliance Reporting* section, select the fields to use for License Compliance.

    Information from the selected *License Mode* field appears on the Dashboard *License Compliance* widget.
6. Do one of the following:
    - **In the *License Mode Field* drop-down list, keep the default as Select Field. This makes all of the values in the *License Mode Field* available for License Compliance. If you have more than one single-select or multiple-select field on the *Asset Fields* list, the first field that appears on the list, and all of its values, is used in the License Compliance widget.**
    - **In the *License Mode Field* drop-down list, select a field, such as License Mode, to be used for License Compliance. By default, this drop-down list contains a single field, but you can add fields as needed. If you select a field, such as License Mode as shown in the following illustration, only the selected field is used for License Compliance.**



In addition, when you select a field, you can choose the values, if any, you want to ignore in the License Compliance chart. Values that are ignored are listed at 100 percent usage and displayed in gray.
By default *License Mode* is the only single- or multiple-select field available, so it is the only field listed. If you add single- or multiple-select fields on the *Asset Fields* table, they appear in this list as well, and they appear on the *Asset Detail* page when you add a License asset. However, only the selected field, or the first field on the *Asset Fields* list, is used in the *License Compliance* widget.

7. **Optional**: Modify the *License Mode* field or values on the *Asset Fields* table.
   a. Click the **Edit** button at the end of a row: .
   b. Change the field information as needed, then click **Save** at the end of the row.
   c. To add a field, click the **Add** button in the table heading: +. Add field information, then click **Save** at the end of the row.
   d. To change the order of fields, drag the **Reorder** button: .
   e. To remove a field, click **Delete** button: .
8. Click **Save** at the bottom of the page.

Related topics

View License Compliance and Configuration information.

Add License assets for Software Catalog inventory

You can add License assets for applications in the Software Catalog inventory. Adding License assets enables you to view license compliance information on the *License Compliance* list and on the License Compliance *Dashboard* widget.

Software Catalog applications must be classified as *Discovered*, *Not Discovered*, or *Locally Cataloged*. You cannot add License assets for applications classified as *Uncataloged*.

When you associate License assets with applications, you can also view license information on the *Software Catalog Detail* page. If the Organization component is enabled on your appliance, you manage license information for each organization separately.

TIP: To add License assets for multiple applications at once, you can import the information from spreadsheets or CSV files. See Example: Import license data from prepared spreadsheets.

1. Go to the *Software Catalog* list:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.

b. On the left navigation bar, click **Inventory**, then click **Software Catalog**.

2. Click the name of an application to display the *Software Catalog Detail* page.
3. Near the bottom of the page, in the *License* section, click **Add New License** to display the *License Asset Detail* page.
4. On the *License Detail* page, on the *General* tab, provide the following information:

Option	Description
Name	The name of the license, such as **Office Professional PO #1234**. This is the name that you use to find the asset. If you plan to have multiple licenses associated with an application, provide the purchase order number or purchase date in the fields below to differentiate the licenses.
License Subtype	The Asset Subtype to associate with the license. See About Asset Subtypes, custom fields, and device detail preferences.
Asset Status	The license status, if applicable. You can select a default asset status, or a custom one (if they exist). A default installation of the appliance includes the following asset statuses: • **Active**: Any asset that is deployed, active, or in use. • **Disposed**: An asset that is no longer available for use. • **Expired**: A software license or contract asset that has expired. • **In Stock**: A recently received asset. • **Missing**: Any asset that cannot be located. • **Repair**: An asset that is being repaired. • **Reserved**: An asset that is set aside for a specific person or use. • **Retired**: Any asset that reached its end-of-life state, or is no longer in use. • **Stolen**: An asset that has been reported as stolen. For more information, see View and configure asset lifecycle settings.
Location	The name of the location where the asset is located. See Managing locations.
License Count	The number of installations or seats the license allows. For example, 50.
Applies to Cataloged Software	Applications in the Software Catalog inventory to which the license applies. You can associate License assets with multiple applications in the Software Catalog if necessary. However, it is not necessary to associate a License asset with multiple versions of the same application because the appliance does this automatically to support upgrades and downgrades. You can simply associate the current version with the License asset when you add the license information. In addition, if you assign applications from different publishers, such as Microsoft Office and Adobe Acrobat, to the same License asset, the total number of seats specified in the License asset is assigned to each application. For example, if the License asset has 100 seats, both Microsoft Office and Adobe Acrobat are assigned 100 seats.
Applies to Software	Leave this field blank. A software license cannot be associated with applications from the *Software Catalog* inventory and the *Software* page inventory at the same time. For more information on how to create license assets for cataloged software, see Add License assets for Software page inventory.

Option	Description
License Mode	The mode of the License asset. For applications that require licenses, and to display license usage information on the *License Compliance* page, select either *Enterprise* or *Unit License*. **NOTE:** Most modes, including *Not Specified*, *Client License*, *Subscription*, *Shareware*, *Freeware*, *OpenSource*, *No Licensing*, and *Site License*, are not used for License Compliance. The license mode is used in these sections of the **Administrator Console**: • The *License Compliance* list. See View License Compliance information for Software Catalog applications. • The License Compliance chart that is displayed on the *Dashboard*. Values that are marked as ignored on the *Asset Detail* page are shown with a usage level of 100 percent. See About Dashboard widgets.

5. On the *License Detail* page, on the *Purchase* tab, provide the following information:

Option	Description
Contract	The contract asset associated with the license.
Product Key	The product key associated with the license. You can modify and edit the default information, which can be captured for a License Asset Type.
Unit Cost	The unit cost associated with the license. You can modify and edit the default information, which can be captured for a License Asset Type.
Vendor	The name of the Vendor asset you want to associate with the application. the *Vendor* drop-down list is empty unless you have added a Vendor asset. To search for a vendor, begin typing in the list. **NOTE:** Assigning multiple vendors to a single software License asset is not recommended because it can result in inaccurate License Compliance information.
Purchase Order Number	The purchase order number associated with the license.
Purchase Date	The date the purchase was made. Click in the field, then select a date on the calendar.
Purchase	Select one or more purchase records associated with this license. See Managing purchase records.

6. On the *License Detail* page, on the *Maintenance* tab, provide the following information:

Option	Description
Includes Upgrade Rights	Indicates if the license includes upgrade rights. Upgrade rights refer to the ability to upgrade to a newer version of the licensed software, when such versions become

Option	Description
	available. For more information, see About license upgrades. Select one of the following options: • **Yes**: Upgrade rights are calculated by comparing the number of existing licenses for the selected software with the counts of available licenses for newer versions of the same software. • **Yes - Select from list**: Choose one or more software versions for which you want to grant upgrade rights. Under *Upgrade Software list*, click **Select cataloged software to add**. The list that appears is populated with higher versions of the selected software to which the license can be upgraded. When you click an entry in the list, your selection appears in the *Upgrade Software list* box. You can add one or more versions, as needed. To delete an item from the list, select it in the *Upgrade Software list* box, and click **Remove**. • **No**: If you do not want to grant upgrade rights to the selected software, select this option.
Includes Maintenance	Whether the license entitles users to upgrade the installed version of the application. See About License Compliance for Software Catalog applications.
Expiration Date	If the license includes maintenance, the expiration date of the maintenance period. The appliance License Compliance feature leverages Software Catalog information, such as application release dates. If new application versions are released during the maintenance period, they are automatically covered by this License asset.
Includes Downgrade Rights	Indicates if the license includes downgrade rights. Downgrade rights refer to the ability to apply licenses for newer software versions to older versions of the same software. For more information, see About license downgrades. Select one of the following options: • **Yes**: Downgrade rights are calculated by comparing the number of existing licenses for the selected software with the counts of available licenses for older versions of the same software. • **Yes - Select from list**: Choose one or more software versions for which you want to grant downgrade rights. Under *Downgrade Software list*, click **Select cataloged software to add**. The list that appears is populated with lower versions of the selected software to which the license can be downgraded. When you click an entry in the list, your selection appears in the *Downgrade Software list* box. You can add one or more versions, as needed. To delete an item from the list, select it in the *Downgrade Software list* box, and click **Remove**. • **No**: If you do not want to grant downgrade rights to the selected software, select this option.

7. Click **Next**.
8. On the *License Detail* page, on the *Related* tab, provide the following information:

Option	Description
Department	The business group or department that owns the application.
Cost Center	The cost center associated with the department that owns the application.
Approved for Device	The devices that are approved to use the license. This information is used in License Compliance reporting. For example, if devices have the application installed, but are not on the list of approved devices, the devices are listed in the report titled, *Unapproved Software Installation*. However, the appliance does not enforce license

Option	Description
	compliance. For example, the appliance does not prevent applications from being installed on managed devices if a license is expired or otherwise out of compliance.
Barcodes	Add or edit barcodes associated with this license, as required. For more information, see Add barcodes to assets.

9. Click **Next**.
10. On the *License Detail* page, on the *Custom* tab, provide additional custom data. You can modify the License Asset Type to include as many additional fields as necessary to meet your business objectives. For more information, see Add or customize Asset Types.
11. Click **Next**.
12. On the *License Detail* page, on the *Notes* tab, provide the following information:

Option	Description
Notes	Any additional information you want to provide.
License Text	Any supplemental information about the license, such as a license number.

13. Click **Save**.

    The new License asset appears on the *Licenses* page. The *License Count* number does not change until you update the asset. However, the number in the *Installed* column changes when managed devices that have the software installed check in to the appliance. This enables you to track the number of licenses that have been purchased and installed.

Perform the following optional tasks:

- Enable metering for Software Catalog inventory. When metering is enabled, the *License Compliance* page shows whether applications have or have not been used in the past 90 days. See About software metering.
- Set license usage warning thresholds. These thresholds are used by the License Compliance Dashboard widget to identify license compliance issues.

Add License assets for Software page inventory

You can create License assets to track information for applications that require licenses.

Before you create License assets, you should have information such as the number of installations, or seats, allowed by the license, the product key, the purchase order number, and any other information you want to manage in the License asset.

NOTE: To create License assets for applications in the *Software* page inventory, you first must create Software assets for those applications. You do not need to create Software assets for applications in the *Software Catalog* page inventory.

If the Organization component is enabled on your appliance, you can create License assets for each organization separately.

TIP: You can customize License Asset Types to meet your needs. See Customize the License Asset Type.

1. Go to the *License Asset Detail* page:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.

b. Do one of the following:

On the left navigation bar, click **Licenses**. Select **Choose Action** > **New**.

On the left navigation bar, click **Inventory**, then click **Software Catalog**. Click the name of an application. On the *Software Catalog Detail* page, click **Add New License**.

2. On the *License Detail* page, on the *General* tab, provide the following information:

Option	Description
Name	The name of the license, such as **Office Professional PO #1234**. This is the name that you use to find the asset. If you plan to have multiple licenses associated with an application, provide the purchase order number or purchase date in the fields below to differentiate the licenses.
License Subtype	The Asset Subtype to associate with the license. See About Asset Subtypes, custom fields, and device detail preferences.
Asset Status	The license status, if applicable. You can select a default asset status, or a custom one (if they exist). A default installation of the appliance includes the following asset statuses: • **Active**: Any asset that is deployed, active, or in use. • **Disposed**: An asset that is no longer available for use. • **Expired**: A software license or contract asset that has expired. • **In Stock**: A recently received asset. • **Missing**: Any asset that cannot be located. • **Repair**: An asset that is being repaired. • **Reserved**: An asset that is set aside for a specific person or use. • **Retired**: Any asset that reached its end-of-life state, or is no longer in use. • **Stolen**: An asset that has been reported as stolen. For more information, see View and configure asset lifecycle settings.
Location	The name of the location where the asset is located. See Managing locations.
License Count	The number of installations or seats the license allows. For example, 50.
Applies to Cataloged Software	Applications in the Software Catalog inventory to which the license applies. You can associate License assets with multiple applications in the Software Catalog if necessary. However, it is not necessary to associate a License asset with multiple versions of the same application because the appliance does this automatically to support upgrades and downgrades. You can simply associate the current version with the License asset when you add the license information. In addition, if you assign applications from different publishers, such as Microsoft Office and Adobe Acrobat, to the same License asset, the total number of seats specified in the License asset is assigned to each application. For example, if the License asset has 100 seats, both Microsoft Office and Adobe Acrobat are assigned 100 seats.
Applies to Software	Leave this field blank. A software license cannot be associated with applications from the *Software Catalog* inventory and the *Software* page inventory at the same time. For more information on how to create license assets for cataloged software, see Add License assets for Software page inventory.

Option	Description
License Mode	The mode of the License asset. For applications that require licenses, and to display license usage information on the *License Compliance* page, select either *Enterprise* or *Unit License*. **NOTE:** Most modes, including *Not Specified*, *Client License*, *Subscription*, *Shareware*, *Freeware*, *OpenSource*, *No Licensing*, and *Site License*, are not used for License Compliance. The license mode is used in these sections of the **Administrator Console**: • The *License Compliance* list. See View License Compliance information for Software Catalog applications. • The License Compliance chart that is displayed on the *Dashboard*. Values that are marked as ignored on the *Asset Detail* page are shown with a usage level of 100 percent. See About Dashboard widgets.

3. On the *License Detail* page, on the *Purchase* tab, provide the following information:

Option	Description
Contract	The contract asset associated with the license.
Product Key	The product key associated with the license. You can modify and edit the default information, which can be captured for a License Asset Type.
Unit Cost	The unit cost associated with the license. You can modify and edit the default information, which can be captured for a License Asset Type.
Vendor	The name of the Vendor asset you want to associate with the application. the *Vendor* drop-down list is empty unless you have added a Vendor asset. To search for a vendor, begin typing in the list. **NOTE:** Assigning multiple vendors to a single software License asset is not recommended because it can result in inaccurate License Compliance information.
Purchase Order Number	The purchase order number associated with the license.
Purchase Date	The date the purchase was made. Click in the field, then select a date on the calendar.
Purchase	Select one or more purchase records associated with this license. See Managing purchase records.

4. On the *License Detail* page, on the *Maintenance* tab, provide the following information:

Option	Description
Includes Upgrade Rights	Indicates if the license includes upgrade rights. Upgrade rights refer to the ability to upgrade to a newer version of the licensed software, when such versions become

Option	Description
	available. For more information, see About license upgrades. Select one of the following options: • **Yes**: Upgrade rights are calculated by comparing the number of existing licenses for the selected software with the counts of available licenses for newer versions of the same software. • **Yes - Select from list**: Choose one or more software versions for which you want to grant upgrade rights. Under *Upgrade Software list*, click **Select cataloged software to add**. The list that appears is populated with higher versions of the selected software to which the license can be upgraded. When you click an entry in the list, your selection appears in the *Upgrade Software list* box. You can add one or more versions, as needed. To delete an item from the list, select it in the *Upgrade Software list* box, and click **Remove**. • **No**: If you do not want to grant upgrade rights to the selected software, select this option.
Includes Maintenance	Whether the license entitles users to upgrade the installed version of the application. See About License Compliance for Software Catalog applications.
Expiration Date	If the license includes maintenance, the expiration date of the maintenance period. The appliance License Compliance feature leverages Software Catalog information, such as application release dates. If new application versions are released during the maintenance period, they are automatically covered by this License asset.
Includes Downgrade Rights	Indicates if the license includes downgrade rights. Downgrade rights refer to the ability to apply licenses for newer software versions to older versions of the same software. For more information, see About license downgrades. Select one of the following options: • **Yes**: Downgrade rights are calculated by comparing the number of existing licenses for the selected software with the counts of available licenses for older versions of the same software. • **Yes - Select from list**: Choose one or more software versions for which you want to grant downgrade rights. Under *Downgrade Software list*, click **Select cataloged software to add**. The list that appears is populated with lower versions of the selected software to which the license can be downgraded. When you click an entry in the list, your selection appears in the *Downgrade Software list* box. You can add one or more versions, as needed. To delete an item from the list, select it in the *Downgrade Software list* box, and click **Remove**. • **No**: If you do not want to grant downgrade rights to the selected software, select this option.

5. Click **Next**.
6. On the *License Detail* page, on the *Related* tab, provide the following information:

Option	Description
Department	The business group or department that owns the application.
Cost Center	The cost center associated with the department that owns the application.
Approved for Device	The devices that are approved to use the license. This information is used in License Compliance reporting. For example, if devices have the application installed, but are not on the list of approved devices, the devices are listed in the report titled, *Unapproved Software Installation*. However, the appliance does not enforce license

Option	Description
	compliance. For example, the appliance does not prevent applications from being installed on managed devices if a license is expired or otherwise out of compliance.
Barcodes	Add or edit barcodes associated with this license, as required. For more information, see Add barcodes to assets.

7. Click **Next**.
8. On the *License Detail* page, on the *Custom* tab, provide additional custom data. You can modify the License Asset Type to include as many additional fields as necessary to meet your business objectives. For more information, see Add or customize Asset Types.
9. Click **Next**.
10. On the *License Detail* page, on the *Notes* tab, provide the following information:

Option	Description
Notes	Any additional information you want to provide.
License Text	Any supplemental information about the license, such as a license number.

11. Click **Save**.

The new license asset appears on the *Licenses* page. The *License Count* number does not change until you update the asset. However, the number in the *Installed* column changes when managed devices that have the software installed check in to the appliance. This enables you to track the number of licenses that have been purchased and installed.

Related topics

Customize the License Asset Type

View License Compliance and Configuration information

About reports

Importing license data in CSV files

If your license data is in a spreadsheet, you can export it to CSV (comma-separated value) format, then import it into the appliance. Or, you can use a text editor to create a CSV file that contains the data, then import that file.

If the CSV file contains new assets for Asset Types that you have defined, the new assets are added.

How asset information is handled during import

When asset information is imported, the appliance compares the new information to existing information to determine how the new information should be handled.

Depending on whether the information is new, existing, or duplicated, the appliance performs the following actions:

- **Creates the asset**: If the Primary Key value does not match an existing value, the asset is created.
- **Updates the asset**: If the Primary Key value matches an existing value, the asset information is updated.
- **Flags the asset as a duplicate**: If multiple records for the Asset Type match the value of the CSV field chosen as the Primary Key, OR if multiple records match the associated asset, the asset is flagged as a duplicate. Duplicate records are not imported.

Importing asset data using CSV files

You can import asset data, such as software license data, using CSV (comma separated value) files.

Prepare asset data before importing

Verify that asset data is appropriate and formatted properly before importing it.

1. Define the basic fields for your assets. If you use product names, make sure they are useful and help to identify the asset. See Adding Software assets.
2. Add header rows to your data. In the Asset Management component, columns without headers are referred to by their column number, so using column header rows can make it easier to identify data.
3. Verify that all columns map to equivalent *Asset Fields* in the Asset Type.

   Asset Types include default fields, such as *Asset Name*, *Purchase Order Number*, and *Vendor*, but you can add custom asset fields if necessary. See About adding and deleting asset fields.

   TIP: To view default fields go to the *Asset Detail* page. See Customizing Asset Types.

4. Decide what field or fields to use for the primary key (PK) for the imported assets.

   Primary Keys are the fields, or combinations of fields, used as unique identifiers for assets being imported. When assets are imported, the appliance uses Primary Keys to determine whether to update an existing record or create a record. You can select one field, or a combination of fields, as the PK.

5. Save the spreadsheet as a CSV file, in a location you can access from the Administrator Console.

Example: Import license data from prepared spreadsheets

You can import license data from prepared CSV files.

This example describes how to import License assets for Software Catalog inventory, either as a one-time import, or a scheduled import using a file from a network share. The example shows only the fields that are required for License asset import. You can add additional files, such as unit cost, publisher, product keys, and so on to meet your information management needs.

If you want to assign the imported assets to an Asset Subtype, add the subtype before you import the assets. See Add Asset Subtypes and select Device Detail page preferences.

1. Create a file in a spreadsheet program such as Excel.
2. Add the following columns and rows. The first row is a header column:

Asset Name	License Count	License Mode	Includes Maintenance	Applies to Software Catalog
Software Title 1	100	Enterprise	Yes	Software Title 1
Software Title 2	150	Enterprise	Yes	Software Title 2
Software Title 3	200	Enterprise	Yes	Software Title 3
Software Title 4	500	Enterprise	Yes	Software Title 4

3. Save the file in CSV format.

The values in each column are separated by commas. For example: `Software Title 1,100,Enterprise,Yes,Software Title 1`

4. Go to the *Upload File* page in the *Import Assets* section:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Asset Management**, then click **Import Assets**.

    # If one or more asset import operations are scheduled, the Import Assets list page appears, listing the import operations. To import assets from an CSV file, click **Choose Action** > **New** to start the *Import Assets* wizard.

    # If there are no scheduled asset imports on the appliance, the *Import Assets* wizard appears.

5. In the *Import Assets* wizard, select one of the following options:

Option	Description
Upload an Asset Import CSV file	Select this option to complete a one-time asset import from a CSV file. Then, click **Browse** or **Choose File**, then select the CSV file.
Schedule an Asset Import	Select this option to perform multiple asset import from a CSV file located on a network drive, at selected time intervals. Then, provide the following information: • **Select Asset Import File Transfer Protocol**: # **Samba**: Select this option to access the file using the Samba protocol, and provide the following information: # **Enter the UNC path to the Samba share**: Type the directory path to the CSV file. # **FTP**: Select this option to access the file on an FTP server, and provide the following information: # **Enter the FTP Server hostname or IP address**: Type the host name or IP address of the FTP server. # **Enter the FTP sub-directory if one exists**: Type the directory path to the CSV file on the FTP server. # **Secure FTP**: Select this option to access the file on a secure FTP server, and provide the following information: # **Enter the Secure FTP Server hostname or IP address**: Type the host name or IP address of the secure FTP server. # **Enter the SFTP full path**: Type the directory path to the CSV file on the secure FTP server. • **Asset Import CSV file name**: Type the name of the CSV file that you want to import. • **Credentials**: Select the credential that you want to use to access the specified network resource. Any credentials

Option	Description
	that are defined in the appliance appear in the list. For more information, see Managing credentials.

6. If the CSV file contains a header row, as it does in this example, select the *File Header Row* check box, then click **Next**.
7. **Scheduled asset imports only**. On the *Asset Import Selection Schedule* page that appears, create a schedule for importing the CSV file.
    a. In the *Asset Import Schedule Name* field, type the name that you want to assign to this schedule.
    b. Select **Enable Asset Schedule**.
    c. In the *Schedule* section, specify the import schedule, as required.

Option	Description
None	Run in combination with an event rather than on a specific date or at a specific time.
Every n hours	Run at a specified interval.
Every day/specific day at HH:MM	Run daily at a specified time, or run on a designated day of the week at a specified time.
Run on the nth of every month/ specific month at HH:MM	Run on the same day every month, or a specific month, at the specified time.
Run on the nth weekday of every month/specific month at HH:MM	Run on the specific weekday of every month, or a specific month, at the specified time.

Custom	Run according to a custom schedule.
	Use standard 5-field cron format (extended cron format is not supported):
	`* * * * *`
	`| | | | +————————day of week (0-6)(Sun=0)`
	`| | | +————————month (1-12)`
	`| | +————————day of month (1-31)`
	`| +————————hour (0-23)`
	`+————————minute (0-59)`
	Use the following when specifying values:
	• **Spaces ( )**: Separate each field with a space.
	• **Asterisks (*)**: Include the entire range of values in a field with an asterisk. For example, an asterisk in the hour field indicates every hour.
	• **Commas (,)**: Separate multiple values in a field with a comma. For example, `0,6` in the day of the week field indicates Sunday and Saturday.
	• **Hyphens (-)**: Indicate a range of values in a field with a hyphen. For example, `1-5` in the day of the week field is equivalent to `1,2,3,4,5`, which indicates Monday through Friday.
	• **Slashes (/)**: Specify the intervals at which to repeat an action with a slash. For example, `*/3` in the hour field is equivalent to `0,3,6,9,12,15,18,21`. The asterisk (`*`) specifies every hour, but `/3` restricts this to hours divisible by 3.

Option	Description
	Examples: • `15 * * * * Run 15 minutes after every hour every day` • `0 22 * * * Run at 22:00 every day` • `0 0 1 1,6 * Run at 00:00 on January 1 and June 1` • `30 8,12 * * 1-5 Run weekdays at 08:30 and 12:30` • `0 2 */2 * * Run every other day at 02:00`

8. On the*Asset Type Selection* page that appears, complete the following steps:
   a. In the *Asset Type* drop-down list, select **License**.
   b. In the *Asset Subtype* drop-down list, select **Productivity**.

   NOTE: In this example, the Asset Subtype, *Productivity*, has been added to the License Asset Type. The *Subtype* drop-down list is empty if you have not added subtypes for the License Asset Type. During import, all assets are assigned to the selected subtype.

   c. Click **Next**.

   The *Mapping* page appears.
9. In the *CSV Fields* drop-down list, select the fields that correspond to the appliance *Required Standard Fields* and *Required Asset Fields*. The mapping of these fields depends on the contents of your CSV file and the Asset Type. For the example in this section, use the following values:

   # *Asset Name*=**Name**
   # *Location*=**Location**
   # *Asset Status*=**Asset Status**

   NOTE: If you do not specify this mapping, the default status that is associated with the selected Asset Type is assigned to each imported asset entry.

   # *License Count*=**License Count**
   # *Applies to Cataloged Software*=**Software Catalog**
   # *License Mode*=**Mode**

   NOTE: You cannot import Asset Assignee values unless the imported Asset is a Device.
10. Select the **PK** check box next to the *Asset Name* field.

    NOTE: Primary Keys are the fields, or combinations of fields, used as unique identifiers for assets being imported. When assets are imported, the appliance uses Primary Keys to determine whether to update an existing record or create a record. You can select one field, or a combination of fields, as the PK.
11. If the assets you are importing use barcodes, in the *Barcode Fields* area, indicate how you want to import the barcodes.

Option	Description
Update asset barcodes with selected	Check if the barcodes supplied in this area already exist, and if they do, update them. If they do not exist, they are created for the specified assets.
Replace all asset barcodes with selected	Replace the existing barcodes with the specified barcodes.

Option	Description
Barcode Data	The field in the CSV file that contains the barcode. There can be only one barcode of the same type per asset.
Barcode Name	The field in the CSV file that contains the barcode tag. Barcode numbers are always unique, they cannot be shared between multiple assets. However, it is possible for an active asset to share a barcode with an archived asset.
Barcode Format	The field in the CSV file that contains the barcode format. For example, UPC-A, Code 11, or UPC-E.

12. Click **Preview** to verify the data on the *Confirmation* page.
13. **One-time imports only**. Complete the following steps.
    a. Click **Import** to complete the import process.

       The *Result for Asset Import* **page appears.**

    b. Click **Done** to return to the *Assets* page.
14. **Scheduled imports only**. Complete one of the following steps:

    # Click **Save** to save your newly created scheduled import. The *Import Assets* list page appears, showing the scheduled import entry in the list.

    # Click **Run Now** to import assets from the CSV file, and to save your scheduled import settings.

    The *Import Assets* **list page appears.**

When the import is complete, the assets appear in the *Assets* list. If the titles of the software matched titles in the Software Catalog inventory, the assets are associated with the inventory items and you can view them on the *Software Catalog Detail* page for the items. The progress bar on the top of the page shows the completion of the task.

Managing License Compliance

You can track the number of software licenses that have been purchased, the number in use on managed devices, and the number that are available. This type of tracking helps you to ensure that your company complies with software license requirements.

For example, if you have 100 licenses for the Adobe® Creative Suite, you might want to know how many of those licenses are actually being used on managed devices. In addition, you might want to know when 80 or 90 percent of those licenses are in use so that you can increase license capacity if necessary. You can customize license usage warning thresholds to track license compliance.

View License Compliance information for Software Catalog applications

To ensure that your organization has the correct licenses for installed software, you can view License Compliance information on the *License Compliance* list and on the License Compliance Dashboard widget. The *License Compliance*

list shows all the software license information you have added through License assets, as well as information from the Software Catalog about applications that require licenses.

- The Agent-managed devices in your inventory have software applications that are available in the Software Catalog.
- You have specified the number of seats available to installed Software Catalog applications as License assets, and you have specified the license mode. See Add License assets for Software page inventory.
- You have established warning thresholds for license usage in the appliance or organization general settings. See Configure Admin-level or organization-specific General Settings.

1. To view complete license compliance information, go to the *License Compliance* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Asset Management**, then click **License Compliance**.

NOTE: Information on the *License Compliance* list is updated every day after the appliance daily backup is complete. If the list is empty, either there are no applications in the Software Catalog inventory, or the information on the page has not been updated. In addition, if all the variances show negative numbers, which indicates that there are more installations than license seats, verify that you have added License assets for the applications. See Add License assets for Software Catalog inventory.

2. To force the appliance to update License Compliance information, click *Update Now* above the list on the left. Depending on the number of applications in inventory, this process might take a few minutes.

TIP: When you click **Update Now**, the appliance updates the data for each of the items on the list. However, when you click the **Refresh** button above the list on the right, the appliance simply redisplays the information already collected. It does not obtain new license usage information.

Information on the *License Compliance* page includes:

Column name	Description
Name	The name of the application.
Publisher	The name of the application publisher.
Installed	The number of application installations on Agent-managed devices.
Licensed	The number of seats remaining under the license.
Variance	The difference, if any, between the number of license seats available and the number of application installations. A negative number indicates that the application has been installed on more devices than the license allows, and therefore it is out of compliance.
Used Last 90 Days **Used Last 60 Days** **Used Last 30 Days**	The number of application installations that have been launched in the previous 90, 60, or 30 days. A dash in this column indicates that metering is not enabled for the application. **NOTE:** To obtain accurate usage information, metering must be enabled for the application and for the devices on which the application is installed. See Enabling and configuring metering for devices and applications.
Not Used Last 90 Days **Not Used Last 60 Days**	The number of application installations that have not been launched in the previous 90, 60, or 30 days. A dash in this column indicates that metering is not enabled for the application.

Column name	Description
Not Used Last 30 Days	**NOTE:** To obtain accurate usage information, metering must be enabled for the application and for the devices on which the application is installed. See Enabling and configuring metering for devices and applications.
Coverage	The license type. License types include: • **Upgrade**: The installed application has been upgraded from an earlier version (requires a maintenance agreement). • **Downgrade**: The installed application is using a license for a later version (requires downgrade rights). • **Original**: The installed application is using a license that matches its version number. • **None**: The application is installed without a license.
Platform	The operating system on which the application runs.
Edition	The name of the edition related to the application, such as Professional Edition or Standard Edition.

3. To sort the list, click **View By**, then select a view.

   You can view applications by Product, such as Microsoft Office, or by Product and Edition, such as Microsoft Office Professional and Office Standard. For example, if you wanted to see all editions of Microsoft Office applications under one heading, you could select Product in the *View By* drop-down list. The *Licensed* column shows the number of seats available to all applications in the Microsoft Office group. To show Microsoft Office applications by edition, select Product and Edition in the *View By* drop-down list. The *Licensed* column shows the number of seats available to each edition of Microsoft Office.

   TIP: When a group, such as Office, is collapsed to show only the top-level item, a warning icon is displayed to the left of the *Name* column if any item in the group has a negative variance or is using more seats than the license allows: ⚠.

4. To view the License Compliance widget, click **Home** on the left navigation bar to go to the Admin-level *Dashboard* page.

   TIP: If the License Compliance widget is not visible, click **Customize** in the upper right to install it. See Customize Dashboard pages.

5. To view or change information about the number of seats available under a license, go to the detail page for the *License* asset. See View assets and search for asset information.

Reclaim unused software licenses

Appliance administrators can set a policy that allows cataloged software to be uninstalled based on how frequently specific software applications are used on user devices in order to acquire underutilized software and re-use it where needed.

You have an option to reclaim licenses for a specific software application that is not used in the last 30, 60, or 90 days, or all associated licenses.

1. Navigate to the *License Compliance* page:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.

b. On the left navigation bar, click **Asset Management**, then click **License Compliance**.

2. In the **Name** column, expand the name of the application, and select a version of the software license that you want to reclaim, as required.

   NOTE: You can only reclaim licenses for a single software version at a time. Selecting multiple versions results in an error.

3. To reclaim licenses for the software version, choose **Choose Action** > **Reclaim Sofware**, and select one of the following options, as required:

   - **Not Used Last 30 Days**
   - **Not Used Last 60 Days**
   - **Not Used Last 90 Days**
   - **All**

   The *Managed Installation Detail* page appears, allowing you to create a process that removes the installation of the selected software item from the associated end user devices .

4. Create a new Managed Installation, as required. For more information, see the following sections, as applicable:

   # Create Managed Installations for Windows devices
   # Create Managed Installations for macOS X devices
   # Create Managed Installations for RPM files

Update software License Compliance information manually

You can manually update software License Compliance information any time. If you have a large number of applications, however, the process of updating the information might take several minutes.

The Agent-managed devices in your inventory have software applications that are available in the Software Catalog.

Software License Compliance information is updated automatically every day after the appliance daily backup process runs. Manually updating License Compliance information enables you to get the latest information available.

NOTE: If you have not added License assets for applications in inventory, the *License Compliance* page shows the number of seats available to applications as 0, and the variance is the number of software installations.

1. Go to the *License Compliance* page:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Asset Management**, then click **License Compliance**.
2. Click **Update Now** above the list.

   The appliance checks for the latest license usage information and the list is updated.

   TIP: Clicking the **Refresh** button above the list on the right simply redisplays the information already collected. It does not obtain new license usage information.

Customize license usage warning thresholds

You can customize license usage warning thresholds to specify the license usage percentage that is considered to be at warning or critical levels.

License compliance information appears on the appliance Dashboard. If the Organization component is enabled on your appliance, you customize license usage warning thresholds for each organization separately.

1. Go to Admin-level *General Settings* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Settings**, then click **Control Panel**.
    c. On the *Control Panel*, click **General Settings**.
2. In the *General Options* tab, scroll down to the *Asset License Usage Threshold* section.
3. In the *Warning Threshold* and *Critical Threshold* fields, enter new values.

    The default *Warning Threshold* is 90. The default *Critical Threshold* is 100.
4. To save, click **Save and Restart Services**.

    Threshold limits are set. If you have created License assets, License Compliance information appears on the *Dashboard* page of the Administrator Console.

Related topics

Add License assets for Software page inventory

View License Compliance and Configuration information

View License Compliance and Configuration information

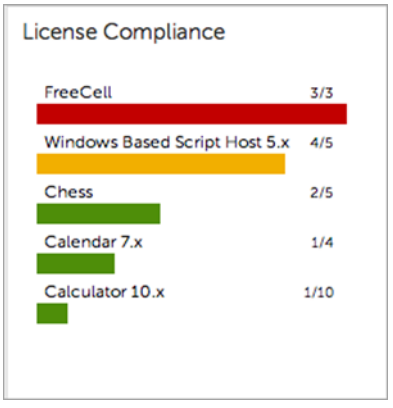
If you have set up License assets for applications, you can view License Compliance and Configuration information for those applications.

Information is available for License assets associated with applications listed under the *Software* tab and applications listed under the *Software Catalog* tab. See Setting up License Compliance.

If you have multiple organizations, you view license information for each organization separately.

1. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
2. Click **Home**.

    Software compliance information appears in the *License Compliance* widget.

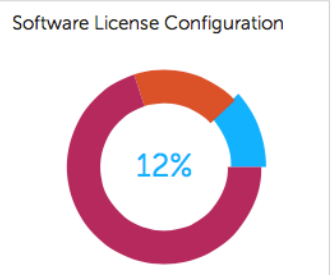


NOTE: The appliance updates the data in the *License Compliance* widget every eight hours. Clicking the **Refresh** button, however, does not update the data; it simply redisplays the data that has already been collected.

The following colors indicate the usage level:

Color	Description
Red	Usage is at or above the critical threshold setting.
Orange	Usage is at or above the warning threshold setting but below the critical threshold setting.
Green	Usage is below the warning threshold setting.

The *Software License Configuration* widget displays the percentage of software licenses that are categorized as unit licenses, site licenses, and other license modes.



Optional: View additional information on the *License Compliance* page. See View License Compliance information for Software Catalog applications.

Setting up Service Desk

Setting up Service Desk entails setting up roles for Service Desk staff, and configuring ticket and email settings.

Setting up roles for user accounts

Service Desk uses permission-based roles to control access to Service Desk features and information. These roles can be assigned to users automatically when they log in. You can use the default roles, or create roles as needed.

About default roles

Default roles are available for standard user account types such as administrator, end-user, and limited-access.

The following roles are available by default. For more information about managing Organizational roles, see Managing Organization Roles and User Roles.

Role	Description
Organization Roles	Organization Roles are supersets of permissions that are assigned to organizations, and they define the permissions that are available to organization users. For example, if an organization is assigned an Organization Role that has the *Distribution* tab hidden, users in that organization, including the Admin user, cannot access the *Distribution* tab. **NOTE:** Organization Roles are available only on appliances with the Organization component enabled.

Role	Description
Default Role	The Default Role in the Organization Roles section has Write and Read permission for all tabs. You can create additional Organization Roles, but you cannot edit or delete the Default Role.
User Roles	Roles assigned to users to control their access to the **Administrator Console** and **User Console**. If the Organization component is enabled on your appliance, the permissions available to these roles depends on the Organization Role assigned to the organization.
Administrator	The most powerful user role on the appliance. By default, users with the **Administrator** role have permission to see or change information and settings. This includes promoting or demoting other users by changing their roles. The **Administrator** role cannot be altered or deleted. Assign this role only to trusted administrators. Staff members assigned the **Administrator** role have permission to manage and modify Service Desk tickets from the *Tickets* tab in the **Administrator Console**, though they might not be able to own tickets themselves. Users with the **Administrator** role can also use the security, scripting, and distribution features to resolve Service Desk tickets, then document the issues in the Knowledge Base. The **Administrator** role primarily interacts with the appliance through the **Administrator Console**.
No Access	Users with this role cannot log on to the **Administrator Console** or **User Console**.
Read Only Administrator	This role has the ability to view but not change any information or settings in the appliance. This role is useful for oversight personnel, such as supervisors. This role primarily interacts with the appliance through the **Administrator Console**.
User Console Only	This role is for appliance users. By default, this role has permission to create, view, and modify Service Desk tickets. This role interacts with the appliance exclusively through the **User Console**.

Create a Service Desk staff role

You can create a Service Desk staff role to establish permissions for users who work on Service Desk settings and components.

By default, users with the **Administrator** role have permission to change all Service Desk components, including creating and removing users. In addition, you can create a more limited Service Desk role for your organization. Users with this role have permission to work on tickets, add items that can be downloaded from the **User Console**, add articles to the Knowledge Base, and manage announcements that appear on the **User Console** home page. However, they do not manage users, run reports, or change appliance settings. This guide refers to this group as **Service Desk Admin**.

If the Organization component is enabled on your appliance, you can create separate Service Desk Admin roles for each organization.

1. Go to the *Role Detail* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Settings**, then click **Roles**.

c. Select **Choose Action** > **New**.

2. In the *Name* field, provide name, such as Service Desk Admin.
3. In the *Description* field, provide a brief description of the role, such as Used for Service Desk Administrators.

This appears on the *Roles* list.

4. Click the **[Expand All]** link next to Administrator Console *Permissions* to display the permissions settings for all categories.
5. Select these custom permissions for the new role:

Category	Item	Permission level
Home	**All**	All Read
Inventory	**Devices**	WRITE
	Software	WRITE
	Software Catalog	WRITE
	License Compliance	HIDE
	Processes	HIDE
	Startup Programs	HIDE
	Services	HIDE
	Discovery Schedules	HIDE
	Discovery Results	HIDE
	SNMP Inventory Configurations	HIDE
Monitoring	**Devices**	READ
	Alerts	WRITE
	Profiles	HIDE
	Maintenance Windows	HIDE
	Log Enablement Packages	HIDE
Assets	**All**	HIDE
Distribution	**All**	HIDE
Scripting	**All**	HIDE
Security	**All**	HIDE

Category	Item	Permission level
Service Desk	**Tickets**	WRITE
	User Downloads	WRITE
	Knowledge Base	WRITE
	Announcements	WRITE
	Archive	READ
	Configuration	READ
Reporting	**All**	All Hide
Settings	**All**	All Hide
User Console	**All**	All Read

6. Click **Save**.

The *Roles* page shows the new role. When a user who is assigned to this role logs in, the appliance component bar shows the available features.

Assign user roles

After you import or create user accounts, you can assign user roles to those accounts.

NOTE: User accounts can be imported from an LDAP server. See Importing users from an LDAP server.

1. Go to the *Users* list:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Settings**, then click **Users**.
2. Assign the **Administrator** role to your Service Desk administrators:
   a. Select the check box next to one or more users.
   b. Select **Choose Action** > **Apply Role** > **Administrator**.

   By default, Administrator users have owner/submitter permissions.
3. Assign the **Service Desk Staff** role to your team users:
   a. Select the check box next to one or more users.
   b. Select **Choose Action** > **Apply Role** > **Service Desk Staff**.
4. Assign the **All Ticket Owners** label to your Service Desk team members:
   a. Select the check box next to one or more users.
   b. Select **Choose Action** > **Apply Label** > **All Ticket Owners**.

   The label is applied, and it appears next to the username.
5. Create a label named **User**, then apply the **User** label and role to users.

Related topics

Define custom ticket fields

Create a Service Desk staff role

Add an All Ticket Owners label

Apply labels and roles to Service Desk staff

You can apply labels and roles to Service Desk staff members to manage their permissions.

For instructions on creating labels and roles, see Setting up roles for user accounts and Setting up labels for user accounts.

1. Add a user to the **DefaultTicketOwners@mydomain.com** alias.
2. Go to the *User Detail* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Settings**, then click **Users**.
    c. Display the *User Detail* page by doing one of the following:
    # Click the name of a user.
    # Select **Choose Action** > **New**.
3. In the *Restrict To Label* field, click **Edit**.
4. In the label window, drag the **All Ticket Owners** label to the *Restrict to Labels* field, then click **Save**.

    NOTE: If the label does not exist, you need to create it.

5. In the *Role* field, select the **Service Desk Staff** role.
6. Click **Save**.

The user has permission to own, modify, fix, and close tickets. The user automatically receives email when a ticket is created.

Related topics

Add an All Ticket Owners label

Create a Service Desk staff role

Create the DefaultTicketOwners account

If you want your Service Desk staff to receive email notifications when new tickets are created, you can create a DefaultTicketOwners user account.

You can then configure the *Ticket Detail* page to use that account as described in Configuring ticket settings.

To learn about email notifications, see About email notifications.

1. Go to the *User Detail* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Settings**, then click **Users**.
    c. Select **Choose Action** > **New**.
2. At minimum, provide the following details:

Field	Description
Login	DefaultTicketOwners
Name	DefaultTicketOwners

Field	Description
Email	DefaultTicketOwners@**mydomain.com**
Password	Enter a password
Confirm Password	Enter the password again
Role	No Access
Restrict to Label	All Ticket Owners

3. Click **Save**.
4. To assign this new user as the default ticket owner, choose the **DefaultTicketOwners** as described in Configuring ticket settings.

NOTE: The first default owner always remains the default owner of a ticket. For example, if you move an existing ticket to another category with a different default owner, the default owner of the ticket does not change.

Configuring email settings

You can set up an email notification strategy for a queue. If you have multiple queues, you can configure email settings for each queue separately.

An email notification strategy is described in the System requirements.

By default, Service Desk automatically sends an email to alert your staff if a ticket remains in a particular state too long. In addition, a ticket with a priority of **High** is escalated if it is not modified or closed within 30 minutes. To change the escalation times and the list of tickets to which they apply, see Customize the Ticket Detail page.

In general, the appliance should never be configured to email itself. For example, if a queue's email address is `helpdesk@example.com`, the `helpdesk@example.com` email address should not be a valid selection for the *Category CC* list or any of the settings where email addresses can be specified.

The following email notification strategy is used by most Quest KACE customers to prevent their staff from being inundated with unnecessary notifications:

- When a ticket is created, all Service Desk staff receive email notification. To learn about email notification caveats, see About email notifications.
- After a Service Desk staff member takes ownership of a ticket, the remaining staff does not receive email about the ticket unless it is escalated, although they can search for it.
- The ticket submitter and owner are notified by email each time their ticket's *State* or *Status* changes.
- The ticket owner is notified of any changes to the ticket.
- If a ticket is escalated, the ticket owner, and anyone else in the *Category CC* list, is notified.

About email notifications

When Service Desk tickets are created or changed, the appliance sends email notifications based on the ticket submission method, Email on Events settings, and actions taken.

The following rules are applied to email notifications:

- When tickets are submitted or modified through the **Administrator Console** or **User Console**, the ticket submitter does not receive an email confirmation, unless *New Ticket Via Portal*\ is selected for the *Submitter* in the *Email on Events* section on the *Service Desk Queue Email Settings* page (for more information about queue-specific email

settings, see Configure email triggers). Other users associated with the ticket, such as the **Owner**, **Approver**, **CC List**, and **Category CC**, receive email notifications as specified in the *Email on Events* section of the *Queue Detail* page. See Configuring email triggers and email templates for complete details.

- When tickets are created through email, the ticket submitter receives an email confirmation. However, when a ticket is modified by email, the submitter does not receive a confirmation.
- Change notification email messages are intentionally delayed when tickets are changed. This delay is designed to reduce the number of email notifications sent when changes are made. For example, a ticket owner might add a comment and save the ticket, then make a second, immediate change to the ticket. Only one change notification is sent.

  NOTE: Email messages are prepended with: +++++ Please reply above this line to add a comment +++++.

- When managed devices or user accounts are deleted from inventory, email notifications for any Service Desk tickets related to those devices are suppressed to avoid unnecessary notifications.

About Ticket Rules

If the standard email behavior does not meet your needs, you can use Ticket Rules to change the behavior.

For more information about Ticket Rules, see Using Ticket Rules.

Many of the more complex Ticket Rules, such as modifying the behavior of email notifications, are published on the **Quest Support** site, https://support.quest.com/contact-support.

About POP3 email accounts

You can configure the appliance to receive email from POP3 servers.

To do so, you need to:

- Enable and configure an external SMTP server in the appliance network settings. See Use an external SMTP server or Secure SMTP server.
- **Optional**. Configure Service Desk email preferences. See Configure email preferences.
- Configure SMTP server and POP3 settings in Service Desk ticket queues. See Configure queue-specific email settings.

If you do not use a POP3 email server, you can use the KACE SMA's built-in SMTP server to accept incoming email messages from your internal email server.

IMPORTANT: The appliance POP3 email server must pass authentication information and the email text itself as clear text.

Create and configure POP3 email accounts

You can create and configure POP3 email accounts for use by the Service Desk users and staff.

The two accounts are:

- **Support@mydomain.com**. This email address is used to:
  - # Receive all new tickets when they are created.
  - # Allow users and Service Desk staff to automatically create and modify tickets.
  - # Serve as the email address to which your users can reply.

The email delivered to this address is not read, but Service Desk staff is notified of the ticket changes resulting from the email.

- **DefaultTicketOwners@mydomain.com**. This email alias is used to:
  - # Allow Service Desk staff to communicate with each other.
  - # Allow the appliance to send automated email notification about new and open tickets.

1. Create Support@**mydomain**.com as a valid email address on your POP3 email server.
2. Configure DefaultTicketOwners@**mydomain**.com as the Service Desk staff email alias, and add all of your Service Desk staff email addresses to it. This is the general-purpose email alias that your Service Desk staff uses to communicate with each other.
3. If you want to use an external SMTP server used by the appliance, configure it on the *Network Settings* page in the System Administration Console. See Change appliance network settings.

   TIP: If you want to use POP3 for Service Desk ticket emails, you can configure the POP3 settings on the queue level.

4. **Optional**. Configure Service Desk email preferences. See Configure email preferences.
5. If you want to use different SMTP or POP3 settings for each queue, you can specify them on the queue level. See Configure queue-specific email settings.

Configure email preferences

You can create and configure preferences for the email sent to and from the Service Desk users and staff.

By default, the Service Desk is configured to use an internal SMTP server for sending ticket-related emails. You have an option to use an external SMTP server, however, you must configure it in the appliance network settings. For more information, see Change appliance network settings.

1. Go to the *Service Desk Email Preferences* page:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Service Desk**, then click **Configuration**.
   c. On the **Configuration** panel, in the *Email Configuration* section, click **Configure Email Preferences**.
2. On the *Service Desk Email Preferences* page that appears, in the *Outbound Email* tab, select the *Include "Reply above this line" text on outbound email communications* check box.

   It is recommended to use this feature to prevent the entire email chain from being added to each comment.

3. Specify the text that you want to detect in the email subject. When the Service Desk receives a ticket-related email with the specified subject, it will stop processing that email.
   a. In the *Inbound Email* tab, in the *Ignore emails with following text in the subject* field, type the words that you want to detect. You can specify multiple entries, using a semi-colon as a separator. For example: Out of Office;Mail Delivery Failure.
4. Configure the thresholds for all inbound email notifications during a specific period. When these levels are reached, the Service Desk will stop sending email notifications.

   NOTE: When the overall threshold is reached, notifications will pause for all tickets. If a per-ticket threshold is reached, notifications will be paused only for the affected ticket. When the number of email updates in the given period becomes lower than the configured threshold, the notifications will resume.

Option	Description
Total Emails per Ticket	The maximum number of all emails the Service Desk receives and responds with email notifications. The default value is 100 emails.
Received within the interval of x minutes	The time interval in minutes during which the specified number of emails are received. The default value is one minute. To disable this restriction, you can set to a high number such as 99999.

5. Configure the thresholds for inbound email notifications per ticket, during a specific period. When these levels are reached, the Service Desk will stop sending email notifications.

Option	Description
Total Emails per Ticket	The maximum number of all emails the Service Desk receives for each ticket, and responds with email notifications. The default value is 5 emails per ticket.
Received within the interval of x minutes	Specify the time interval in minutes during which the specified number of emails for each ticket are received. The default value is one minute. To disable this restriction, set this option to a high number such as 99999.

6. Click **Save**.

Next, you can configure POP3 email accounts for specific Service Desk queues. For more information, see Configure queue-specific email settings.

Configuring email triggers and email templates

You can set up triggers that automatically send email from the appliance and use templates to set the content of those email messages.

The *Email on Events* section determines which actions trigger an email to the various appliance users. Email templates determine the content of the messages.

Timing of email messages

The following email events trigger the appliance to send email immediately:

- **Comment**: The system sends email notifications for comments when users add comments and click **Submit** on the ticket form. When users add comments and click **Save** on the ticket form, however, only the *Any Change* notification is sent.
- **Ticket Closed**: If the Satisfaction Survey is enabled, an email that describes the Satisfaction Survey is sent immediately when tickets are closed.

The following email events trigger the appliance to send email every few minutes to prevent email overload:

- Any Change
- Owner Change
- Status Change
- Approval Change
- Resolution Change
- Escalation
- SLA Violation
- New Ticket Via Email

Configure email triggers

You can configure email triggers for a queue. If you have multiple queues, you can configure the email triggers for each queue separately.

1. Go to the Service Desk *Queue Detail* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Service Desk**, then click **Configuration**.
    c. On the **Configuration** panel, in the *Email Configuration* section, click **Setup email on events**.
    d. Display the *Queue Detail* page by doing one of the following:
    # Click the name of a queue.
    # Select **Choose Action** > **New**.
2. On the *Queue Detail* page, under *Email Address*, click **[edit]** link to display the *Service Desk Queue Email Settings* page.
3. On the *Service Desk Queue Email Settings* page, in the *Email on Events* tab, select the options for sending email when the specified events occur. Each column represents a type of Service Desk user (role) and each row represents a ticket event.

Service Desk user (role)	Description
Owner	The person who is expected to resolve the ticket.
Submitter	The person whose issue is being resolved.
Approver	The person who can approve or reject the ticket for processing.
Ticket CC	One or more email addresses that are stored in the *CC* field of the ticket.
Category CC	One or more email addresses that are stored in the *CC List* of the *Category Value* of the ticket. See Configure CC lists for ticket categories.
Queue Owners	One or more owners of the ticket queue, as specified by the *Owner* label. This only applies to the *New Ticket Via Email* and *New Ticket via Portal* events.

When a ticket event occurs, email is sent to the selected roles or users. For example, if you select the **Any Change** box in the *Owner* column, email is sent to the ticket owner whenever the ticket is changed. For the *Comment* and *Ticket Closed* triggers, email is sent immediately. For other ticket changes, however, email is sent every few minutes to prevent email overload.

NOTE: If users have the KACE GO mobile app installed on their smart phone or tablet, the system sends push notifications for the selected Service Desk ticket events.

Option	Description
Any Change	Any information on the ticket is changed.
Owner Change	The ticket's *Owner* field is changed.

Option	Description
Status Change	The ticket's *Status* field is changed.
Comment	Information, attachments, or screen shots are added to the ticket's *Comments* section. The system sends email notifications for comments when users add comments and click **Submit** on the ticket form. When users add comments and click **Save** on the ticket form, however, only the *Any Change* notification is sent.
Approval Change	The ticket's approval status has changed.
Resolution Change	The ticket's resolution has changed.
Response SLA Escalation	The ticket has not been updated to a stalled or closed status within the escalation time defined by the ticket priority.
Resolution SLA Violation	The ticket has not been resolved by its due date.
Ticket Closed	The ticket's *Status* field is changed to **Closed**. This event is used to present a Satisfaction Survey to submitters. See Using the Satisfaction Survey.
New Ticket Via Email	A user sends an email message to the Service Desk and a ticket is created.
New Ticket Via Portal	A ticket is created through the **User Console**.

4. Click **Save**.

Related topics

Configuring Mobile Device Access

Configure email templates

You can configure the email templates that Service Desk uses to generate email messages for a queue. If you have multiple queues, you customize the email templates for each queue separately.

1. Go to the Service Desk *Queue Detail* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Service Desk**, then click **Configuration**.
    c. On the **Configuration** panel, click **Create and manage queues** in **Queue** section.

d. Display the *Queue Detail* page by doing one of the following:

Click the name of a queue.

Select **Choose Action** > **New**.

2. On the *Queue Detail* page, under *Email Address*, click **[edit]** link to display the *Service Desk Queue Email Settings* page.
3. On the *Service Desk Queue Email Settings* page, complete one of the following steps.
   - **To edit all email templates, click Customize All Emails.**
   - **To edit a specific email template, in the *Events* area, in the row containing the email template you want to edit, in the *Customize Email* column, click .**
4. On the page that appears, change one or more of the selected email templates, as required.

NOTE: If the default text for any of the templates is changed, the email messages will not be translated into different languages.

The following email template are available:

Ticket-related template	Description	Default recipients
Response SLA Escalated	Used to send periodic notifications according to the Escalation Time configured for the ticket priority in the queue. For example, if tickets with the priority of **High** have an Escalation Time of 30 minutes, this email is sent every 30 minutes for High priority tickets until the ticket priority changes or until the ticket is closed.	Owners, the ticket CC list, and ticket Category CC list
Ticket Created from Email(Queue Owners)	Used to acknowledge that a ticket has been created through email.	Owners, Submitters
Ticket Created from Portal	Used to acknowledge that a ticket has been created through the **User Portal**.	Owners, submitters
Ticket Modified	Used to notify recipients when ticket information is changed or added.	Owners and the ticket CC list
Comment Submitted	Used to notify recipients that comments are added to tickets.	Owners, submitters, approvers, the ticket CC list, and the ticket Category CC list
Ticket Closed	Used to present a Satisfaction Survey to submitters when tickets are closed. See Using the Satisfaction Survey.	Submitters
Email Ticket Manually	Used to for messages that are forwarded using the *Email Ticket* action on *Ticket Detail* pages. **TIP:** If you use HTML/Markdown, the $ticket_fields_visible token must be enclosed in the `<pre>` tag to prevent formatting, such as line breaks, from being discarded. For example:	Manually entered by the sender

Ticket-related template	Description	Default recipients
	<pre>$ticket_fields_visible</pre>	
Resolution SLA Violated	Used to notify recipients that a ticket has remained open past the due date calculated using the SLA (Service Level Agreement) settings and the ticket priority.	None. Configurable on the *Queue Detail* page

Error-related template	Description	Recipients
Error Creating Ticket from Email	Used to notify senders that the ticket could not be created for reasons other than **unknown email address**.	Submitters
Unknown Email Address Response	Used to notify senders that the ticket could not be created because the submitter's email address is unknown.	Submitters

Table 6. Tokens used in all email templates

Token	Description
$helpdesk_email	The email address associated with the Service Desk queue. This address is configured on the *Queue Detail* page.
$helpdesk_name	The name of the Service Desk queue. This name is configured on the Queue Detail page.
$userui_url	A link to the **User Console**. Access to the **User Console** requires login credentials.

Table 7. Tokens used in ticket-related email templates

Token	Description
$change_desc	A formatted representation of the changes that were made the last time the ticket was saved, including both field changes and comments.
$last_attachment	The most recent attachment added to the ticket.
$last_comment	The most recent comment added to the ticket.
$mobile_ticket_url	A link to the ticket KACE GO mobile app. When displayed in an email on an Android or iOS mobile device, this links opens the associated ticket in the KACE GO mobile app.
$process_description	The process description. It can include important pre-requisites that the users need to complete before proceeding to create a ticket based on a process template.
$process_name	The name of the process template.

Token	Description
$process_status	The status of the process template such as Approval Required, Approval Timed Out, Approval Received, Approval Rejected, Process Cancelled, and Process Complete.
$process_type	The type of the process. In a default installation, only the *Service Desk* process type is included. You can create new process types, as required. For example, you can create a process type for accessing a specific application, or a group of applications. For more information, see Define process types.
$summary	The current summary of the ticket.
$ticket_approver_email	The email address of the ticket approver. Having this address is especially useful for *Comments* email notifications.
$ticket_approver_name	The name of the ticket approver. **NOTE:** The approver name and contact information is derived from the USER record associated with the fields on the ticket.
$ticket_approver_phone_home	Contact information for the ticket approver.
$ticket_approver_phone_mobile	Contact information for the ticket approver.
$ticket_approver_phone_pager	Contact information for the ticket approver.
$ticket_approver_phone_work	Contact information for the ticket approver.
$ticket_custom_X_label $ticket_custom_X_value	The label and value used for a custom field, where **X** represents the index number of the custom field. For example, if a queue has a ticket field labeled, *CUSTOM_5*, and that field is configured with the label *Location Name*, the system replaces `$ticket_custom_5_label` with the text, `Location Name`. The token, `$ticket_custom_5_value` is replaced with the ticket value that was saved for the *Location Name* field, such as, *Topeka* or *Albuquerque*. By default, all ticket queues are configured with 15 custom fields, but this number can be increased as needed. **NOTE:** Each queue can have different custom fields and different email template configurations.
$ticket_due_date	The due date as saved on the ticket. Administrators can override automatic due dates with manual due dates if necessary.
$ticket_escalation_minutes	The time, in minutes, between periodic notifications. This time is determined by the Escalation Time configured for the ticket priority in the queue. For example, if tickets with the priority of **High** have an Escalation Time of 30 minutes, this email is sent every 30 minutes for High priority tickets until the ticket priority changes or until the ticket is closed. This token is typically used in the Ticket Escalated email template, to inform recipients of the frequency of email notifications.

Token	Description

$ticket_fields_visible	Include all the ticket fields that are visible for the user who is forwarding the ticket by email.
	TIP: If you use HTML/Markdown, the $ticket_fields_visible token must be enclosed in the `<pre>` tag to prevent formatting, such as line breaks, from being discarded. For example:
	`<pre>$ticket_fields_visible</pre>`

$ticket_history	The complete history of the ticket. **NOTE:** For some tickets, the history information can become very detailed and too large to send through email. If the complete history is not needed, use `$ticket_history_X` to limit the number of records to include.
$ticket_history_X	A specified number of records in the ticket history. `X` indicates the number of records to include, beginning with the most recent.
$ticket_id	A unique identifier assigned to the ticket, also called the ticket number. Using this identifier is the primary method for users to identify tickets.
$ticket_number	A formatted version of the ticket ID. This version begins with `TICK` followed by a minimum of five digits. For example, a ticket with ID `4321` is displayed as `TICK:04321`. This format is especially useful in email Subject lines to make sure that email replies link to the correct tickets.
$ticket_owner_email	The email address of the Service Desk administrator assigned to the ticket.
$ticket_owner_name	The name of the Service Desk administrator assigned to the ticket. **NOTE:** The owner name and contact information is derived from the USER record associated with the fields on the ticket.
$ticket_owner_phone_home	Contact information for the Service Desk administrator assigned to the ticket.
$ticket_owner_phone_mobile	Contact information for the Service Desk administrator assigned to the ticket.
$ticket_owner_phone_pager	Contact information for the Service Desk administrator assigned to the ticket.
$ticket_owner_phone_work	Contact information for the Service Desk administrator assigned to the ticket.
$ticket_priority	The priority assigned to the ticket. Default values include High, Medium, and Low.

Token	Description
$ticket_resolution	Information about what was done to resolve the ticket as described in the ticket's *Resolution* field.
$ticket_status	The status of the ticket. Defaults include New, Opened, Closed, Need More Info, Reopened, Waiting Overdue, Waiting on Customer, and Waiting on Third Party.
$ticket_submitter_email	The email address of the submitter.
$ticket_submitter_name	The name of the submitter. **NOTE:** The submitter name and contact information is derived from the USER record associated with the fields on the ticket.
$ticket_submitter_phone_home	Contact information for the submitter.
$ticket_submitter_phone_mobile	Contact information for the submitter.
$ticket_submitter_phone_pager	Contact information for the submitter.
$ticket_submitter_phone_work	Contact information for the submitter.
$ticket_title	The title of the ticket as it appears on the *Ticket Detail* page.
$ticket_url	A link to the ticket in the **User Console**. Access to the **User Console** requires login credentials.
$ticket_http_url	A link to the ticket in the **User Console**. This format is used for backward compatibility on older systems. Access to the **User Console** requires login credentials.
$ticket_https_url	A secure link to the ticket in the **User Console**. Use this token if SSL is enabled on your appliance. This ensures that links sent through email work correctly.
$userui_url	A link to the home page of the **User Console**. Access to the **User Console** requires login credentials.

Table 8. Tokens used in merged ticket email templates

Token	Description
$ticket_merged_number	The number of the merged ticket.
$ticket_merged_title	The title of the merged ticket as it appears on the *Ticket Detail* page.
$ticket_merged_changer_name	The name of the user who merged the tickets.
$ticket_merged_url	A link to the merged ticket in the **User Console**. Access to the **User Console** requires login credentials.

Table 9. Tokens used in error-related email templates

Token	Description
$error_text	Used to identify a problem processing the submitted tokens. This error appears when: • The system does not recognize a variable • A variable is recognized, but the user does not have permission to change the field • The variable attempts to change the approval status of the ticket but the user is not the approver
$quoted_mail	The content of the original email message.
$subject	The subject of the original email message.

NOTE: Tokens that are invalid are ignored and they are not replaced in email messages. For example, if you add an unknown token such as `$today`, it is ignored, and it appears in the email message as `$today`.

5. **Optional**: For each email template, create HTML-based content instead of using plain text.
   a. Select **Send as HTML** to use a HTML-based email instead of plain text.

      An HTML editor appears, with a full range of text editing options for formatting your content, such as buttons for bold text, hyperlinks, lists, or text color.

   b. Use the controls in the editor to format the template content. For example:

   # To apply bold text to a text string, select it in the editor, and click B.

   # To add images, click , and provide the URL to the image file.

   - Any images you include this way will not be added as file attachments to the ticket.
   - Deleting an image from the text field will permanently remove it as the image in this field is not stored as an attachment.

   # To add external links, click .

   # To embed externally hosted videos, click .

   c. To quickly add a token, click $, and from the list that appears, select the applicable token.

      See step 4 for more information about each token.

6. For each template, indicate how you want to handle email file attachments.

   # To allow Service Desk to send file attachments, select **Include attachments**. Then, indicate which attachments you want to send:

   # **Most recent change (if applicable)**: Include only the file attachments that are added with the most recent ticket update.

   # **Last uploaded**: Include the last uploaded file attachments.

   # **All**: Include all file attachments.

   - **To prevent Service Desk from sending file attachments with ticket-related email, clear the Include attachments check box.**

7. Click **Save**.

For instructions on how to configure the appliance to use SMTP email, see Configuring SMTP email servers.

Configure CC lists for ticket categories

You can automatically notify users, or groups of users, when tickets are filed in specified categories, such as hardware, software, or networking. To do this, add email addresses to the *CC List* value of each ticket category.

Configuring the *CC List* values of ticket categories is useful if you want to notify users, or groups of users, when tickets are filed in categories that interest them. For example, you could add all of your system administrators to the *CC List* of the Network category to ensure that they are notified of networking issues as they arise.

If you have multiple queues, you configure the ticket category *CC List* values for each queue separately.

1. Go to the Service Desk *Queue Detail* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Service Desk**, then click **Configuration**.
    c. On the **Configuration** panel, click **Create and manage queues** in **Queue** section.
    d. Display the *Queue Detail* page by doing one of the following:
    # Click the name of a queue.
    # Select **Choose Action** > **New**.
2. In the *Email on Events* tab, select all of the check boxes under the *Category CC* column. See Configure email triggers.
3. Click **Save**.
4. In the *Queues* section, select the **Customize field**.
5. In the *Category Values* tab, add email addresses to the *CC List* entries:
    a. Click the **Edit** button in a category row: .
    b. In the *CC List* field, enter a default email address for the category. Use commas to separate email addresses. To enter multiple email addresses, consider using a distribution list.
    c. Click **Save** at the end of the row.
    d. Repeat this process to add *CC List* entries for other categories.
6. Click **Save** at the bottom of the page.

Create a default email address for ticket owners. See Create the DefaultTicketOwners account.

Automatically add email addresses to ticket CC List fields

You can enable Service Desk to automatically add email addresses to the *CC List* field of tickets whenever those addresses appear in the *To* and *Cc* fields of tickets submitted or updated through email.

When this setting is enabled, any email addresses in the *To* and *Cc* fields are automatically added to ticket *CC List* fields unless those addresses are specified in the *System Email Exclusion List*. See Exclude addresses from ticket CC List fields.

NOTE: If your Service Desk was created on an appliance running version 6.3 or earlier, this setting is disabled by default. If the Organization component is enabled on your system, and you create a new organization, however, the setting is enabled by default. The setting is also enabled on new KACE SMAs running version 6.4 or later.

1. Go to the Service Desk *Settings* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Service Desk**, then click **Configuration**.

c. On the *Configuration* panel, click **Service Desk Email Preferences** in the *Email Configuration* section.

2. In the *Inbound Email* tab, select the check box next to *Add email addresses from the CC List to ticket*.
3. Click **Save**.

Configure the email exclusion list to prevent Service Desk from automatically adding unwanted email addresses to ticket *CC List* fields. See Exclude addresses from ticket CC List fields.

Exclude addresses from ticket CC List fields

Service Desk can automatically add email addresses to ticket *CC List* fields when tickets are submitted or updated through email. However, some addresses, such as distribution lists and general company email addresses, should not be added automatically because they increase unnecessary email traffic. To prevent Service Desk from adding unwanted email addresses, you can specify the email addresses you want to exclude.

The email exclusion list is an appliance-level setting. If the Organization component is enabled on your appliance, the email exclusion list is applied to all organizations and Service Desk queues.

NOTE: The email addresses associated with Service Desk queues are never automatically added to ticket *CC List* fields, because sending messages to these addresses could result in new tickets being opened inadvertently. You do not need to add these addresses to the exclusion list.

1. Go to the Service Desk *Settings* page:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Service Desk**, then click **Configuration**.
   c. On the *Configuration* panel, click **Service Desk Email Preferences** in the *Email Configuration* section.
2. In the *Inbound Email* tab, click **System Email Exclusion List** to display the *Define System Email Exclusion List page*.
3. To add an email address to the list, click add: ✚.
4. In the *Add Email* dialog, type an email address, then click **Save**.

   The email address is added to the exclusion list.

Prevent email loops

When tickets are submitted or updated through email, Service Desk sends ticket notifications to respective parties. However, if one or more users who receive such email reply with an automated *Out of Office* response, Service Desk reacts with another ticket update and yet another email notification, potentially causing an infinite email loop.

You can prevent the Service Desk from processing an email when an Out of Office response is received. You also have an option to stop sending email notifications when a high number of incoming ticket-related emails is detected. Any emails that cause the Service Desk to stop sending email notifications are logged.

1. Go to the *Service Desk Email Preferences* page:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Service Desk**, then click **Configuration**.
   c. On the **Configuration** panel, in the *Email Configuration* section, click **Configure Email Preferences**.
2. Specify the text that you want to detect in the email subject. When the Service Desk receives a ticket-related email with the specified subject, it will stop processing that email.

a. In the *Inbound Email* tab, in the *Ignore emails with following text in the subject* field, type the words that you want to detect. You can specify multiple entries, using a semi-colon as a separator. For example: Out of Office;Mail Delivery Failure.

3. Configure the thresholds for all inbound email notifications during a specific period. When these levels are reached, the Service Desk will stop sending email notifications.

NOTE: When the overall threshold is reached, notifications will pause for all tickets. If a per-ticket threshold is reached, notifications will be paused only for the affected ticket. When the number of email updates in the given period becomes lower than the configured threshold, the notifications will resume.

Option	Description
Total Emails per Ticket	The maximum number of all emails the Service Desk receives and responds with email notifications. The default value is 100 emails.
Received within the interval of x minutes	The time interval in minutes during which the specified number of emails are received. The default value is one minute. To disable this restriction, you can set to a high number such as 99999.

4. Configure the thresholds for inbound email notifications per ticket, during a specific period. When these levels are reached, the Service Desk will stop sending email notifications.

Option	Description
Total Emails per Ticket	The maximum number of all emails the Service Desk receives for each ticket, and responds with email notifications. The default value is 5 emails per ticket.
Received within the interval of x minutes	Specify the time interval in minutes during which the specified number of emails for each ticket are received. The default value is one minute. To disable this restriction, set this option to a high number such as 99999.

5. Click **Save**.

Configure the Cache Lifetime for Service Desk widgets

Service Desk widgets available on the *Dashboard* page provide insight into the overall activity of your Service Desk tickets. For example, you can view the number of active tickets sorted by their category or queue. For performance reasons, underlying data for the Service Desk widgets is cached locally for a fixed duration. The default minimum is 30 minutes. This can be increased as needed. You can force a data refresh for a specific widget by clicking the refresh icon in the widget.

For more information about *Dashboard* widgets, see About Dashboard widgets.

1. Go to the Service Desk *Settings* page:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Service Desk**, then click **Configuration**.
   c. On the *Configuration* panel, click **Set dashboard cache lifetime** link in the Settings section.
2. Under *Dashboard Settings*, in the *Cache Lifetime field*, specify the length of time in minutes during which the data populating the Service Desk Dashboard widgets will be preserved in the database. The minimum is 30 minutes.
3. Click **Save**.

Creating and managing organizations

If the **Organization** component is enabled on your appliance, you can create and manage separate organizations, with separate inventory and settings, to meet your business needs.

TIP: If the Organization component is enabled on your appliance, but you do not see the drop-down list in the top-right corner of the **Administrator Console** next to the login information, there are two possibilities: Either fast switching is not enabled, or your user role does not have permission to manage organizations.

TIP: See Enable fast switching for organizations and linked appliances.

About organizations

Organizations are logical instances of an appliance that run on a single appliance. Each organization is supported by its own database, and you manage each organization's inventory and other components separately.

For example, in a school environment, you could create one organization for teachers and another organization for students. You could then automatically assign managed devices to each organization and manage them separately. Further, you could assign organization-specific roles to administrators and users to control their access to the appliance **Administrator Console** and **User Console**. Administrators in one organization would not need to view the devices and inventory items in the other organization. You can add up to 50 organizations on a single appliance.

For information about configuring general organization settings for the appliance, see Configure appliance General Settings with the Organization component enabled.

About the Default organization

The organization named **Default** is the only organization that is available when you first set up the appliance. New devices that are not assigned to an organization by a filter are assigned to the Default organization.

You can rename the Default organization and edit its settings as needed. See Add or edit organizations.

Tracking changes to organization settings

If History subscriptions are configured to retain information, you can view the details of the changes made to settings, assets, and objects.

This information includes the date the change was made and the user who made the change, which can be useful during troubleshooting. See About history settings.

Managing Organization Roles and User Roles

If the Organization component is enabled on your appliance, there are two types of roles: Organization Roles, which are applied to organizations, and User Roles, which are applied to individual user accounts.

If the Organization component is enabled on your appliance, there are two types of roles: Organization Roles, which are applied to organizations, and User Roles, which are applied to individual user accounts.

This section describes the default Organization and User Roles, and explains how to manage Organization Roles. For information about managing User Roles, see About user accounts and user authentication.

Available default roles

Default roles provide a variety of permission settings for organizations and users.

The following roles are available by default.

Role	Description
Organization Roles	Organization Roles are supersets of permissions that are assigned to organizations, and they define the permissions that are available to organization users. For example, if an organization is assigned an Organization Role that has the *Distribution* tab hidden, users in that organization, including the Admin user, cannot access the *Distribution* tab. **NOTE:** Organization Roles are available only on appliances with the Organization component enabled.
Default Role	The Default Role in the Organization Roles section has Write and Read permission for all tabs. You can create additional Organization Roles, but you cannot edit or delete the Default Role.
User Roles	Roles assigned to users to control their access to the **Administrator Console** and **User Console**. If the Organization component is enabled on your appliance, the permissions available to these roles depends on the Organization Role assigned to the organization.
Administrator	The most powerful user role on the appliance. By default, users with the **Administrator** role have permission to see or change information and settings. This includes promoting or demoting other users by changing their roles. The **Administrator** role cannot be altered or deleted. Assign this role only to trusted administrators. Staff members assigned the **Administrator** role have permission to manage and modify Service Desk tickets from the *Tickets* tab in the **Administrator Console**, though they might not be able to own tickets themselves. Users with the **Administrator** role can also use the security, scripting, and distribution features to resolve Service Desk tickets, then document the issues in the Knowledge Base. The **Administrator** role primarily interacts with the appliance through the **Administrator Console**.
No Access	Users with this role cannot log on to the **Administrator Console** or **User Console**.
Read Only Administrator	This role has the ability to view but not change any information or settings in the appliance. This role is useful for oversight personnel, such as supervisors. This role primarily interacts with the appliance through the **Administrator Console**.
User Console Only	This role is for appliance users. By default, this role has permission to create, view, and modify Service Desk tickets. This role interacts with the appliance exclusively through the **User Console**.

Add or edit Organization Roles

You can add or edit Organization Roles as needed.

Before you create organizations, create the Organization Roles you want to assign to those organizations as described in this section. Organization Roles define the permissions that are available to organization users.

1. Go to the *Organization Role Detail* page:
    a. Log in to the appliance System Administration Console, `http://`**appliance_hostname**`/system`, or select **System** from the drop-down list in the top-right corner of the page.
    b. On the left navigation bar, click **Organizations**, then click **Roles**.
    c. Display the *Organization Role Detail* page by doing one of the following:
    # Click the name of a role.
    # Select **Choose Action** > **New**.

    NOTE: You cannot edit the Default Role.

2. Provide the following information:

Option	Description
Name	(Required) Enter a name for the role.
Description	(Optional) Enter a description of the role.

3. To assign Administrator Console permissions:
    - **In the Administrator Console *Permissions* section, click a component name to expand it, or click Expand All to expand all components.**
    - **To assign the same access level to all sections, select All Write, All Read, or All Hide.**
    - **To assign different access levels to different sections, select the Custom option, then select an access level in the drop-down list next to the name of each section.**
4. To assign User Console permissions:
    - **In the User Console *Permissions* section, click the User Console link to expand the permissions section.**
    - **To assign the same access level to all sections of the User Console, select All Write, All Read, or All Hide.**
    - **To assign different access levels to different sections, select the Custom option, then select an access level in the drop-down list next to the name of each section.**
5. Click **Save**.

    NOTE: If you assign the **Hide** permission to **General** and **User Authentication** under *Settings*, the *Control Panel* is hidden.

The role appears on the *Roles* page. When you add an organization, the role appears on the *Role* drop-down list. See Adding, editing, and deleting organizations.

Duplicate Organization Roles

When you duplicate an Organization Role, its properties are copied into the new role. If you are creating a role that is similar to an existing role, duplicating the role can be faster than creating a role from scratch.

1. Go to the *Organization Role Detail* page:
    a. Log in to the appliance System Administration Console, `http://`**appliance_hostname**`/system`, or select **System** from the drop-down list in the top-right corner of the page.
    b. On the left navigation bar, click **Organizations**, then click **Roles**.
    c. Click the name of a role.
2. Click **Duplicate** at the bottom of the page to duplicate the organization details.

The page refreshes.

3. Provide the following information:

Option	Description
Name	(Required) Enter a name for the role.
Description	(Optional) Enter a description of the role.

4. To assign Administrator Console permissions:
   - **In the Administrator Console *Permissions* section, click a component name to expand it, or click Expand All to expand all components.**
   - **To assign the same access level to all sections, select All Write, All Read, or All Hide.**
   - **To assign different access levels to different sections, select the Custom option, then select an access level in the drop-down list next to the name of each section.**
5. To assign User Console permissions:
   - **In the User Console *Permissions* section, click the User Console link to expand the permissions section.**
   - **To assign the same access level to all sections of the User Console, select All Write, All Read, or All Hide.**
   - **To assign different access levels to different sections, select the Custom option, then select an access level in the drop-down list next to the name of each section.**
6. Click **Save**.

Delete roles

With the exception of the Default Role, you can delete Organization Roles as needed. You cannot delete the Default Role, and you cannot delete a role if it is assigned to an organization.

The following roles cannot be deleted:

- the Default Role
- any roles assigned to an organization
- any roles associated with a label

1. Go to the *Roles* list:
   a. Log in to the appliance System Administration Console, `http://`**appliance_hostname**`/system`, or select **System** from the drop-down list in the top-right corner of the page.
   b. On the left navigation bar, click **Organizations**, then click **Roles**.
2. Select the check box next to one or more roles.
3. Select **Choose Action** > **Delete**, then click **Yes** to confirm.

Adding, editing, and deleting organizations

You can add, edit, and delete organizations as needed. In addition, you can rename the Default organization and edit its settings.

Add or edit organizations

You can add or edit up to 50 organizations on a single appliance.

When you add organizations, you need to assign them Organization Roles. You can use the Default Role, but if you want to use a custom Organization Role, add that role before you add the organization. See Add or edit Organization Roles.

1. Go to the *Organization Detail* page:
    a. Log in to the appliance System Administration Console, `http://`**appliance_hostname**`/system`, or select **System** from the drop-down list in the top-right corner of the page.
    b. On the left navigation bar, click **Organizations**, then click **Organizations**.
    c. Display the *Organization Detail* page by doing one of the following:
    # Click the name of an organization.
    # Select **Choose Action** > **New**.
2. If you are adding an organization, provide the following information, then click **Save**.

Option	Description
Name	Enter a name for the organization. You can modify the name later if required. If the fast switching option is enabled, this name appears in the drop-down list in the top-right corner of the page. See Enable fast switching for organizations and linked appliances.
Description	A description of the organization. You can modify the description later if necessary.
Role	The user role you want to assign to the organization. You can modify this selection later if required. **NOTE:** To create a role, go to **Organizations** > **Roles**.
Client Drop Size	A file-size filter for the organization's Client Drop location. The Client Drop location is a storage area (Samba share) for the organization on the appliance. This storage area is used to upload large files, such as application installers and appliance backup files, to the appliance. Uploading files to the Client Drop location is an alternative to uploading files through the **Administrator Console** using the default HTTP mechanism, which can result in browser timeouts for large files. The *Client Drop Size* filter determines whether files uploaded to the organization's Client Drop location are displayed on the *Upload and Associate Client Drop File* list on the *Software Detail* page. For example, if the Client Drop Size filter is set to 1 GB, the *Upload and Associate Client Drop File* list shows files that are 1 GB in size or larger. Files that are less than 1 GB in size are not displayed on the list. Application files are moved from the organization's Client Drop location to the appropriate area when the file is selected on the *Software Detail* page and saved. Appliance backup files that are placed in the Client Drop location are automatically identified as appliance backup files, and they become available for selection on the *Backup Settings* page within five minutes. If you have multiple organizations, each organization has its own Client Drop location and Client Drop Size filter setting. See Copy files to the appliance Client Drop location.

3. Add, edit, or view the following information:

Option	Description
Name	Modify the name of the organization as needed. If the fast switching option is enabled, this name appears in the drop-down list in the top-right corner of the page. See Enable fast switching for organizations and linked appliances.

Option	Description
Locale	The language to use for the organization's **Administrator Console** and **User Console**.
Virtual Host Name	A unique domain name for this organization. When this field is configured, and you log in to the appliance from the specified location, the appliance selects this organization automatically, and you only need to provide your user credentials. If you use Security Assertion Markup Language (SAML) login, the configured virtual host name logs you directly into that organization's Identity Provider (IdP). For more information about SAML login, see Configure SAML for single sign on.
Virtual Host IP	A unique IP address for this organization. When this field is configured, and you log in to the appliance from the specified location, the appliance selects this organization automatically, and you only need to provide your user credentials. If you use SAML login, the configured virtual host IP address logs you directly into that organization's IdP. For more information about SAML login, see Configure SAML for single sign on.
Description	A description of the organization. You can modify the description later if necessary.
Database Name	(Read-only) Displays the name of the database the organization is using.
Report User	(Read-only) The username used to generate reports. The report username provides access to the database (for additional reporting tools), but does not give write access to anyone.
Report User Password	The report user password. This password is used only by the reporting system and MySQL.
Role	The user role you want to assign to the organization. You can modify this selection later if required. **NOTE:** To create a role, go to **Organizations** > **Roles**.
Client Drop Size	A file-size filter for the organization's Client Drop location. The Client Drop location is a storage area (Samba share) for the organization on the appliance. This storage area is used to upload large files, such as application installers and appliance backup files, to the appliance. Uploading files to the Client Drop location is an alternative to uploading files through the **Administrator Console** using the default HTTP mechanism, which can result in browser timeouts for large files. The *Client Drop Size* filter determines whether files uploaded to the organization's Client Drop location are displayed on the *Upload and Associate Client Drop File* list on the *Software Detail* page. For example, if the Client Drop Size filter is set to 1 GB, the *Upload and Associate Client Drop File* list shows files that are 1 GB in size or larger. Files that are less than 1 GB in size are not displayed on the list. Application files are moved from the organization's Client Drop location to the appropriate area when the file is selected on the *Software Detail* page and saved. Appliance backup files that are placed in the Client Drop location are automatically identified as appliance backup files, and they become available for selection on the *Backup Settings* page within five minutes. If you have multiple organizations, each organization has its own Client Drop location and Client Drop Size filter setting. See Copy files to the appliance Client Drop location.

Option	Description
Filters	The filters you want to use to assign new devices to the organization when devices check in to the appliance. To select multiple filters, use **Ctrl**-click or **Command**-click.
Devices	(Read-only) Displays the number of devices assigned to the organization.

4. Specify the following settings in Agent tab:

NOTE: To reduce the load on the appliance, limit the number of Agent connections to 500 per hour. The number of connections that appears next to the inventory, scripting, and metering intervals, applies to the current organization only. If the Organization component is enabled on your appliance, the total number of Agent connections for all organizations should not exceed 500 per hour.

Option	Suggested Setting	Notes
Enable Agent Logging	Enabled	Whether the appliance stores scripting results provided by Agents installed on managed devices. Agent logs can consume as much as 1GB of disk space in the database. If disk space is not an issue, enable *Agent Logging* to keep all log information for Agent-managed devices. These logs can be useful during troubleshooting. To save disk space, and enable faster Agent communication, disable *Agent Logging*.
Agent Debug Trace	Enabled	If selected, this option allows you to record the Agent's debug trace. This information allows administrators to monitor the Agent's performance, and to diagnose common problems.
Agent Inventory	12 hours	The frequency at which Agents on managed devices report inventory. This information is displayed in the *Inventory* section.
Agentless Inventory	1 Day	The frequency at which Agentless devices report inventory. This information is displayed in the *Inventory* section.
Catalog Inventory	24 hours	The frequency at which managed devices report inventory to the *Software Catalog* page.
Metering	4 hours	The frequency at which managed devices report metering information to the appliance. Requires metering to be enabled on devices and applications.
Scripting Update	4 hours	The frequency at which Agents on managed devices request updated copies of scripts that are enabled on managed devices. This interval does not affect how often scripts run.
Max Download Speed	As required	The maximum download speed, as required. Choose from the available options.
Konea Connection Timeout	80 seconds	Configurable konea tunnel timeout check for bootup MI.
Enable Wait for Bootup Tasks	Disabled	If selected, this option stops the agent from executing bootup tasks.

Option	Suggested Setting	Notes
Enable Wait for Login Tasks	Disabled	If selected, this option stops the agent from executing login tasks.

5. In the Agent Settings tab in the *Agent Status Icon Settings* section, specify the following settings:

Option	Suggested Setting	Notes
Agent Status Icon On Device	Enabled	If selected, this option allows you to display the agent status on managed devices.
Enable Agent Snooze on Device	Enabled	If selected, this option allows you to suspend the agent's activity on managed devices using the system tray (Windows) or menu bar (Mac OS). **NOTE:** Some critical background tasks are still allowed to run, including inventory, replication tasks, and urgent alerts.
Agent Snooze Max Count (per day)	1 snooze	The maximum number of times you can snooze the agent each day on managed devices.
Agent Status Icon Shortcuts	As required	Use this section to display links in the KACE Agent menu on agent-managed devices. You can specify up to ten links. Standard Uniform Resource Identifier (URI) links are supported, such as `https`, `ssh`, and `ftp` URLs. To add a link: 1. Click +. 2. In the *Display Name* column, type the text that you want to display in the menu. For example, *My FTP link*. 3. In the URL column, type the fully qualified URL address. For example, `https://www.quest.com/`. The URL supports the following replacement variables: # $(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) For complete information about these and other replacement variables, see Token replacement variables. You can use the column headings to sort the list. In the KACE Agent menu, the links appear in the order they are listed on this page.

NOTE: Any changes that you make in this section take effect only after the KACE Agent on the managed device reconnects to the appliance, either by restarting each individual agent, or the appliance.

6. In the *Notify* tab, specify the message to use for Agent communications:

Option	Suggested Setting	Notes
Agent Splash Page Message	Default text: `KACE Systems Management Appliance is verifying your PC Configuration and managing software updates. Please Wait...`	The message that appears to users when Agents are performing tasks, such as running scripts, on their devices.
Agent Splash Bitmap	As required	The path to an existing .bmp file that you want to use as the splash logo.
Disable Bootup Splash	Disabled	If selected, this option stops the agent from displaying the boot-up splash logo.
Disable Login Splash	Disabled	If selected, this option stops the agent from displaying the login splash logo.

7. In the *Agentless Settings* tab, specify communications settings for Agentless devices:

Option	Description
SSH Timeout	The time, in seconds, after which the connection is closed if there is no activity.
SNMP Timeout	The time, in seconds, after which the connection is closed if there is no activity.
Retry Attempts	The number of times the connection is attempted.
WinRM Timeout	The time, in seconds, after which the connection is closed if there is no activity.
VMware Timeout	The amount of time in seconds to wait for a connection to the VMware vSphere API service running on a VMware host.

8. In the *Agentless Settings* tab, specify communications settings for Agentless devices:

Option	Description
SSH Timeout	The time, in seconds, after which the connection is closed if there is no activity.
SNMP Timeout	The time, in seconds, after which the connection is closed if there is no activity.
Retry Attempts	The number of times the connection is attempted.
WinRM Timeout	The time, in seconds, after which the connection is closed if there is no activity.
VMware Timeout	The amount of time in seconds to wait for a connection to the VMware vSphere API service running on a VMware host.

9. Click **Save**.

The organization is added. If fast switching is enabled, and the default **admin** account passwords for the System and for your organizations are the same, you can switch between organizations and the System using the drop-down list in the top-right corner of the page. To see new organizations in the list, you need to log out of the **Administrator Console** and then log back in. In addition, if the option to require organization selection at login is enabled at the System level, the organization is available in the drop-down list on the Administrator Console login page, `http://appliance_hostname/admin`, where **appliance_hostname** is the hostname of your appliance.

NOTE: For new organizations, the password for the default **admin** account is the same as the password for the default **admin** account at the System level. This is assigned automatically. To change the **admin** account password, edit the admin user account.

NOTE: However, be aware that organizations with different **admin** account passwords are not available for **fast switching** using the drop-down list in the top-right corner of the page.

For more information about System-level settings, see Configure appliance General Settings with the Organization component enabled.

Related topics

Managing organization filters

View appliance logs

Managing user accounts for organizations

Configure Two-Factor Authentication for organizations

Two-Factor Authentication (2FA) provides stronger security for users logging into the appliance by adding an extra step to the login process. It relies on the Google Authenticator app to generate verification codes. The app generates a new six-digit code at regular intervals. When enabled, end users will be prompted for the current verification code each time they log in.

To download the Google Authenticator app, visit one of the following sites, as applicable:

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

You can enable or disable 2FA access to the **Administrator Console** and **User Console** for one or more organizations using the **System Administration Console**, as described below. Alternatively, you can enable 2FA access to the **Administrator Console** and **User Console** for all users in an organization using the *Two-Factor Authentication* page in the **Administrator Console** For more information, see Enable Two-Factor Authentication for all users.

1. Go to the *Organizations* list page:
    a. Log in to the appliance System Administration Console, `http://`**appliance_hostname**`/system`, or select **System** from the drop-down list in the top-right corner of the page.
    b. On the left navigation bar, click **Organizations**, then click **Organizations**.
2. On the *Organization* list page that appears, select one or more organizations for which you want to configure 2FA.
3. To enable 2FA for all users in the selected organizations in the Administrator Console, click **Choose Action** > **Two-Factor Authentication** > **Admin Portal** > **Required for all Users**.
4. To disable 2FA for all users in the selected organizations in the Administrator Console, click **Choose Action** > **Two-Factor Authentication** > **Admin Portal** > **Not Required**.
5. To enable 2FA for all users in the selected organizations in the User Console, click **Choose Action** > **Two-Factor Authentication** > **User Portal** > **Required for all Users**.
6. To disable 2FA for all users in the selected organizations in the User Console, click **Choose Action** > **Two-Factor Authentication** > **User Portal** > **Not Required**.

Delete organizations

You can delete organizations as needed. However, if you have a single organization on your appliance, you cannot delete that organization until you add another one. The appliance must always have at least one organization available.

1. Go to the *Organization Detail* page:
    a. Log in to the appliance System Administration Console, `http://`**appliance_hostname**`/system`, or select **System** from the drop-down list in the top-right corner of the page.
    b. On the left navigation bar, click **Organizations**, then click **Organizations**.
    c. Click the name of an organization.
2. Select **Choose Action** > **Delete**, then click **Yes** to confirm.

The organization, including information in the organization database, is removed from the appliance.

Customizing the logos used for the User Console and organization reports

You can change the logo displayed on the **User Console** and in organization reports to match your company branding.

The **User Console**, and the reports you run when logged in to the organization through the **Administrator Console**, use the Quest logo by default. To upload your own logo, see the *Logo Overrides* section in Configure appliance General Settings without the Organization component.

Managing user accounts for organizations

Organization user accounts enable users to access the features of the **Administrator Console**, **User Console**, and Service Desk based on their roles assigned to their accounts.

You can use LDAP servers for user authentication, or you can add and edit user accounts manually. See:

- Managing organization user accounts
- Managing System-level user accounts
- Using an LDAP server for user authentication

> **CAUTION: Use caution when changing the password for the default admin account of an organization. Organizations whose admin account passwords differ are not available for fast switching using the drop-down list in the top-right corner of the page.**
>
> **CAUTION: See Enable fast switching for organizations and linked appliances.**

Managing organization filters

Organization filters assign devices to organizations when devices are inventoried.

Organization filters are similar to labels, but they serve a specific purpose: Organization filters automatically assign devices to organizations when devices are inventoried.

There are two types of organization filters:

- **Data Filter**: Assigns devices to organizations automatically based on search criteria. When devices are inventoried, they are assigned to the organization if they meet the criteria. This filter is similar to Smart Labels in that it assigns devices to organizations automatically if they match specified criteria.
- **LDAP Filter**: Assigns devices to organizations automatically based on LDAP or Active Directory interaction. When devices are inventoried, the query runs against the LDAP server. If devices meet the criteria, they are automatically assigned to the organization.

To add or edit organization filters, see:

- Add or edit organization Data Filters
- Add or edit organization LDAP Filters

After you add a filter, you can associate it with an organization on the *Organization Detail* page. See Adding, editing, and deleting organizations.

How organization filters work

Organizations can use multiple filters, but the same filter cannot be assigned to multiple organizations.

Organization filters run according to the following rules:

- When devices are inventoried, one or more filters runs against them. If there are multiple filters, they run according to the **Order** or **Evaluation Order** number in the filter details.
- If devices match the criteria, they are assigned to the organization.
- If devices do not match the criteria, they are assigned to the Default organization. An administrator can then manually move devices from the Default organization to the appropriate organization. See Redirect devices.

Add or edit organization Data Filters

You can add or edit organization Data Filters to automatically assign devices to organizations.

1. Go to the *Organization Filters Detail* page:
    a. Log in to the appliance System Administration Console, `http://`**appliance_hostname**`/system`, or select **System** from the drop-down list in the top-right corner of the page.
    b. On the left navigation bar, click **Organizations**, then click **Filters**.
    c. Display the *Organization Filter* page by doing one of the following:
    # Click the name of a filter.
    # Select **Choose Action** > **New Data Filter**
2. Provide the following information:

Option	Description
Enabled	Whether the filter is enabled. Filters have to be enabled before they can be applied.
Name	The name of the filter. This name appears on the *Organization Filters* list.
Description	A description of the filter.
Order	The run order of the filter. Filters run according to the number specified. Low numbers run before high numbers.

3. In the **Device Filter Criteria** section, select filter criteria:

a. Select a device attribute in the left-most drop-down list in the top row.

For example: IP Address.

TIP: The appliance supports both IPv6 (Internet Protocol version 6) and IPv4 addresses.

b. Select a condition in the second drop-down list.

For example: matches Regex.

c. In the text box, enter a value for the attribute.

For example, to find devices from a specified IP address range, such as the entire subnet 67.18.250.255, use the star sign (*) as a wildcard as follows: 67.18.250.*.

d. **Optional**: To add attributes, select an operator, such as [**and**], in the left-most drop-down list of the second row.

The fields in the row become active.

e. **Optional**: To add rows to the criteria section, click **Add Criteria**.

An additional row appears.

4. Click **Save**.

Add or edit organization LDAP Filters

You can add LDAP Filters to automatically assign devices to organizations using LDAP criteria.

NOTE: If the LDAP server requires credentials for administrative login (that is, non-anonymous login), supply those credentials. If user name and password are not provided, the tree lookup is not performed. Each LDAP Filter might connect to a different LDAP server.

1. Go to the *Organization Filters Detail* page:
   a. Log in to the appliance System Administration Console, `http://`**appliance_hostname**`/system`, or select **System** from the drop-down list in the top-right corner of the page.
   b. On the left navigation bar, click **Organizations**, then click **Filters**.
   c. Display the *Organization Filter Detail* page by doing one of the following:
   # Click the name of a LDAP filter.
   # Select **Choose Action** > **New LDAP Filter**
2. Provide the following information:

Option	Description
Enabled	Whether the filter is enabled. Filters have to be enabled before they can be applied.
Name	The name of the filter. This name appears on the *Organization Filters* list.
Description	A description of the filter.
Evaluation Order	The run order of the filter. Filters run according to the number specified. Low numbers run before high numbers.

3. Specify LDAP criteria:

Option	Description
LDAP Server	The IP address or the hostname of the LDAP server. If the IP address is not valid, the appliance waits to timeout, resulting in login delays during LDAP authentication.

Option	Description
	NOTE: To connect through SSL, use an IP address or hostname. For example: ldaps://hostname.
Port	The LDAP port number, which is usually 389 (LDAP) or 636 (secure LDAP).
Base Dn	The LDAP criteria used to filter the main location for devices. This criteria specifies a location or container in the LDAP or Active Directory structure, and the criteria should include all the devices that you want to identify. Enter the most specific combination of OUs, DCs, or CNs that match your criteria, ranging from left (most specific) to right (most general). For example, this path might lead to the container with devices that you want to identify: `OU=computers,DC=company,DC=com.`
Advanced Search	The search filter. For example: `(&(objectCategory=Computer)(sAMAccountName=KBOX_COMPUTER_NAME))`
LDAP Login	The credentials of the account the appliance uses to log in to the LDAP server to read accounts. For example: `LDAP Login:CN=service_account,CN=Users,DC=company,DC=com.` If no username is provided, an anonymous bind is attempted. Each LDAP Label can connect to a different LDAP or Active Directory server.
LDAP Password	The password of the account the appliance uses to log in to the LDAP server.

During the filter processing, the appliance will replace all KBOX_ defined variables with their respective runtime values.

Currently supported variables for organization device filters:

```
KBOX_COMPUTER_NAME
KBOX_COMPUTER_DESCRIPTION
KBOX_COMPUTER_MAC
KBOX_COMPUTER_IP
KBOX_USER
KBOX_USER_DOMAIN
KBOX_DOMAINUSER
```

Should the external server require credentials for administrative login (aka non-anonymous login) please supply those credentials. If no LDAP user name is given then an anonymous bind will be attempted. Each LDAP filter may connect to a different LDAP/AD server.

NOTE: To test your Filter, replace any KBOX_ variables with real values. Click **Test** and review the results.

4. Click **Save**.

Test organization filters

You can test organization filters to verify that they produce expected results.

1. Go to the Organizations *Devices* list:
    a. Log in to the appliance System Administration Console, `http://`**appliance_hostname**`/system`, or select **System** from the drop-down list in the top-right corner of the page.

b. On the left navigation bar, click **Organizations**, then click **Devices**.

2. Click the **Test Organization Filter** tab above the list on the right side of the page.
3. Select a filter in the **Select a Filter** drop-down list.
4. Click **Test**.

   Test results are displayed. If necessary, you can refilter the devices displayed in the list. See Filter devices.

   NOTE: If you do not see any devices listed in the test results, either no existing devices match the criteria, or the criteria are invalid. To edit the criteria, see Add or edit organization Data Filters.

Delete organization filters

You can delete organization filters provided that they are not associated with an organization.

1. Go to the *Organizations* list:
   a. Log in to the appliance System Administration Console, `http://`**appliance_hostname**`/system`, or select **System** from the drop-down list in the top-right corner of the page.
   b. On the left navigation bar, click **Organizations**, then click **Organizations**.
2. If the filter is associated with an organization:
   a. Click the name of an organization to display the *Organization Detail* page.
   b. In the *Filters* field, click the **x** next to the filter you want to delete.
   c. At the bottom of the page, click **Save**.

      Filters are updated only after you click Save.

   The filter is no longer associated with the organization.
3. Click **Organizations** > **Filters** to display the *Organization Filters* page.
4. To delete a filter, do one of the following:
   - **Select the check box next to one or more filters, then select Choose Action > Delete.**
   - **Click the linked name of a filter, then on the *Organization Filter Detail* page, click Delete.**
5. Click **Yes** to confirm.

Managing devices within organizations

You can search for, filter, and redirect, devices assigned to organizations.

Using Filter for Advanced Search

If you need more granularity than keyword searches provide, you can use Filter. Filter enables you to specify values for each field in the inventory record and search the entire inventory listing for that value.

For example, if you need to know which devices have a particular version of BIOS installed to upgrade only those affected devices, you can search for BIOS information. See Searching at the page level with advanced options.

TIP: You can apply filters to devices displayed in search results.

Filter devices

If you have organization filters, you can filter devices to verify that the filters are being applied correctly.

1. Go to the *Organization Devices* list:

a. Log in to the appliance System Administration Console, `http://`**appliance_hostname**`/system`, or select **System** from the drop-down list in the top-right corner of the page.
b. On the left navigation bar, click **Organizations**, then click **Devices**.

2. Select the check box next to one or more devices.
3. Select **Choose Action** > **Apply Filter**.

   The selected devices are checked against existing filters. If devices were reassigned to organizations, the new organization name appears next to the old organization name in the *Organization* column.

Redirect devices

You can redirect, or manually reassign, devices to organizations as needed.

For example, a device that has been assigned to organization **A** can be manually redirected to organization **B** so that it appears in the organization **B** inventory.

1. Go to the *Organization Devices* list:
   a. Log in to the appliance System Administration Console, `http://`**appliance_hostname**`/system`, or select **System** from the drop-down list in the top-right corner of the page.
   b. On the left navigation bar, click **Organizations**, then click **Devices**.
2. Select the check box next to one or more devices.
3. Select **Choose Action** > **Assign**, then select an organization name to redirect the selected devices to the organization.

Understanding device details

The *Device Details* page in the System-level *Organizations* section provides details about devices that are assigned to organizations.

To access the *Device Details* page in the *Organizations* section, go to the appliance System level and select **Organizations** > **Devices**, then select a device name in the list. For information about device details, see Managing inventory information.

Running single organization and consolidated reports

If the Organization component is enabled on your appliance, and if you have multiple organizations on your appliance, you can run single-organization reports for each organization separately. In addition, you can run consolidated reports that provide information for all organizations in a single report.

For information on report creation, see Creating reports.

Importing and exporting appliance resources

You can transfer resources among organizations on an appliance, and if you have multiple appliances, you can transfer resources among appliances as well.

About importing and exporting resources

Resources, such as Managed Installations and Smart Labels, can be imported and exported among organizations and appliances.

If you have multiple KACE SMAs, you can transfer resources among them using the built-in Samba share directories on the appliances. In addition, if the Organization component is enabled on your appliance, you can transfer resources among organizations. This is useful for resources, such as scripts, that are created for one organization, but that might be useful to other organizations as well.

You can import and export the following resources:

- Notifications
- Managed Installations
- Reports
- Scripts
- Smart Labels
- Software
- Service Desk processes, ticket queues, and ticket rules

Transferring resources among appliances using Samba share directories

You can use Samba share directories as staging areas to transfer resources among appliances.

To do this, export the resources from one appliance, then import them to a different appliance.

Export resources from an appliance

Export resources from an appliance to make those resources available for import to other appliances.

1. Log in to the Administrator Console of the appliance where the resources are located.
2. Enable Samba share file sharing.

   See Enable file sharing at the System level.
3. Go to the *Share Resources* list:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Settings**, then click **Resources**.
   c. On the *Resources Panel*, click **Export**.
4. **Optional**: To filter the list, use the *View By* drop-down list and *Search* field, which appear above the table on the right.

For example, select a resource in the *View By* drop-down list to display only that resource category, or enter a term in the *Search* field to display items that match that term.

5. Select the check box next to one or more resources.
6. Do one of the following:
   - # **Choose Action** > **Export to Local Share**
   - # **Choose Action** > **Export to Network Share**

   NOTE: Select **Export to Network Share** to save the data to a shared location that exists on the network and can be accessed from other devices. **Select Export to Local Share** to save the data to a location on a device that is only accessible from that device.
7. **Optional**: On the *Annotate Exported Resource(s)* page, enter any additional information in the **Note** field.
8. Click **Save**.

   The exported resources first appear on the *Resource Sharing Status* page with a *Status* of *New Request*.

When the export is complete, the *Status* changes to *Completed*. The exported resources are available on the Samba share for import. See Import resources to organizations.

Most import and export tasks take only a moment to complete, but very large resources take more time.

Import resources to an appliance

You can import resources to appliances as needed.

You have exported resources from an appliance. See Transferring resources among appliances using Samba share directories.

1. To view the Samba share location, do one of the following:
   - **If the Organization component is not enabled on your appliance, select Settings > Security Settings.**
   - **If the Organization component is enabled on your appliance, select an organization in the drop-down list in the top-right corner of the page, then select Settings > General Settings.**
2. Using a third-party file copying utility, copy the resources from the **exporting** appliance Samba share to the **importing** appliance Samba share.
3. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
4. On the **importing** appliance, select **Settings** > **Resources** to display the *Resources* panel.
5. Click **Import** to display the *Import Appliance Resources* page, which shows all of the appliance resources available to import.
6. Select **Choose Action** > **Import from Network Share** to display the *Import Resources From SAMBA Directory* page.
7. Select the resources to import, then click **Import**.

   The imported resources first appear on the *Resource Manager Queue* page with a *Status* of *New Request*.

When the import is complete, the *Status* changes to *Completed*. The imported resources are available and listed on their respective tabs, such as *Reporting*.

Most import and export tasks take only a moment to complete, but very large resources take more time.

Transferring resources among organizations

If the Organization component is enabled on your appliance, you can transfer resources among organizations by exporting them from one organization and importing them into other organizations.

Export resources from organizations

Export resources from organizations to make those resources available for import to other organizations.

1. In the top-right corner of the page, select the organization you want to export resources from.
2. Go to the *Export Resources* list:
    a. On the left navigation bar, click **Settings**, then click **Resources**.
    b. On the *Resources Panel*, click **Export**.

    The *Export Resources* page appears, listing all of the organization resources available for export.
3. Select the check box next to one or more resources.
4. Select **Choose Action** > **Export to Local Share** or **Export to Network Share** to display the *Annotate Exported Resource(s)* dialog.
5. **Optional**: Enter any additional information in the *Note* field.
6. Click **Save**.

    The exported resource first appears on the *Resource Manager Queue* page with a *Status* of *New Request*.

When the export is complete, the *Status* changes to *Completed*. The exported resources are available for other organizations on your appliance to import. For instructions, see Import resources to organizations.

Most import and export tasks take only a moment to complete, but very large resources take more time.

Import resources to organizations

You can import resources to organizations as needed.

You have exported resources from an organization. See Transferring resources among organizations.

To import appliance resources from another appliance, follow the instructions in Transferring resources among appliances using Samba share directories.

1. In the drop-down list in the top-right corner of the page, select the organization to which you want to import resources.
2. Go to the *Import Resources* list:
    a. On the left navigation bar, click **Settings**, then click **Resources**.
    b. On the *Resources Panel*, click **Import**.
3. Select the check box next to one or more resources.
4. Select **Choose Action** > **Import from Local Share**.

    The imported resource first appears on the *Resource Sharing Status* page with a *Status* of *New Request*.

When the import is complete, the *Status* changes to *Completed*. The imported resources are available and listed on their respective tabs, such as *Reporting*.

Most import and export tasks take only a moment to complete, but very large resources take more time.

Managing exported resources at the System level

If the Organization component is enabled on the appliance, you can manage exported or shared resources at the System level.

This provides access to resources that have been exported or made available for sharing from any organization on the appliance.

View or delete shared resources

If the Organization component is enabled on your appliance, you can view resources that have been exported from any organization on the appliance.

1. Go to the *Shared Resources* list:
    a. Log in to the appliance System Administration Console, `http://`**appliance_hostname**`/system`, or select **System** from the drop-down list in the top-right corner of the page.
    b. On the left navigation bar, click **Settings**, then click **Resources**.
    c. Click **Shared**.
2. To delete a resource:
    a. Select the check box next to one or more resources.
    b. Select **Choose Action** > **Delete**, then click **Yes** to confirm.

Move shared resources from the local appliance to network locations

If the Organization component is enabled on your appliance, you can move shared resources from the local appliance to a network share.

1. Go to the *Shared Resources* list:
    a. Log in to the appliance System Administration Console, `http://`**appliance_hostname**`/system`, or select **System** from the drop-down list in the top-right corner of the page.
    b. On the left navigation bar, click **Settings**, then click **Resources**.
    c. Click **Shared**.
2. Select **Choose Action** > **Export to Network Share**, then click **Yes** to confirm.

View or delete the status of resource exports

If the Organization component is enabled on your appliance, you can view the status of resources that have been exported from any organization at the System level.

Status information is automatically deleted after 24 hours, but you can delete the status manually as needed.

1. Go to the *Resource Sharing Status* list:
    a. Log in to the appliance System Administration Console, `http://`**appliance_hostname**`/system`, or select **System** from the drop-down list in the top-right corner of the page.
    b. On the left navigation bar, click **Settings**, then click **Resources**.
    c. On the *Resources Panel*, click **Status**.
2. To delete a status:
    a. Select the check box next to a status.
    b. Select **Choose Action** > **Delete**, then click **Yes** to confirm.

Managing inventory

You can use the appliance to manage devices, software, processes, and services in inventory.

Using the Inventory Dashboard

The Inventory Dashboard provides an overview of managed devices for the selected organization (if applicable), or the appliance.

If the Organization component is enabled on the appliance, and you are logged in to the Administrator Console (`http://`**appliance_hostname**`/admin`), the Inventory Dashboard shows information for the selected organization.

You can access the *Inventory Dashboard* if one or more roles associated with your user account grants access to this dashboard. If you want to hide it, edit your user roles, as needed. For more information, see Add or edit User Roles.

TIP: The appliance updates the summary widgets periodically. To update most of the widgets any time, click the icon and then the **Force Refresh** button. To update an individual widget, hover over the widget, then click the **Refresh** button above the widget. Some widgets may require additional steps.

About the Inventory Dashboard widgets

Inventory Dashboard widgets provide overviews of managed devices for the organization or appliance, as selected.

This section describes the widgets available on the *Inventory Dashboard*. If the Organization component is enabled on your appliance, the widgets show the information for the selected organization at the Admin level and for the appliance at the System level.

This dashboard provides a high-level overview of your device usage. Use it to quickly review the state of your devices and look for any indicators that can improve your device inventory. For example, you can focus on the device disk capacity and reassign resources where they are most needed.

Widget	Description
Device Reports	This widget contains links to common inventory reports. Use them to quickly generate a specific report, such as *Devices by memory*, *Devices by OS*, and others.
Connections	This widget shows the number of connections to the appliance web server. A high number indicates a high load on the server, which might reduce appliance response time. If the Organization component is enabled on your appliance, the widget shows the information for the selected organization.
Device Check-In Rate	This widget displays the number of devices that have connected to the appliance in the past 60 minutes. If the Organization component is enabled on your appliance, this widget is available at the System level.
Provisioning	This widget shows the status of KACE Agent provisioning or installation tasks. If the Organization component is enabled on your appliance, the widget shows the information for the selected organization.

Widget	Description
Shortcuts	This widget contains links to common Inventory pages and wizards. Use them to quickly navigate to specific pages, such as the Agent Provisioning Assistant, the *Discovery Schedules* page, and others.
Agent Version Counts	This widget show the counts of agents for each version. This information can be useful during an upgrade.
Inventory Counts	This widget displays the counts of devices associated with each device management method, such as Agent Managed, Agentless, and others. It also shows the number of Agents that have been updated in the last eight hours.
Devices by Disk Capacity	This widget shows a donut chart, where each section of the chart indicates the percentage of free disk space on the managed devices. Clicking the widget title displays a report with links to the associated devices. Hovering over each section of the chart displays the percentage of managed devices that have the selected percentage of free disk space. For example, if you hover over the red part of the chart, the widget displays the percentage of devices whose free disk space is lower than 25%.
Managed Operating Systems	This widget shows the percentage of managed devices that are running each operating system. If the Organization component is enabled on your appliance, this widget shows the percentage of devices in the selected organization.
Provision Platforms	This widget shows the percentage of operating systems installed on Agent-managed devices. If the Organization component is enabled on your appliance, the widget shows the information for the selected organization.
Devices By Manufacturer	This widget shows the top device manufacturers represented in device inventory. If the Organization component is enabled on your appliance, this widget shows the percentage of devices in the selected organization.
Devices By Model	This widget shows the top device models represented in the device inventory. If the Organization component is enabled on your appliance, this widget shows the percentage of devices in the selected organization.
Devices By Memory	This widget shows a bar chart, where each bar represents a number of devices that have an indicated amount of RAM installed on them.
Devices By Processor	This widget shows a bar chart, where each bar represents a number of devices that have a specific processor configuration.
Devices By Subtype	This widget shows a donut chart, where each section of the chart indicates the percentage of the managed devices by device subtype.
VMware Device Counts	This widget shows the counts of each VMware device type, such as vCenters, ESXi hosts, virtual machines, and provisioned virtual machines. Clicking the widget title displays the *Devices* list page.
VMware Device Reports	This widget contains links to five popular VMware inventory reports. Clicking the widget title displays the *Reports* list page with the *Virtual Infrastructure* filter applied.

Widget	Description
VMware ESXi Device By Status	This widget displays a donut chart showing the current status of ESXi devices. There are four possible values: *OK*, *Warning*, *Error* and *Unknown*. Clicking the widget title displays a new VMware inventory report that lists all ESXi devices by current status.
VMware ESXi Version Counts	This widget shows the counts of the top five ESXi versions. Clicking the widget title displays a new VMware inventory report that shows all ESXi devices by version.

Customize the Inventory Dashboard

You can customize the Inventory Dashboard to show or hide widgets as needed.

1. Go to the *Inventory Dashboard*.
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Inventory**, then click **Device**s.
2. Hover over the widget, then use any of the following buttons:
   # : Refresh the information in the widget.
   # : Display information about the widget.
   # : Edit the widget.
   # : Remove the widget.
   # : Resize the widget.
   # : Drag the widget to a different position on the page.
3. The widgets are editable, allowing you to filter the information that they display. To edit a widget, click and in the dialog box that appears, provide the required information. You can edit the chart type. Based on the chart type you select here from the drop down list, the relevant fields populate.
4. Click the button in the top-right corner of the page to view the list of available widgets.

   For information on how to add widgets to the dashboard refer Adding a Widget to Inventory Dashboard

Work with Inventory Dashboard

When you click the icon, the dashboard settings panel displays. You get to see the following options:

Dashboard Name	Description
Dashboard Settings	You can customize the look and feel of the widgets. For more information, refer to Setting an Inventory Dashboard
Add Widget	You can add a new widget. For more information, refer to Adding a Widget to Inventory Dashboard

Email Dashboard	You can share the dashboard through email. For more information, refer to Emailing Inventory Dashboard
Force Refresh	You can refresh all the widget data on the dashboard. For more information, refer to Refreshing Inventory Dashboard Data Manually

Setting an Inventory Dashboard

You can customize the look and feel of the widgets and the dashboards.

You can change the color used in the dashboard charts, edit the dashboard name and its description, change the display of the widgets.

To customize a dashboard,

1. Click the icon to open the Dashboard Settings panel.
2. Make changes to the fields as required:

Fields	Description
Name	Add/Edit name for the dashboard. This is displayed on the dashboard.
Description	Add/Edit description of the dashboard. This describes the dashboard.
Choose Your Colors	Click on the color selector to choose your dashboard chart colors. Drag and drop the colors to arrange them in the desired order. The colors at the top of the list will be used first by each chart.
Layout	Chose one of the layout options. The widgets and other elements are displayed in the selected layout.

3. Click **Save**.

   The changes gets reflected on the dashboard.

Adding a Widget to Inventory Dashboard

You can add widgets to the Dashboard.

There is a list of widgets in the panel. You can enter a keyword in the Search text box to refine the list, then click on your selection.

To add widgets to the dashboard,

1. Click the icon to open the **Add Widget** panel.
2. Search for the desired widget in the following ways:
   - **In the Sort By drop-down, select the widget by title or newest.**
   - **In the Search field, enter a keyword to refine the list.**

   The refined result displays.
3. Click the desired widget.

   The widget gets added to the dashboard.

Emailing Inventory Dashboard

You can share a dashboard snapshot through email, send it to multiple users, and configure the frequency of email.

To email a dashboard,

1. Click the icon to open the dashboard settings panel.
2. Click the Email Dashboard option to open the Email Dashboard panel.
3. Select appropriate option from the given options:
    a. **Send Now**: You can send an email immediately.
    b. **Schedule**: You can set the frequency of sending a snapshot of dashboard through email.

The detailed steps for each option are given below:

Send email now

To send email immediately,

1. Click **Send Now** to open the Email Dashboard dialog.
2. Enter details in the Email Address, Subject, and Message fields.
3. Choose the layout in which you want the widgets to appear.
4. Click Send.

The dashboard is sent through email.

Schedule

To set the frequency of sending a snapshot of dashboard through email,

1. Click **Schedule** to open the Schedule dialog.
2. Enter details in the Subject and **Message** fields.
3. Choose the layout in which you want the widgets to appear.
4. To add recipients, select the names from the **Select user to add drop down list**.

    NOTE: You can add multiple recipients from the list.

5. Select the frequency from the drop down list.
6. In the **Next Run** field that appears after you select the **Frequency**, set the date, month, and time for the next email delivery.
7. Click Save. The dashboard is sent through email according to the set schedule.

Refreshing Inventory Dashboard Data Manually

To update the widgets,

1. Click the icon to open the dashboard settings panel.
2. Click **Force Refresh** to open the Confirm dialog box.
3. Click Yes to confirm refresh all widget data on the dashboard.

Using Device Discovery

Use device Discovery to identify devices that are connected to your network and to retrieve information about those devices.

Use Discovery Results to label devices or add devices to inventory.

About Device Discovery and device management

Devices that can be discovered include laptops, desktops, servers, mobile devices, virtual devices, printers, network devices, wireless access points, routers, switches and more.

These devices can be discovered even if they do not have the KACE Agent installed on them. You can run Discovery scans on-demand or schedule scans to run at specific times.

Discovery Results show the availability and details of devices. After devices are discovered, you can add devices to inventory by:

- **Installing the KACE Agent on devices**. The KACE Agent can be installed on Windows, Mac®, Red Hat®, SUSE®, and Ubuntu® devices. See Provisioning the KACE Agent.
- **Enabling Agentless management for devices**. Agentless management is especially useful for devices that cannot have the KACE Agent installed, such as devices with unsupported operating systems. See Managing Agentless devices.

Tracking changes to Discovery settings

If History subscriptions are configured to retain information, you can view the details of the changes made to settings, assets, and objects.

This information includes the date the change was made and the user who made the change, which can be useful during troubleshooting. See About history settings.

Discovering devices on your network

To discover devices, you can scan your network by creating a Discovery Schedule. The Discovery Schedule specifies the protocols to use during the scan, the IP Address range to be scanned, and the frequency of the scan.

Depending on what you want out of a discovery scan and what devices you are working with, you can choose from various Discovery types.

- **Quick "what and where" Discovery**: See Add a Discovery Schedule to perform a quick "what and where" scan of your network.
- **Thorough Discovery**: You can use this type of discovery to get more device information than what is available from the "what and where" type. See Add a Discovery Schedule for a thorough scan of managed Windows, Mac, Linux, and UNIX computers.
- **External Integration Discovery**: A different type of thorough discovery that is aimed at certain computer devices that are not Windows-, Mac Os X-, or Linux-based. For more information, see:
  - # Add a Discovery Schedule for a KACE Cloud Mobile Device Manager device
  - # Add a Discovery Schedule for a Google Workspace device
  - # Add a Discovery Schedule for an Workspace ONE device
- **Non-computer Discovery**: See Add a Discovery Schedule for SNMP-enabled non-computer devices.

You can scan for devices across a single subnet or multiple subnets. You can also define a scan to search for devices listening on a particular port.

When adding Discovery Schedules, you should balance the scope of the scan (the number of IP addresses you are scanning) with the depth of the probe (the number of attributes you are scanning), so that you do not overwhelm the network or the appliance. For example, if you need to scan a large number of IP addresses frequently, keep the number of ports, TCP/IP connections, and so on, relatively small. As a rule, scan a particular subnet no more than once every few hours.

Add a Discovery Schedule to perform a quick "what and where" scan of your network

Use one of the available schedules to quickly obtain Discovery Results that show the availability of devices.

This type of Discovery scans for any device type in your network: managed computers or non-computer devices.

If you want to add an Nmap Discovery Schedule, there are several issues to consider. See Things to take into consideration with Nmap discovery.

1. Go to the *Discovery Schedule Detail* page:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Inventory**, then click **Discovery Schedules**.
   c. Select **Choose Action** > **New**.
2. Select the *Discovery Type* to display the form with the options for the selected type.

   Depending on the type you select, the following options appear on the right side of the pane :

   # **Ping**. *DNS Lookup* and *Ping* discovery options appear.
   # **Socket**. *DNS Lookup* and *Socket* discovery options appear.
   # **Active Directory**. *DNS Lookup* and *Active Directory* discovery options appear.
   # **External Integration [KACE Cloud Mobile Device Manager, G Suite, Workspace ONE]**. *KACE Cloud Mobile Device Manager*, *G Suite*, and *Workspace ONE* discovery options appear.

   NOTE: Any devices discovered through External Integration such as KACE Mobile Device Manager, G Suite, Workspace ONE devices do not count toward the appliance license limit.

   # **Authenticated [WinRM, SNMP, SSH, VMware, Hyper-V]**. *DNS Lookup*, *Relay*, *WinRM, Hyper-V, VMM*, *SNMP*, *SSH*, and *VMware* discovery options appear.
   # **Nmap**. *DNS Lookup* and *Nmap* discovery options appear.
   # **Custom**. *DNS Lookup*, *Ping*, **Nmap**, *WinRM*, *SNMP*, *SSH*, and *VMware* discovery options appear.
3. In the *Name* field, enter a name for the scan.

   This name appears on the *Discovery Schedules* page.
4. In the *IP Address Range* field, enter an IP address range to scan. Use hyphens to specify individual IP address class ranges. For example, type 192.168.2-5.1-200 to scan for all IP addresses between 192.168.2-5.1 and 192.168.2-5.200, inclusive.

   TIP: The appliance supports both IPv6 (Internet Protocol version 6) and IPv4 addresses.

   CAUTION: A maximum of 25,000 IP addresses is supported. If you specify an IP range that results in more than 25,000 addresses, a warning appears when you attempt to save the provisioning schedule.
5. Select the Discovery Type options. The options that appear depend on the Discovery Type you have chosen:

Option	Item	Description
DNS Lookup		Enable Discovery to identify the name of the device. DNS Lookup is important if you want device names to appear in the Discovery Results and Inventory lists. You can select the DNS Lookup options for each Discovery type.
	Name Server for Lookup	The hostname or IP address of the name server. **TIP:** The appliance supports both IPv6 (Internet Protocol version 6) and IPv4 addresses.
	Timeout	The time, in seconds, after which a DNS lookup expires. If an address is not found during this time, the process “times out.”
Relay		Enable a KACE Agent to act as a tunnel WinRM, SSH and SNMP traffic to the agent connection protocol for WinRM, SSH and SNMP discovery schedules, agentless inventory, and agent provisioning.
	Relay Device	Specify the device that you want to use as a relay for agentless device inventory. A relay device that is used during discovery as a relay is used for agentless inventory, when a new device is provisioned automatically from discovery results. Selected relay devices are listed on the following pages: • On the *Agentless Device Connection Details* page, when a new device is provisioned automatically from discovery results. For more information about this page, see Enable Agentless management by entering device information manually. • On the *Provisioning Schedule Detail* page, when agent provisioning is initiated from discovery results. For more information, see Install the KACE Agent on a device or multiple devices. • On the *Agentless Device Connection Details* page, when a new device is provisioned automatically from discovery results. For more information about this page, see Enable Agentless management by entering device information manually.
Ping		Perform a ping test during the network scan. During this test, the appliance sends a ping test to determine whether a system responds.
Socket		Perform a connection test during the network scan. During this test, the appliance sends a packet to the port to determine whether the port is open.
	TCP Port List	Enable a port scan using TCP (Transmission Control Protocol). Use a comma to separate each port number.
	UDP Port List	Enable a port scan using UDP (User Datagram Protocol). Use a comma to separate each port number.
Active Directory		Enable the appliance to check for device information on an Active Directory server. During Active Directory scans, the status is

Option	Item	Description
		indicated as an approximate percentage instead of the number of devices scanned.
	Use Secure LDAP (LDAPS)	Enable the appliance to use a secure port for LDAP communication.
	Privileged User	The username of the administrator account on the Active Directory server. For example, username@example.com.
	Privileged User Password	The password of the administrator account on the Active Directory server.
	Search Context	The criteria used to search for devices. This criteria specifies a location or container in the Active Directory structure to be searched. Enter the most specific combination of OUs, DCs, or CNs that match your criteria, ranging from left (most specific) to right (most general). For example: DC=company,DC=com
KACE Cloud Mobile Device Manager		This option allows you to access mobile devices such as smart phones and tablets connected to the KACE Cloud Mobile Device Manager (MDM). You must obtain a tenant name and a Secret Key from the KACE Cloud MDM in order to access the devices associated with it.
	Tenant Name	The name of the tenant on the KACE Cloud MDM associated with the devices that you want to manage.
	Credentials	The details of the account that is used to connect to the KACE Cloud MDM device. Select an existing credential from the drop-down list, or select **Add new credential** to add a new credential, as required. For more information, see Add and edit Secret Key credentials.
	Auto Provision Devices	If selected, all mobile devices discovered in the next scan are added to inventory. **NOTE:** Use this option with care, to avoid expanding your inventory to an unexpected extent.
G Suite		Working with G Suite devices requires credentials that grant the appliance access to a Google Apps Domain using the Admin SDK API. You must obtain a Client ID and a Client Secret from Google so that you can get an approval code for the appliance to use.
	Discover Chrome Devices	If selected, any Chrome devices will be discovered in the next scan.
	Discover Mobile Devices	If selected, any G Suite mobile devices will be discovered in the next scan.

Option	Item	Description
	Credentials	The details of the account that is used to connect to the Chrome device. Select an existing credential from the drop-down list, or select **Add new credential** to add a new credential, as required. The selected credential must have an approval code that can be associated with the appropriate device type. For example, if you want to discover G Suite mobile devices, you cannot use a credential whose approval code is generated for Chrome devices. For more information, see Add and edit Google Workspace credentials.
	Auto Provision Devices	If selected, all Chrome and mobile devices discovered in the next scan are added to inventory. **NOTE:** Use this option with care, to avoid expanding your inventory to an unexpected extent.
Workspace ONE		VMware® Workspace ONE® is an enterprise-level mobility management platform that allows you to manage a wide range of different device types.
	Host	The host name of the Workspace ONE administration console.
	REST API Key	The REST API key, available in the Workspace ONE administration console. The key must be provided to enable integration with Workspace ONE through API calls.
	Credentials	The details of the service account required to connect to the device and run commands. Select an existing credential from the drop-down list, or select **Add new credential** to add a new credential, as required. See Add and edit User/Password credentials.
	Auto Provision Devices	If selected, all Workspace ONE devices discovered in the next scan are added to inventory. **NOTE:** Use this option with care, to avoid expanding your inventory to an unexpected extent.
WinRM, Hyper-V, VMM		WinRM is the connection type to use for Windows devices.
	Timeout	The time, in seconds, up to 1 minute, after which the connection is closed if there is no activity.
	Require Kerberos	If selected, Kerberos is required for authentication. NTLM will not be used as an alternative when Kerberos is unavailable. Using Kerberos requires DNS Lookup to be enabled in the same discovery configuration. The DNS Server is also required in the local appliance network settings.
	Scan for Hyper-V and Virtual	If selected, the appliance imports a Microsoft Hyper-V or System Center Virtual Machine Manager infrastructure using agentless management. For more information about this feature, see Add a

Option	Item	Description
	Machine Manager	Discovery Schedule for a Microsoft Hyper-V or System Center Virtual Machine Manager.
	Port	If this field is left blank, the default port 5985 is used.
	Credentials	The details of the service account required to connect to the device and run commands. Select an existing credential from the drop-down list, or select **Add new credential** to add a new credential, as required. See Add and edit User/Password credentials.
SNMP		SNMP (Simple Network Management Protocol) is a protocol for monitoring managed devices on a network.
	SNMP Full Walk	Enable a Full Walk of data in the MIB (management information base) on devices. If this option is cleared, the appliance does a Bulk GET, which searches three core OIDs (object identifiers). When selecting this option, be aware that a Full Walk can take up to 20 minutes per device. The default, Bulk GET, takes approximately one second and acquires all of the information needed for Discovery. **IMPORTANT: SNMP inventory walk does not support non-English characters on Windows devices. If it encounters non-English characters, the SNMP inventory process reports an error and stops loading inventory information.**
	Timeout	The time, in seconds, after which the scan ends if no response is returned.
	Maximum Attempts	The number of times the connection is attempted.
	Credentials(SNMPv1/v2)	The details of the SNMP v1/v2 credentials required to connect to the device and run commands. Select an existing credential from the drop-down list, or select **Add new credential** to add a new credential, as required. See Add and edit SNMP credentials.
	Credentials(SNMPv3)	The details of the SNMP v3 credentials required to connect to the device and run commands. Select an existing credential from the drop-down list, or select **Add new credential** to add a new credential, as required. See Add and edit SNMP credentials.
SSH		Use the SSH protocol with authentication. **IMPORTANT: Discovery though SSH is not supported for Windows devices.** **IMPORTANT: After a Discovery Schedule is saved, you cannot change SSH to SNMP authentication.**

Option	Item	Description
	Timeout	The time, up to 5 minutes, after which the connection is closed if there is no activity.
	Try SSH2 Connection	Enable the SSH2 protocol for connecting to and communicating with devices. Use SSH2 if you want device communications to be more secure (recommended).
	Credentials	The details of the service account required to connect to the device and run commands. Select an existing credential from the drop-down list, or select **Add new credential** to add a new credential, as required. See Add and edit User/Password credentials.
VMware	Timeout	The time after which the scan ends if no response is returned.
	Credentials	The details of the service account required to connect to the device and run commands. Select an existing credential from the drop-down list, or select **Add new credential** to add a new credential, as required. See Add and edit User/Password credentials.
Nmap		**NOTE:** Running more than one of the four Nmap discovery types at a time, although possible, is not recommended. It can extend the length of a run and can cause erratic OS detection results.
	Timeout	The time after which the scan ends if no response is returned.
	Fast Scan	Enable the appliance to quickly scan 100 commonly used ports. If this option is cleared, all available TCP ports are scanned, which can take much longer than the fast scan.
	Nmap Operating System Detection (Best Guess)	Enable the appliance to detect the operating system of the device based on fingerprinting and port information. This option might increase the time required for the scan.
	TCP Port Scan	Enable a port scan using TCP (Transmission Control Protocol) of 1000 commonly used TCP ports. If this option is cleared, and UDP is selected, the appliance performs a UDP scan. If both TCP and UDP are cleared, the appliance uses a TCP scan. If you select this option, Quest recommends that you set the *Timeout* value to 10 minutes to decrease the likelihood of erroneous results. Do not combine this scan with the *Fast Scan* option. Doing so results in only 100 commonly used ports being scanned.
	UDP Port Scan	Enable a port scan using UDP (User Datagram Protocol) of up to 1000 UDP ports. UDP scans are generally less reliable, and have lower processor overhead, than TCP scans because TCP requires a handshake when communicating with devices whereas UDP

Option	Item	Description
		does not. However, UDP scans might take longer than TCP scans, because UDP sends multiple packets to detect ports, whereas TCP sends a single packet. If you select this option, Quest recommends that you set the *Timeout* value to 30 minutes to decrease the likelihood of erroneous results. Do not combine this scan with the *Fast Scan* option. Doing so results in only 100 commonly used ports being scanned. If this option is cleared, the appliance does not scan ports using UDP.

6. **Optional**: Enter an email address for being notified of when the discovery scan completes. The email includes the name of the discovery schedule.
7. Specify the scan schedule:

TIP: To maintain the scan inventory without scanning, set the schedule of the scan configuration to **None**.

Option	Description
None	Run in combination with an event rather than on a specific date or at a specific time.
Every n hours	Run at a specified interval.
Every day/specific day at HH:MM	Run daily at a specified time, or run on a designated day of the week at a specified time.
Run on the nth of every month/ specific month at HH:MM	Run on the same day every month, or a specific month, at the specified time.
Run on the nth weekday of every month/specific month at HH:MM	Run on the specific weekday of every month, or a specific month, at the specified time.

Custom	Run according to a custom schedule.
	Use standard 5-field cron format (extended cron format is not supported):
	`* * * * *`
	`| | | | +----------day of week (0-6)(Sun=0)`
	`| | | +-----------month (1-12)`
	`| | +-----------day of month (1-31)`
	`| +-----------hour (0-23)`
	`+-----------minute (0-59)`

Option	Description
	Use the following when specifying values: • **Spaces ( )**: Separate each field with a space. • **Asterisks (*)**: Include the entire range of values in a field with an asterisk. For example, an asterisk in the hour field indicates every hour. • **Commas (,)**: Separate multiple values in a field with a comma. For example, `0,6` in the day of the week field indicates Sunday and Saturday. • **Hyphens (-)**: Indicate a range of values in a field with a hyphen. For example, `1-5` in the day of the week field is equivalent to `1,2,3,4,5`, which indicates Monday through Friday. • **Slashes (*/*)**: Specify the intervals at which to repeat an action with a slash. For example, `*/3` in the hour field is equivalent to `0,3,6,9,12,15,18,21`. The asterisk (`*`) specifies every hour, but `/3` restricts this to hours divisible by 3. Examples: • `15 * * * * Run 15 minutes after every hour every day` • `0 22 * * * Run at 22:00 every day` • `0 0 1 1,6 * Run at 00:00 on January 1 and June 1` • `30 8,12 * * 1-5 Run weekdays at 08:30 and 12:30` • `0 2 */2 * * Run every other day at 02:00`
View Task Schedule	Click to view the task schedule. The *Task Schedule* dialog box displays a list of scheduled tasks. Click a task to review the task details. For more information, see View task schedules.

8. Click **Save**.

Related topics

About Discovery Results

View and search Discovery Results

Stop a running discovery scan

Delete Discovery Schedules

Things to take into consideration with Nmap discovery

For successful outcomes with Nmap discovery, there are some issues to consider and best practices to adopt to improve speed and accuracy and to avoid problems.

Best practices for improving the speed and accuracy of discovery

To improve the speed and accuracy of Nmap discovery:

- **Avoid using DNS Lookup**. *DNS Lookup* can slow down scan times by up to 500 percent if you specify an invalid or unreachable IP address for the DNS.
- **Run one discovery type at a time**. Although it is possible to run multiple discovery types simultaneously, doing so can extend the length of a run and can cause erratic OS detection results.
- **Select Nmap Operating System Detection (Best Guess) if you are unsure what to run**. This selection can give you a reasonable view into your subnet or subnets. At a minimum, using Best Guess can identify what OSs

are on what devices. If you do not get the expected results, for example if some devices appear with *unknown* as the *Operating System*, try increasing the timeout value and rerunning the discovery.

- **Discovery does not work correctly through a VPN**. Use another source for access to the devices.

Issues that can impede discovery

Be aware that devices that are offline or otherwise inaccessible at the time of a scan are ignored because they appear to be nonexistent.

If you know that there are devices that should be reported, but are not, they are either:

- Being blocked by a firewall
- Actively blocking pings
- Actually offline (no power)
- Thwarting fingerprinting, through various methods.

Some devices, typically security devices, hide themselves from view, or misrepresent themselves to avoid detection.

Troubleshooting unknown operating systems

If the *Operating System* appears as *unknown* in the *Discovery Results* list page:

- Check to see if the Nmap checkmark is present in the *Nmap* column. If not, the device was offline during the scan, and the operating system could not be determined.
- If the Nmap checkmark is present, but the *Operating System* is unknown, the most likely cause is a firewall that is blocking the ports that Nmap is using to determine what OS is running on the device.

  For example, if you scan using only UDP ports 7 and 161, the device appears online with the Nmap checkmark displayed. However, the *Operating System* appears *unknown*, because UDP ports alone are not sufficient to determine what OS is running on the device.

Add a Discovery Schedule for a thorough scan of managed Windows, Mac, Linux, and UNIX computers

To scan your network for devices and capture information about devices, you use Discovery Schedules. After devices are discovered using the Active Directory or Authenticated discovery type, you can add those discovered devices to inventory.

1. Go to the *Discovery Schedule Detail* page:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Inventory**, then click **Discovery Schedules**.
   c. Select **Choose Action** > **New**.
2. Select the *Discovery Type* to display the form with the options for the selected type.

   Depending on the type you select, the following options appear before the *Notify* section:

   # **Active Directory**. *DNS Lookup* and *Active Directory* discovery options appear.
   # **Authenticated [WinRM, SNMP, SSH, VMware, Hyper-V]**. *DNS Lookup*, *Relay*, *WinRM, Hyper-V, VMM*, *SNMP*, *SSH*, and *VMware* discovery options appear.
3. In the *Name* field, enter a name for the scan.

This name appears on the *Discovery Schedules* page.

4. In the *IP Address Range* field, do one of the following:

   - **If you select the *Active Directory* Discovery Type, enter the IP address of the Active Directory server to be scanned.**
   - **Enter an IP address range to scan. Use hyphens to specify individual IP address class ranges.For example, type 192.168.2-5.1-200 to scan for all IP addresses between 192.168.2-5.1 and 192.168.2-5.200, inclusive.**

   TIP: The appliance supports both IPv6 (Internet Protocol version 6) and IPv4 addresses.

   CAUTION: A maximum of 25,000 IP addresses is supported. If you specify an IP range that results in more than 25,000 addresses, a warning appears when you attempt to save the provisioning schedule.

5. Select the Discovery options. The options that appear depend on the Discovery Type you have chosen:

Option	Item	Description
DNS Lookup		Enable Discovery to identify the name of the device. DNS Lookup is important if you want device names to appear in the Discovery Results and Inventory lists. You can select the DNS Lookup options for each Discovery type.
	Name Server for Lookup	The hostname or IP address of the name server. **TIP:** The appliance supports both IPv6 (Internet Protocol version 6) and IPv4 addresses.
	Timeout	The time, in seconds, after which a DNS lookup expires. If an address is not found during this time, the process “times out.”
Relay		Enable a KACE Agent to act as a tunnel WinRM, SSH and SNMP traffic to the agent connection protocol for WinRM, SSH and SNMP discovery schedules, agentless inventory, and agent provisioning.
	Relay Device	Specify the device that you want to use as a relay for agentless device inventory. A relay device that is used during discovery as a relay is used for agentless inventory, when a new device is provisioned automatically from discovery results. Selected relay devices are listed on the following pages: • On the *Agentless Device Connection Details* page, when a new device is provisioned automatically from discovery results. For more information about this page, see Enable Agentless management by entering device information manually. • On the *Provisioning Schedule Detail* page, when agent provisioning is initiated from discovery results. For more information, see Install the KACE Agent on a device or multiple devices. • On the *Agentless Device Connection Details* page, when a new device is provisioned automatically from discovery results. For more information about this page, see Enable Agentless management by entering device information manually.

Option	Item	Description
Active Directory		Enable the appliance to check for device information on an Active Directory server. During Active Directory scans, the status is indicated as an approximate percentage instead of the number of devices scanned.
	Use Secure LDAP (LDAPS)	Enable the appliance to use a secure port for LDAP communication.
	Privileged User	The username of the administrator account on the Active Directory server. For example, username@example.com.
	Privileged User Password	The password of the administrator account on the Active Directory server.
	Search Context	The criteria used to search for devices. This criteria specifies a location or container in the Active Directory structure to be searched. Enter the most specific combination of OUs, DCs, or CNs that match your criteria, ranging from left (most specific) to right (most general). For example: `DC=company,DC=com`.
WinRM, Hyper-V, VMM		WinRM is the connection type to use for Windows devices.
	Timeout	The time, in seconds, up to 1 minute, after which the connection is closed if there is no activity.
	Require Kerberos	If selected, Kerberos is required for authentication. NTLM will not be used as an alternative when Kerberos is unavailable. Using Kerberos requires DNS Lookup to be enabled in the same discovery configuration. The DNS Server is also required in the local appliance network settings.
	Scan for Hyper-V and Virtual Machine Manager	This field is only used if you want to monitor a a Microsoft Hyper-V or System Center Virtual Machine Manager infrastructure. Ensure this option is cleared. For more information about this feature, see Add a Discovery Schedule for a Microsoft Hyper-V or System Center Virtual Machine Manager.
	Port	If this field is left blank, the default port 5985 is used.
	Credentials	The details of the service account required to connect to the device and run commands. Select existing credentials from the drop-down list, or select **Add new credential** to add credentials not already listed. See Add and edit User/Password credentials.
SSH		Use the SSH protocol with authentication. **IMPORTANT: Discovery though SSH is not supported for Windows devices.**

Option	Item	Description
		NOTE: After a Discovery Schedule is saved, you cannot change SSH to SNMP authentication.
	Timeout	The time, up to 5 minutes, after which the connection is closed if there is no activity.
	Try SSH2 Connection	Enable the SSH2 protocol for connecting to and communicating with devices. Use SSH2 if you want device communications to be more secure (recommended).
	Credentials	The details of the service account required to connect to the device and run commands. Select existing credentials from the drop-down list, or select **Add new credential** to add credentials not already listed. See Add and edit User/Password credentials.

6. **Optional**: Enter an email address for being notified of when the discovery scan completes. The email includes the name of the discovery schedule.
7. Specify the scan schedule:

TIP: To maintain the scan inventory without scanning, set the schedule of the scan configuration to **None**.

Option	Description
None	Run in combination with an event rather than on a specific date or at a specific time.
Every n hours	Run at a specified interval.
Every day/specific day at HH:MM	Run daily at a specified time, or run on a designated day of the week at a specified time.
Run on the nth of every month/ specific month at HH:MM	Run on the same day every month, or a specific month, at the specified time.
Run on the nth weekday of every month/specific month at HH:MM	Run on the specific weekday of every month, or a specific month, at the specified time.

Custom	Run according to a custom schedule.
	Use standard 5-field cron format (extended cron format is not supported):
	`* * * * *`
	`| | | | +----------day of week (0-6)(Sun=0)`
	`| | | +----------month (1-12)`
	`| | +----------day of month (1-31)`
	`| +----------hour (0-23)`
	`+----------minute (0-59)`

Option	Description
	Use the following when specifying values: • **Spaces ( )**: Separate each field with a space. • **Asterisks (*)**: Include the entire range of values in a field with an asterisk. For example, an asterisk in the hour field indicates every hour. • **Commas (,)**: Separate multiple values in a field with a comma. For example, `0,6` in the day of the week field indicates Sunday and Saturday. • **Hyphens (-)**: Indicate a range of values in a field with a hyphen. For example, `1-5` in the day of the week field is equivalent to `1,2,3,4,5`, which indicates Monday through Friday. • **Slashes (*/*)**: Specify the intervals at which to repeat an action with a slash. For example, `*/3` in the hour field is equivalent to `0,3,6,9,12,15,18,21`. The asterisk (`*`) specifies every hour, but `/3` restricts this to hours divisible by 3. Examples: • `15 * * * * Run 15 minutes after every hour every day` • `0 22 * * * Run at 22:00 every day` • `0 0 1 1,6 * Run at 00:00 on January 1 and June 1` • `30 8,12 * * 1-5 Run weekdays at 08:30 and 12:30` • `0 2 */2 * * Run every other day at 02:00`
View Task Schedule	Click to view the task schedule. The *Task Schedule* dialog box displays a list of scheduled tasks. Click a task to review the task details. For more information, see View task schedules.

8. Click **Save**.

Related topics

About Discovery Results

View and search Discovery Results

Stop a running discovery scan

Delete Discovery Schedules

Obtain a Client ID and Client Secret for use in discovering Chrome devices

Working with Chrome devices requires credentials that grant the appliance access to a Google Apps Domain using the Admin SDK API. You must obtain a Client ID and a Client Secret from Google so that you can get an approval code for the appliance to use.

- You have a Google Apps for Business domain or Google Apps for Education domain, with Chrome Device Management support.
- You have a Google User admin account that is a member of the business or education domain. The account must be assigned the super user role.
- You have a Google account that can be used as your developer account in this procedure. This account does not have to be the same as the admin account, nor does it have to be a member of the business or education domain.

The appliance is enabled to import device information about devices and users from a Google Apps Domain when the appliance has access to the Admin SDK API. Part of the credentialing process requires setting up a Google project, enabling the Admin SDK API from within it, and creating a Client ID and Client Secret.

1. Sign in to your developer account at https://console.developers.google.com/.
2. Create a project.
    a. Click **Projects** in the left navigation bar.
    b. Click **Create Project** to display the *New Project* dialog.
    c. Type a project name
    d. Use the auto-generated *Project ID* or type a unique ID of your choice.
    e. Click **Create**.

    The *Project Dashboard* for the new project appears.
3. Enable the Admin SDK API.
    a. Click **APIs & auth** in the left navigation bar to expand the section, and click **APIs**.
    b. Find *Admin SDK* under *Browse APIs*, and click the **OFF** *Status* button on the far right of the line to toggle the status to **ON** and enable the API.
    c. Read and agree to the terms of service and click **Accept**.
4. Create an OAuth Client ID and Client Secret.

    NOTE: Quest recommends that you create a separate Client ID for each appliance that is configured to discover Chrome devices.

    a. In the **APIs & auth** section of the left navigation bar, click **Credentials**.
    b. In the *OAuth* section, click **Create new Client ID** to display the *Create Client ID* dialog.
    c. Click **Configure consent screen** to display the *Consent screen* dialog.
    d. Select your email from the *EMAIL ADDRESS* drop-down list, type the name of your product in *PRODUCT NAME*, and click **Save** to return to the *Create Client ID* dialog.
    e. Select **Installed application**.
    f. Select **Other** as the *Installed Application Type*, and click **Create Client ID**.

    The *Credentials* page displays the created *Client ID* and *Client Secret*.

    g. Make note of the Client ID and Client Secret values.

    The values are needed when you configure authorization credentials in the appliance for Chrome device discovery.

Add a Third Party Discovery Schedule to scan your network for G Suite devices and capture information about those devices. See Add a Discovery Schedule for a Google Workspace device.

Add a Discovery Schedule for a KACE Cloud Mobile Device Manager device

If you use the KACE Cloud Mobile Device Manager (MDM) to manage access to smart phones and tablets, you can discover managed mobile devices using discovery scheduling. To scan your network for KACE Cloud MDM devices and capture information about those devices, add an External Integration Discovery Schedule.

NOTE: Any KACE Cloud MDM devices discovered using this method do not count toward the appliance license limit.

1. Go to the *Discovery Schedule Detail* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Inventory**, then click **Discovery Schedules**.

c. Select **Choose Action** > **New**.

2. Select the *Discovery Type* to display the form with the options for the selected type, in this case *External Integration [KACE Cloud Mobile Device Manager, G Suite, Workspace ONE]*.
3. In the *Name* field, enter a name for the scan.

   This name appears on the *Discovery Schedules* page.
4. Expand *KACE Cloud Mobile Device Manager* and select the Discovery options.

Option	Description
Tenant Name	The name of the tenant on the KACE Cloud MDM associated with the devices that you want to manage.
Credentials	The details of the account that is used to connect to the KACE Cloud MDM device. Select an existing credential from the drop-down list, or select **Add new credential** to add a new credential, as required. For more information, see Add and edit Secret Key credentials.
Auto Provision Devices	If selected, all mobile devices discovered in the next scan are added to inventory. **NOTE:** Use this option with care, to avoid expanding your inventory to an unexpected extent.

5. **Optional**: In the *Notify* section, enter an email address for being notified of when the discovery scan completes. The email includes the name of the discovery schedule.
6. Specify the scan schedule:

   TIP: To maintain the scan inventory without scanning, set the schedule of the scan configuration to **None**.

Option	Description
None	Run in combination with an event rather than on a specific date or at a specific time.
Every n hours	Run at a specified interval.
Every day/specific day at HH:MM	Run daily at a specified time, or run on a designated day of the week at a specified time.
Run on the nth of every month/ specific month at HH:MM	Run on the same day every month, or a specific month, at the specified time.
Run on the nth weekday of every month/specific month at HH:MM	Run on the specific weekday of every month, or a specific month, at the specified time.

Custom	Run according to a custom schedule.
	Use standard 5-field cron format (extended cron format is not supported):
	`* * * * *`
	`| | | | +————————day of week (0-6)(Sun=0)`
	`| | | +————————month (1-12)`
	`| | +————————day of month (1-31)`
	`| +————————hour (0-23)`
	`+————————minute (0-59)`

Option	Description
	Use the following when specifying values: • **Spaces ( )**: Separate each field with a space. • **Asterisks (*)**: Include the entire range of values in a field with an asterisk. For example, an asterisk in the hour field indicates every hour. • **Commas (,)**: Separate multiple values in a field with a comma. For example, `0,6` in the day of the week field indicates Sunday and Saturday. • **Hyphens (-)**: Indicate a range of values in a field with a hyphen. For example, `1-5` in the day of the week field is equivalent to `1,2,3,4,5`, which indicates Monday through Friday. • **Slashes (*/*)**: Specify the intervals at which to repeat an action with a slash. For example, `*/3` in the hour field is equivalent to `0,3,6,9,12,15,18,21`. The asterisk (`*`) specifies every hour, but `/3` restricts this to hours divisible by 3. Examples: • `15 * * * * Run 15 minutes after every hour every day` • `0 22 * * * Run at 22:00 every day` • `0 0 1 1,6 * Run at 00:00 on January 1 and June 1` • `30 8,12 * * 1-5 Run weekdays at 08:30 and 12:30` • `0 2 */2 * * Run every other day at 02:00`
View Task Schedule	Click to view the task schedule. The *Task Schedule* dialog box displays a list of scheduled tasks. Click a task to review the task details. For more information, see View task schedules.

7. Click **Save**.

Related topics

About Discovery Results

View and search Discovery Results

Stop a running discovery scan

Delete Discovery Schedules

Add a Discovery Schedule for a Google Workspace device

To scan your network for Google Workspace devices and capture information about those devices, add an External Integration Schedule.

- You have a Google Apps for Business domain or Google Apps for Education domain, with Chrome Device Management support.
- You have a Google User admin account that is a member of the business or education domain. The account must be assigned the super user role.
- You have a Google account to be used as your developer account, and have created a project with a Client ID and Client Secret. See Obtain a Client ID and Client Secret for use in discovering Chrome devices.

NOTE: Any Google Workspace devices discovered using this method do not count toward the appliance license limit.

1. Go to the *Discovery Schedule Detail* page:

a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
b. On the left navigation bar, click **Inventory**, then click **Discovery Schedules**.
c. Select **Choose Action** > **New**.

2. Select the *Discovery Type* to display the form with the options for the selected type, in this case *External Integration [KACE Cloud Mobile Device Manager, Google Workspace, Workspace ONE]*.
3. In the *Name* field, enter a name for the scan.

   This name appears on the *Discovery Schedules* page.
4. Expand *Google Workspace* and select the Discovery options.

Option	Description
Discover Chrome Devices	If selected, any Chrome devices will be discovered in the next scan.
Discover Mobile Devices	If selected, any Google Workspace mobile devices will be discovered in the next scan.
Credentials	The details of the account that is used to connect to the Chrome device. Select existing credentials from the drop-down list, or select **Add new credential** to add credentials not already listed. **IMPORTANT: The selected credential must have an approval code that can be associated with the appropriate device type. For example, if you want to discover G Suite mobile devices, you cannot use a credential whose approval code is generated for Chrome devices.** For more information, see Add and edit Google Workspace credentials.
Auto Provision Devices	If selected, all Chrome devices discovered in the next scan are added to inventory. **NOTE:** Use this option with care, to avoid expanding your inventory to an unexpected extent.

5. **Optional**: In the *Notify* section, enter an email address for being notified of when the discovery scan completes. The email includes the name of the discovery schedule.
6. Specify the scan schedule:

   TIP: To maintain the scan inventory without scanning, set the schedule of the scan configuration to **None**.

Option	Description
None	Run in combination with an event rather than on a specific date or at a specific time.
Every n hours	Run at a specified interval.
Every day/specific day at HH:MM	Run daily at a specified time, or run on a designated day of the week at a specified time.
Run on the nth of every month/ specific month at HH:MM	Run on the same day every month, or a specific month, at the specified time.

Option	Description
Run on the nth weekday of every month/specific month at HH:MM	Run on the specific weekday of every month, or a specific month, at the specified time.

Custom	Run according to a custom schedule.
	Use standard 5-field cron format (extended cron format is not supported):
	`* * * * *`
	`| | | | +----------day of week (0-6)(Sun=0)`
	`| | | +-----------month (1-12)`
	`| | +-----------day of month (1-31)`
	`| +-----------hour (0-23)`
	`+-----------minute (0-59)`
	Use the following when specifying values:
	• **Spaces ( )**: Separate each field with a space.
	• **Asterisks (*)**: Include the entire range of values in a field with an asterisk. For example, an asterisk in the hour field indicates every hour.
	• **Commas (,)**: Separate multiple values in a field with a comma. For example, `0,6` in the day of the week field indicates Sunday and Saturday.
	• **Hyphens (-)**: Indicate a range of values in a field with a hyphen. For example, `1-5` in the day of the week field is equivalent to `1,2,3,4,5`, which indicates Monday through Friday.
	• **Slashes (/)**: Specify the intervals at which to repeat an action with a slash. For example, `*/3` in the hour field is equivalent to `0,3,6,9,12,15,18,21`. The asterisk (`*`) specifies every hour, but `/3` restricts this to hours divisible by 3.
	Examples:
	• `15 * * * * Run 15 minutes after every hour every day`
	• `0 22 * * * Run at 22:00 every day`
	• `0 0 1 1,6 * Run at 00:00 on January 1 and June 1`
	• `30 8,12 * * 1-5 Run weekdays at 08:30 and 12:30`
	• `0 2 */2 * * Run every other day at 02:00`

View Task Schedule	Click to view the task schedule. The *Task Schedule* dialog box displays a list of scheduled tasks. Click a task to review the task details. For more information, see View task schedules.

7. Click **Save**.

Related topics

About Discovery Results

View and search Discovery Results

Stop a running discovery scan

Delete Discovery Schedules

Add a Discovery Schedule for an Workspace ONE device

VMware® Workspace ONE® is an enterprise-level mobility management platform that allows you to manage a wide range of different device types. You can integrate with Workspace ONE to collect discover devices managed with Workspace ONE using REST API calls.

NOTE: Any Workspace ONE devices discovered using this method do not count toward the appliance license limit.

1. Go to the *Discovery Schedule Detail* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Inventory**, then click **Discovery Schedules**.
    c. Select **Choose Action** > **New**.
2. Select the *Discovery Type* to display the form with the options for the selected type, in this case *External Integration [KACE Cloud Mobile Device Manager, G Suite, Workspace ONE]*.
3. In the *Name* field, enter a name for the scan.

    This name appears on the *Discovery Schedules* page.
4. Expand *Workspace ONE* and select the Discovery options.

Option	Description
Host	The host name of the Workspace ONE administration console.
REST API Key	The REST API key, available in the Workspace ONE administration console. The key must be provided to enable integration with Workspace ONE through API calls.
Credentials	The details of the service account required to connect to the device and run commands. Select existing credentials from the drop-down list, or select **Add new credential** to add credentials not already listed. See Add and edit User/Password credentials.
Auto Provision Devices	If selected, all Workspace ONE devices discovered in the next scan are added to inventory. **NOTE:** Use this option with care, to avoid expanding your inventory to an unexpected extent.

5. **Optional**: In the *Notify* section, enter an email address for being notified of when the discovery scan completes. The email includes the name of the discovery schedule.
6. Specify the scan schedule:

    TIP: To maintain the scan inventory without scanning, set the schedule of the scan configuration to **None**.

Option	Description
None	Run in combination with an event rather than on a specific date or at a specific time.
Every n hours	Run at a specified interval.
Every day/specific day at HH:MM	Run daily at a specified time, or run on a designated day of the week at a specified time.

Option	Description
Run on the nth of every month/ specific month at HH:MM	Run on the same day every month, or a specific month, at the specified time.
Run on the nth weekday of every month/specific month at HH:MM	Run on the specific weekday of every month, or a specific month, at the specified time.

Custom	Run according to a custom schedule.
	Use standard 5-field cron format (extended cron format is not supported):
	`* * * * *`
	`| | | | +----------day of week (0-6)(Sun=0)`
	`| | | +----------month (1-12)`
	`| | +----------day of month (1-31)`
	`| +----------hour (0-23)`
	`+----------minute (0-59)`
	Use the following when specifying values:
	• **Spaces ( )**: Separate each field with a space.
	• **Asterisks (*)**: Include the entire range of values in a field with an asterisk. For example, an asterisk in the hour field indicates every hour.
	• **Commas (,)**: Separate multiple values in a field with a comma. For example, `0,6` in the day of the week field indicates Sunday and Saturday.
	• **Hyphens (-)**: Indicate a range of values in a field with a hyphen. For example, `1-5` in the day of the week field is equivalent to `1,2,3,4,5`, which indicates Monday through Friday.
	• **Slashes (/)**: Specify the intervals at which to repeat an action with a slash. For example, `*/3` in the hour field is equivalent to `0,3,6,9,12,15,18,21`. The asterisk (`*`) specifies every hour, but `/3` restricts this to hours divisible by 3.
	Examples:
	• `15 * * * * Run 15 minutes after every hour every day`
	• `0 22 * * * Run at 22:00 every day`
	• `0 0 1 1,6 * Run at 00:00 on January 1 and June 1`
	• `30 8,12 * * 1-5 Run weekdays at 08:30 and 12:30`
	• `0 2 */2 * * Run every other day at 02:00`

View Task Schedule	Click to view the task schedule. The *Task Schedule* dialog box displays a list of scheduled tasks. Click a task to review the task details. For more information, see View task schedules.

7. Click **Save**.

Related topics

About Discovery Results

View and search Discovery Results

Stop a running discovery scan

Delete Discovery Schedules

Add a Discovery Schedule for a VMware ESXi host or a vCenter Server

If your business uses a virtual VMware-based environment, you can discover VMware ESXi hosts or vCenter Servers using discovery scheduling. To scan your network for VMware ESXi hosts or vCenter Servers and capture information about those devices, add an Authenticated Discovery Schedule.

A provisioned VMware ESXi host consumes an Agent-based license. Virtual machines associated with that host do not consume any licenses. The vCenter in which the ESXi host is running does not consume a license. It acts as a bridge to connect to provisioned ESXi hosts.

1. Go to the *Discovery Schedule Detail* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Inventory**, then click **Discovery Schedules**.
    c. Select **Choose Action** > **New**.
2. Select the *Discovery Type* to display the form with the options for the selected type, in this case *Authenticated [WinRM, SNMP, SSH, VMware, Hyper-V]*.
3. In the *Name* field, enter a name for the scan.

    This name appears on the *Discovery Schedules* page.
4. Expand the *VMware* section and configure the Discovery options.

Option	Description
Timeout	The time after which the scan ends if no response is returned.
Credentials	The details of the service account required to connect to the device and run commands. Select existing credentials from the drop-down list, or select **Add new credential** to add credentials not already listed. See Add and edit User/Password credentials.

5. **Optional**: In the *Notify* section, enter an email address for being notified of when the discovery scan completes. The email includes the name of the discovery schedule.
6. Specify the scan schedule:

    TIP: To maintain the scan inventory without scanning, set the schedule of the scan configuration to **None**.

Option	Description
None	Run in combination with an event rather than on a specific date or at a specific time.
Every n hours	Run at a specified interval.
Every day/specific day at HH:MM	Run daily at a specified time, or run on a designated day of the week at a specified time.
Run on the nth of every month/ specific month at HH:MM	Run on the same day every month, or a specific month, at the specified time.

Option	Description
Run on the nth weekday of every month/specific month at HH:MM	Run on the specific weekday of every month, or a specific month, at the specified time.

Custom	Run according to a custom schedule.
	Use standard 5-field cron format (extended cron format is not supported):
	`* * * * *`
	`| | | | +----------day of week (0-6)(Sun=0)`
	`| | | +----------month (1-12)`
	`| | +----------day of month (1-31)`
	`| +----------hour (0-23)`
	`+----------minute (0-59)`
	Use the following when specifying values:
	• **Spaces ( )**: Separate each field with a space.
	• **Asterisks (*)**: Include the entire range of values in a field with an asterisk. For example, an asterisk in the hour field indicates every hour.
	• **Commas (,)**: Separate multiple values in a field with a comma. For example, `0,6` in the day of the week field indicates Sunday and Saturday.
	• **Hyphens (-)**: Indicate a range of values in a field with a hyphen. For example, `1-5` in the day of the week field is equivalent to `1,2,3,4,5`, which indicates Monday through Friday.
	• **Slashes (/)**: Specify the intervals at which to repeat an action with a slash. For example, `*/3` in the hour field is equivalent to `0,3,6,9,12,15,18,21`. The asterisk (`*`) specifies every hour, but `/3` restricts this to hours divisible by 3.
	Examples:
	• `15 * * * * Run 15 minutes after every hour every day`
	• `0 22 * * * Run at 22:00 every day`
	• `0 0 1 1,6 * Run at 00:00 on January 1 and June 1`
	• `30 8,12 * * 1-5 Run weekdays at 08:30 and 12:30`
	• `0 2 */2 * * Run every other day at 02:00`

View Task Schedule	Click to view the task schedule. The *Task Schedule* dialog box displays a list of scheduled tasks. Click a task to review the task details. For more information, see View task schedules.

7. Click **Save**.

Related topics

About Discovery Results

View and search Discovery Results

Stop a running discovery scan

Delete Discovery Schedules

Add a Discovery Schedule for a Microsoft Hyper-V or System Center Virtual Machine Manager

If your business uses a virtual Hyper-V-based environment, you can discover Microsoft Hyper-V or System Center Virtual Machine Manager (SCVMM) devices using discovery scheduling. To scan your network for Hyper-V or SCVMM devices, and to capture information about those devices, add an Authenticated Discovery Schedule.

The devices imported into the appliance using this method do not consume any licenses. Each SCVMM and Hyper-V device consumes only an agentless license used to inventory the underlying Windows systems. SCVMM and Hyper-V devices that are also provisioned with the KACE Agent each consume two licenses.

1. Go to the *Discovery Schedule Detail* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Inventory**, then click **Discovery Schedules**.
    c. Select **Choose Action** > **New**.
2. Select the *Discovery Type* to display the form with the options for the selected type, in this case *Authenticated [WinRM, SNMP, SSH, VMware, Hyper-V]*.
3. In the *Name* field, enter a name for the scan.

    This name appears on the *Discovery Schedules* page.
4. Expand the *WinRM, Hyper-V, VMM* section and configure the Discovery options.

Option	Description
Timeout	The time, in seconds, up to 1 minute, after which the connection is closed if there is no activity.
Require Kerberos	If selected, Kerberos is required for authentication. NTLM will not be used as an alternative when Kerberos is unavailable. Using Kerberos requires DNS Lookup to be enabled in the same discovery configuration. The DNS Server is also required in the local appliance network settings.
Scan for Hyper-V and Virtual Machine Manager	Select this option to allow the appliance to import a Microsoft Hyper-V or System Center Virtual Machine Manager infrastructure using agentless management. For more information about this feature, see Add a Discovery Schedule for a Microsoft Hyper-V or System Center Virtual Machine Manager.
Port	If this field is left blank, the default port 5985 is used.
Credentials	The details of the service account required to connect to the device and run commands. Select an existing credential from the drop-down list, or select **Add new credential** to add a new credential, as required. See Add and edit User/Password credentials. **NOTE:** The same credentials specified for a SCVMM device are used to connect to each managed Hyper-V device. For more information, see System Center Virtual Machine Manager Credential Requirements.

5. **Optional**: In the *Notify* section, enter an email address for being notified of when the discovery scan completes. The email includes the name of the discovery schedule.
6. Specify the scan schedule:

TIP: To maintain the scan inventory without scanning, set the schedule of the scan configuration to **None**.

Option	Description
None	Run in combination with an event rather than on a specific date or at a specific time.
Every n hours	Run at a specified interval.
Every day/specific day at HH:MM	Run daily at a specified time, or run on a designated day of the week at a specified time.
Run on the nth of every month/ specific month at HH:MM	Run on the same day every month, or a specific month, at the specified time.
Run on the nth weekday of every month/specific month at HH:MM	Run on the specific weekday of every month, or a specific month, at the specified time.

Custom	Run according to a custom schedule.
	Use standard 5-field cron format (extended cron format is not supported):
	`* * * * *`
	`| | | | +————————day of week (0-6)(Sun=0)`
	`| | | +————————month (1-12)`
	`| | +————————day of month (1-31)`
	`| +————————hour (0-23)`
	`+————————minute (0-59)`
	Use the following when specifying values:
	• **Spaces ( )**: Separate each field with a space.
	• **Asterisks (*)**: Include the entire range of values in a field with an asterisk. For example, an asterisk in the hour field indicates every hour.
	• **Commas (,)**: Separate multiple values in a field with a comma. For example, `0,6` in the day of the week field indicates Sunday and Saturday.
	• **Hyphens (-)**: Indicate a range of values in a field with a hyphen. For example, `1-5` in the day of the week field is equivalent to `1,2,3,4,5`, which indicates Monday through Friday.
	• **Slashes (/)**: Specify the intervals at which to repeat an action with a slash. For example, `*/3` in the hour field is equivalent to `0,3,6,9,12,15,18,21`. The asterisk (`*`) specifies every hour, but `/3` restricts this to hours divisible by 3.
	Examples:
	• `15 * * * * Run 15 minutes after every hour every day`
	• `0 22 * * * Run at 22:00 every day`
	• `0 0 1 1,6 * Run at 00:00 on January 1 and June 1`
	• `30 8,12 * * 1-5 Run weekdays at 08:30 and 12:30`
	• `0 2 */2 * * Run every other day at 02:00`

Option	Description
View Task Schedule	Click to view the task schedule. The *Task Schedule* dialog box displays a list of scheduled tasks. Click a task to review the task details. For more information, see View task schedules.

7. Click **Save**.

Related topics

About Discovery Results

View and search Discovery Results

Stop a running discovery scan

Delete Discovery Schedules

System Center Virtual Machine Manager Credential Requirements

The credentials used to inventory a System Center Virtual Machine Manager (SCVMM) device and all of its managed Hyper-V devices have specific requirements.

- The domain account must be a member of the SCVMM **Read-Only Administrator** profile or a profile with the same/greater privileges.
- The domain account must be a member of the local **Hyper-V Administrators** group on each Hyper-V device.
- The domain account must have permissions to perform Windows agentless inventory using WinRM on the SCVMM and Hyper-V devices.

Add a Discovery Schedule for SNMP-enabled non-computer devices

To scan your network for non-computer devices and capture information about those devices, you can add an Authenticated —SNMP Discovery Schedule.

To enable SNMP, port 161 must be open on the appliance and on the device.

SNMP (Simple Network Management Protocol) is a protocol for monitoring managed devices on a network. SNMP v3 uses authentication and encryption algorithms to increase the security of SNMP communications. When you configure the SNMP v3 options, the appliance performs an SNMP v3 scan on selected devices. If that scan fails, the appliance attempts an SNMP v2 or v1 scan using the specified Public String.

SNMP scan results include all SNMP-capable devices. Remote shell extensions enable the appliance to connect to devices, run commands, and capture Discovery information.

NOTE: After a Discovery Schedule is saved, you cannot change SNMP to SSH authentication.

1. Go to the *Discovery Schedule Detail* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Inventory**, then click **Discovery Schedules**.
    c. Select **Choose Action** > **New**.
2. Select the *Discovery Type* to display the form with the options for the selected type, in this case *Authenticated [WinRM, SNMP, SSH, VMware, Hyper-V]*.

The following options appear before the *Notify* section:

- *DNS Lookup*
- *Relay*
- *WinRM, Hyper-V, VMM*
- *SSH*
- *SNMP*

For this procedure only *DNS Lookup* and *SNMP* are pertinent

3. In the *Name* field, enter a name for the scan.

   This name appears on the *Discovery Schedules* page.

4. In the *IP Address Range* field, enter an IP address range to scan. Use hyphens to specify individual IP address class ranges. For example, type 192.168.2-5.1-200 to scan for all IP addresses between 192.168.2-5.1 and 192.168.2-5.200, inclusive.

   TIP: The appliance supports both IPv6 (Internet Protocol version 6) and IPv4 addresses.

   CAUTION: A maximum of 25,000 IP addresses is supported. If you specify an IP range that results in more than 25,000 addresses, a warning appears when you attempt to save the provisioning schedule.

5. Expand *DNS Lookup* and select the Discovery options.

   Including DNS Lookup enables Discovery to identify the name of the device. DNS Lookup is important if you want device names to appear in the Discovery Results and Inventory lists.

Option	Description
Name Server for Lookup	The hostname or IP address of the name server. **TIP:** The appliance supports both IPv6 (Internet Protocol version 6) and IPv4 addresses.
Timeout	The time, in seconds, after which a DNS lookup expires. If an address is not found during this time, the process “times out.”

6. Expand *Relay* and select the Discovery options.

   Configuring the *Relay* options allows yout to configure a KACE Agent to act as a tunnel WinRM, SSH and SNMP traffic to the agent connection protocol for WinRM, SSH and SNMP discovery schedules, agentless inventory, and agent provisioning.

Option	Description
Relay Device	Specify the device that you want to use as a relay for agentless device inventory. A relay device that is used during discovery as a relay is used for agentless inventory, when a new device is provisioned automatically from discovery results.

Option	Description
	Selected relay devices are listed on the following pages: • On the *Agentless Device Connection Details* page, when a new device is provisioned automatically from discovery results. For more information about this page, see Enable Agentless management by entering device information manually. • On the *Provisioning Schedule Detail* page, when agent provisioning is initiated from discovery results. For more information, see Install the KACE Agent on a device or multiple devices. • On the *Agentless Device Connection Details* page, when a new device is provisioned automatically from discovery results. For more information about this page, see Enable Agentless management by entering device information manually.

7. Expand *SNMP* and select the Discovery options.

Option	Description
SNMP Full Walk	Enable a Full Walk of data in the MIB (management information base) on devices. If this option is cleared, the appliance does a Bulk GET, which searches three core OIDs (object identifiers). When selecting this option, be aware that a Full Walk can take up to 20 minutes per device. The default, Bulk GET, takes approximately one second and acquires all of the information needed for Discovery. **NOTE:** SNMP inventory walk does not support non-English characters on Windows devices. If it encounters non-English characters, the SNMP inventory process reports an error and stops loading inventory information.
Timeout	The time, in seconds, after which the scan ends if no response is returned.
Maximum Attempts	The number of times the connection is attempted.
Credentials (SNMPv1/v2)	The details of the SNMP v1/v2 credentials required to connect to the device and run commands. Select existing credentials from the drop-down list, or select **Add new credential** to add credentials not already listed. See Add and edit SNMP credentials.
Credentials (SNMPv3)	The details of the SNMP v3 credentials required to connect to the device and run commands. Select existing credentials from the drop-down list, or select **Add new credential** to add credentials not already listed. See Add and edit SNMP credentials.

8. **Optional**: In the *Notify* section, enter an email address for being notified of when the discovery scan completes. The email includes the name of the discovery schedule.
9. Specify the scan schedule:

TIP: To maintain the scan inventory without scanning, set the schedule of the scan configuration to **None**.

Option	Description
None	Run in combination with an event rather than on a specific date or at a specific time.
Every n hours	Run at a specified interval.

Option	Description
Every day/specific day at HH:MM	Run daily at a specified time, or run on a designated day of the week at a specified time.
Run on the nth of every month/ specific month at HH:MM	Run on the same day every month, or a specific month, at the specified time.
Run on the nth weekday of every month/specific month at HH:MM	Run on the specific weekday of every month, or a specific month, at the specified time.

Custom	Run according to a custom schedule.
	Use standard 5-field cron format (extended cron format is not supported):
	`* * * * *`
	`| | | | +----------day of week (0-6)(Sun=0)`
	`| | | +----------month (1-12)`
	`| | +----------day of month (1-31)`
	`| +----------hour (0-23)`
	`+----------minute (0-59)`
	Use the following when specifying values:
	• **Spaces ( )**: Separate each field with a space.
	• **Asterisks (*)**: Include the entire range of values in a field with an asterisk. For example, an asterisk in the hour field indicates every hour.
	• **Commas (,)**: Separate multiple values in a field with a comma. For example, `0,6` in the day of the week field indicates Sunday and Saturday.
	• **Hyphens (-)**: Indicate a range of values in a field with a hyphen. For example, `1-5` in the day of the week field is equivalent to `1,2,3,4,5`, which indicates Monday through Friday.
	• **Slashes (/)**: Specify the intervals at which to repeat an action with a slash. For example, `*/3` in the hour field is equivalent to `0,3,6,9,12,15,18,21`. The asterisk (`*`) specifies every hour, but `/3` restricts this to hours divisible by 3.
	Examples:
	• `15 * * * * Run 15 minutes after every hour every day`
	• `0 22 * * * Run at 22:00 every day`
	• `0 0 1 1,6 * Run at 00:00 on January 1 and June 1`
	• `30 8,12 * * 1-5 Run weekdays at 08:30 and 12:30`
	• `0 2 */2 * * Run every other day at 02:00`

View Task Schedule	Click to view the task schedule. The *Task Schedule* dialog box displays a list of scheduled tasks. Click a task to review the task details. For more information, see View task schedules.

10. Click **Save**.

Related topics

About Discovery Results

View and search Discovery Results

Stop a running discovery scan

Delete Discovery Schedules

About Discovery Results

Discovery Results show information identified during Discovery Schedule scans.

If devices in inventory correspond to records in the Discovery Results, the devices' current connection status is displayed. The device name links to the *Inventory Detail* page for that device, and the *Device Action* drop-down list in the *DNS Lookup* column shows the available Device Actions.

NOTE: For information about browser requirements for Device Actions, go to https://support.quest.com/kb/148787.

Discovery Results are a "point-in-time" view, and any newly defined devices for management will reflect their state the next time discovery is run.

See Managing inventory information.

The results showing the IP address at the time of the scan might not reflect the current IP address of a given device if the DHCP-assigned IP address has changed.

View and search Discovery Results

You can view and search Discovery Results for device information and for the properties of the scans used to discover devices.

1. Go to the *Discovery Results* list:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Inventory**, then click **Discovery Results**.
2. To sort the list, do any of the following:
    - **Select Choose Action > Include Unreachable Items. The list displays devices that have a connection to the appliance and devices that cannot currently be reached.**
    - **In the *View By* drop-down list, select Discovery Name. The list is sorted to group according to the name of the Discovery Schedule under which they were discovered.**
3. To view device details, click the link in the *Hostname* or *IP Address [Labels]* column.
4. To search for devices:
    a. Click the **Filter** tab above the list on the right to display the *Advanced Search* panel.
    b. Select search criteria:
    # Select an attribute in the left-most drop-down list. For example: **Device Info: Ping Test**.
    # Select a condition in the next drop-down list. For example: **has**.
    # Select the status attribute in the next drop-down list. For example: **Failed**.
    c. Click **Search**.

Provision the Agent using the discovered IP address or hostname

You can provision the Agent on devices using the IP address or hostname from the *Discovery Results* page.

After devices have been identified in Discovery Results, you can provision or install the Agent on those devices using the links on the *Discovery Results* page. This discovery identifies the devices to be provisioned at the outset, rather than requiring a scan during the provisioning phase to identify devices.

Provisioning the Agent is especially useful for Windows devices. Windows devices can be discovered, but there are few management options available to Windows devices unless the Agent is installed on those devices.

1. Go to the *Discovery Results* list:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Inventory**, then click **Discovery Results**.
2. Select the check box next to one or more devices.
3. Select **Choose Action**, then do one of the following:
    - **Select Provision > Agent: IP Address.**
    - **Select Provision > Agent: Hostname.**

    The *Provisioning Schedule Detail* page appears. Information about the selected devices appears on the page.
4. Edit the provisioning options as needed.

See Install the KACE Agent on a device or multiple devices.

Stop a running discovery scan

You can stop a running scan at any point in its progress.

You can stop a running discovery scan from either the *Discovery Schedules* list or from the *Discovery Schedule Detail* page. You can stop multiple scans from the *Discovery Schedules* list.

When you interrupt a scan with **Stop**, whatever devices in the IP range that has been scanned up to that point appear in *Discovery Results*.

1. Go to the *Discovery Schedules* list:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Inventory**, then click **Discovery Schedules**.
2. Stop a running scan using one of two methods:
    - **Stop one or more running scans using the Choose Action menu.**
        1. Select the check box next to one or more schedules.
        2. Select **Choose ActionStop**, then click **Yes** to confirm.

        NOTE: If any of the selected schedules are not running, selecting **Stop** does not prevent the scan from running at its next scheduled time.
    - **Stop a running scan from its *Discovery Schedule Detail* page.**
        1. Click the Discovery Schedule in the *Name* column to display the *Discovery Schedule Detail* page.
        2. Scroll to the bottom of the page, click **Stop**, then click **Yes** to confirm.

        NOTE: When a scan is running, the **Stop** button takes the place of the **Run Now** button.

Scan activity stops for the designated Discovery Schedule. The *Progress* column on the *Discovery Schedules* list displays *Stopping* until the scan is fully stopped, at which point the progress status changes to *Stopped*.

Delete Discovery Schedules

You can delete Discovery Schedules as needed. When Discovery Schedules are deleted, scan results related to those schedules are also deleted. Devices discovered using the schedules, and added to inventory, remain in inventory.

1. Go to the *Discovery Schedules* list:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Inventory**, then click **Discovery Schedules**.
2. Select the check box next to one or more schedules.
3. Select **Choose Action** > **Delete**, then click **Yes** to confirm.

Managing device inventory

You can use the appliance to manage devices. Devices managed by the appliance are referred to as device inventory.

About managing devices

Managing devices is the process of using the appliance to collect and maintain information about devices on your network and performing tasks such as monitoring device status, creating reports, and so on.

To add devices to the appliance inventory, you can:

- **Install the KACE Agent on devices**. Devices are automatically added to inventory after the Agent is installed on them and the Agent reports inventory to the appliance. See Provisioning the KACE Agent.
- **Enable Agentless management for devices**. Agentless management is especially useful for devices that cannot have the KACE Agent installed, such as devices with unsupported operating systems. See Managing Agentless devices.
- **Upload inventory information for devices manually**. See Adding devices manually in the Administrator Console or by using the API.

NOTE: Your product license agreement entitles you to manage a specified number of devices that are classified as Managed Computers, Chromebooks & Network Devices, and Monitored Computers. Devices count toward these limits even if such devices are MIA (missing in action) or no longer in use. However, devices that are added to inventory manually, or through the API, do not count toward license limits. See View product licensing information.

For information about the features available to devices, see Features available for each device management method.

Features available for each device management method

Device management features vary, depending on the method used to manage the device and the device's operating system.

For Windows devices, installing the Agent provides a full range of features. For Linux® devices and devices that cannot have the Agent installed, such as printers and network devices, Agentless management is the recommended option.

The following table provides a high-level view of the components and features available to managed devices.

NOTE: Under *Agentless*, the *Non-Win* OSs are Mac OS X, CentOS™, Debian®, FreeBSD®, Oracle® Enterprise Linux, Red Hat Enterprise Linux, SUSE, Solaris®, and Ubuntu.

Table 10. Features available to managed devices

Feature or component	Agent	Agentless							WSAPI manual
	Win, Mac, Linux	Win	Non-Win	Google Workspace Devices	KACE MDM	DMM	Workspace ONE	SNMP	
Home									
Dashboard: Includes device information where appropriate. See About Dashboards.	X	X	X	X	X	X	X	X	
Label Management: Labels can be assigned to devices. See About labels.	X	X	X	X	X	X	X	X	X
Search: Devices included in results. See Searching for information and filtering lists.	X	X	X	X	X	X	X	X	X
Inventory									
Devices: List includes devices. See Managing inventory information.	X	X	X	X	X	X	X	X	X
Devices > Force Inventory. See Forcing inventory updates.	X	X	X	X	X	X	X	X	
Devices > MIA settings. See Managing MIA devices.	X	X	X	X	X	X	X	X	
Devices > Apply SNMP Configurations. See Using SNMP Inventory Configurations to identify specific SNMP objects and non-computer devices to add to inventory.								X	
Software page: List includes software from devices. See About the Software page.	X	X	X	X	X	X	X		
Software Catalog page: List includes software from devices. See Viewing Software Catalog information.	X Windows and Mac only								

Feature or component	Agent	Agentless							WSAPI manual
	Win, Mac, Linux	Win	Non-Win	Google Workspace Devices	KACE MDM	DMM	Workspace ONE	SNMP	
Metering: Metering can be enabled for devices. See Using software metering.	X Windows and Mac only								
Blocking software (Mark Not Allowed): Software can be prevented from running on devices. See Using Application Control.	X Windows and Mac only								
Processes: Inventory available for devices. See Managing process inventory.	X	X	X						
Startup programs: Inventory available for devices. See Managing startup program inventory.	X	X	X						
Services: Inventory available for devices. See Managing service inventory.	X	X							
Discovery Schedules: Devices can be discovered. See About Device Discovery and device management.	X	X	X	X	X	X	X	X	X
Discovery Results: Devices can be provisioned from results list. See About Device Discovery and device management.	X	X	X	X	X	X	X	X	
SNMP Inventory Configurations: List of devices can be expanded. See Using SNMP Inventory Configurations to identify specific SNMP objects and non-computer devices to add to inventory.								X	
Inventory: Custom inventory rules. See Writing custom inventory rules.	X								
Monitoring									

Feature or component	Agent	Agentless							WSAPI manual
	Win, Mac, Linux	Win	Non-Win	Google Workspace Devices	KACE MDM	DMM	Workspace ONE	SNMP	
Alerts: Received alerts. See Working with alerts.	X	X	X						
Devices: List includes devices with monitoring enabled. See Managing monitoring for devices.	X	X	X						
Profiles: Alerts are defined through profiles. See Working with monitoring profiles.	X	X	X						
Maintenance Windows: Can set regular schedule for pausing monitoring. See Schedule a Maintenance Window during which time alerts are not collected from a device.	X	X	X						
Log Enablement Packages: These packages enable performance threshold monitoring and monitoring for applications such as Exchange, Internet Information Services (IIS), and so on. See Configuring application and threshold monitoring with Log Enablement Packages.	X	X	X						
Assets									
Assets: Can be created for devices. See About managing assets.	X	X	X	X	X	X	X	X	X
Asset Types: Can be created for devices. See Adding and customizing Asset Types and maintaining asset information.	X	X	X	X	X	X	X	X	X
Locations: Can be defined for devices, users, and assets. See Managing locations.	X	X	X	X	X	X	X	X	X
Import Assets: Can be imported for devices. See Importing license data in CSV files.	X								
Distribution									

Feature or component	Agent	Agentless						WSAPI manual
	Win, Mac, Linux	Win	Non-Win	Google Workspace Devices	KACE MDM	DMM	Workspace ONE	SNMP	
Managed Installations: Can be used to install software on devices. See Using Managed Installations.	X								
File Synchronizations: Can be used to manage files on devices. See Create and use File Synchronization.	X								
Wake-on-LAN: Available for devices with valid IP address and MAC address. See Using Wake-on-LAN.	X	X	X					X	
Replication: Can be used as replication shares. See Using Replication Shares.	X								
Alerts: Can be broadcast to display on devices (different from server monitoring alerts). See Broadcasting alerts to managed devices.	X Windows and Mac only								
Scripting									
Run Now: Can be used to run scripts on devices. See Using the Run and Run Now commands.	X								
Run Now Status: Can be displayed for devices. See Monitor Run Now status and view script details.	X								
Search Scripting Logs: Devices listed in results. See Search the scripting logs.	X								
Security									
Patch Management: Can be used to patch devices. See About patch management.	X Windows and Mac only								

Feature or component	Agent	Agentless							WSAPI manual
	Win, Mac, Linux	Win	Non-Win	Google Workspace Devices	KACE MDM	DMM	Workspace ONE	SNMP	
Dell Updates: Can be used to update devices. See Managing Dell devices and updates.	X Windows only								
Service Desk									
Tickets: Can be created and assigned to devices. See Creating tickets from the Administrator Console and User Console.	X	X	X	X	X	X	X	X	
User Downloads: Software can be downloaded from the **User Console** to devices. See Managing User Downloads.	X								
Knowledge Base. See Managing Knowledge Base articles.	X	X	X	X	X	X	X	X	
Announcements: Can create announcements that appear on the **User Console** home page. See Add, edit, hide, or delete User Console announcements.	X	X	X	X	X	X	X	X	
Configuration. See Setting up Service Desk.	X	X	X	X	X	X	X	X	
Reporting									
Reports: Device information available for reports. See Creating reports.	X	X	X	X	X	X	X	X	
Report Schedules: View report schedules that have been created. See Scheduling reports.	X	X	X	X	X	X	X	X	
Notifications: Devices can be included in notifications. See Scheduling notifications.	X	X	X	X	X	X	X	X	
Settings: Control Panel									
Device Actions: Actions can be performed on devices. See Run actions on devices.	X	X	X					X	

Feature or component	Agent	Agentless							WSAPI manual
	Win, Mac, Linux	Win	Non-Win	Google Workspace Devices	KACE MDM	DMM	Workspace ONE	SNMP	
License Usage Warning levels: Available for applications on devices. See Assign threat levels to applications.	X	X	X	X	X	X	X	X	
History: Device information can be tracked. See Managing asset history.	X	X	X	X	X	X	X	X	
Logs: Device information available. See View appliance logs.	X	X	X	X	X	X	X	X	
Backup and restore: Device information included. See About appliance backups.	X	X	X	X	X	X	X	X	
Organizations									
Filters: Organization filters can be assigned to devices. See Managing organization filters.	X	X	X	X	X	X	X	X	
Redirect Devices: Devices can be reassigned to organizations. See Redirect devices.	X	X	X	X	X	X	X	X	X
Filtering Devices: Devices can be filtered and reassigned to organizations. See Filter devices.	X	X	X	X	X	X	X	X	
Organization settings: Inventory intervals configurable. See Schedule inventory data collection for managed devices.	X	X	X	X	X	X	X	X	

About inventory information

Inventory includes information about the devices, applications, processes, startup programs, and services on managed devices on your network.

Inventory is:

- Collected by the KACE Agent, which is installed on managed devices
- Uploaded using the inventory API
- Obtained through connections to Agentless devices

You can view detailed data about individual managed devices, as well as aggregated data collected across all managed devices. In addition, you can use inventory information in reports, and in decisions about upgrades, troubleshooting, purchasing, policies, and so on.

This section focuses on device inventory. For information about other inventory items, see:

- Managing applications on the Software page
- Managing Software Catalog inventory
- Managing process, startup program, and service inventory

Tracking changes to inventory settings

If History subscriptions are configured to retain information, you can view the details of the changes made to settings, assets, and objects.

This information includes the date the change was made and the user who made the change, which can be useful during troubleshooting. See About history settings.

About inventory change history

Change history for devices begins when there is a change to the information collected during the first report.

The first time a managed device reports inventory to the appliance, the information is considered to be a baseline report. As such, it is not recorded in the change history.

Managing inventory information

To manage inventory information, you can add custom data fields, view devices in inventory, and view device details.

Add custom data fields

You can add custom data fields for applications added manually from the *Software* list.

Adding custom data fields enables you to obtain information from the registry and elsewhere on the device. This information can be viewed on the device detail page and used in reports.

For example, you might want to add custom fields to obtain the *DAT file version number* from the registry, the *file created date*, the *file publisher*, or other data for a device. You could then create labels based on this information to group similar devices, or create reports using this information.

1. Go to the *Software* list:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Inventory**, then click **Software**.
2. Select **Choose Action** > **New**.
3. Enter values in the *Name*, *Version*, and *Publisher* fields.

    This information is used to identify the custom data field on detail pages.
4. In the *Custom Inventory Rule* field, enter the appropriate syntax for the information you want returned:
    - **To return a Registry Value, enter the following, replacing valueType with either `TEXT`, `NUMBER`, or `DATE`. `NUMBER` is an integer value: `RegistryValueReturn(string absPathToKey, string valueName, string` valueType)**

Example: `RegistryValueReturn(HKEY_LOCAL_MACHINE\Software\McAfee.com \Virusscan Online,SourceDisk, TEXT)`

- **On Windows, Mac, and Linux devices, you can retrieve the following attributes from the `stat()` function:**

  ```
  access_time, creation_time, modification_time, block_size, blocks, size, device_id, group, inode, mode, number_links, owner, device_number
  ```

- **On Windows devices, you can retrieve the following attributes from the `VerQueryValue()` function:**

  ```
  FileName, Comments, CompanyName, FileDescription, FileVersion, InternalName, LegalCopyright, LegalTrademarks, OriginalFilename, ProductName, ProductVersion, PrivateBuild, SpecialBuild, AccessedDate, CreatedDate, ModifiedDate
  ```

5. Click **Save**.

See Writing custom inventory rules.

Schedule inventory data collection for managed devices

The appliance collects hardware and software inventory data from Agent-managed and Agentless devices according to the appliance data collection schedule you set.

For Agent-managed devices, software inventory information is available on both the *Software* and *Software Catalog* pages. For more information about these pages, see Differences between the Software page and the Software Catalog page.

For Agentless devices, software information is listed only on the *Software* page. See Managing applications on the Software page.

If the Organization component is enabled on your appliance, you schedule inventory data collection for each organization separately.

1. Do one of the following:

   - **If the Organization component is enabled on your appliance, log in to the appliance System Administration Console, `https://appliance_hostname/system`, or select System in the drop-down list in the top-right corner of the page next to the login information. Then click Organizations. To display the organization's information, click the organization's name.**

     On the *Organization Detail* page that appears, locate the *Communication and Agent Settings* section.

   - **If the Organization component is not enabled on your appliance, log in to the appliance Administrator Console, `https://appliance_hostname/admin`. Then select Settings > Provisioning., and click Communication Settings on the *Provisioning* panel.**

     The *Communication Settings* page appears.

2. In the *Agent and Communications Settings* section, specify the following settings:

   NOTE: To reduce the load on the appliance, limit the number of Agent connections to 500 per hour. The number of connections that appears next to the inventory, scripting, and metering intervals, applies to the current organization only. If the Organization component is enabled on your appliance, the total number of Agent connections for all organizations should not exceed 500 per hour.

Option	Suggested Setting	Notes
Agent Logging	Enabled	Whether the appliance stores scripting results provided by Agents installed on managed devices. Agent logs can consume as much as 1GB of disk space in the database. If disk space is not an issue, enable *Agent Logging* to keep all log information for Agent-managed devices. These logs can be useful during troubleshooting. To save disk space, and enable faster Agent communication, disable *Agent Logging*.

Option	Suggested Setting	Notes
Agent Inventory	12 hours	The frequency at which Agents on managed devices report inventory. This information is displayed in the *Inventory* section.
Agentless Inventory	1 Day	The frequency at which Agentless devices report inventory. This information is displayed in the *Inventory* section.
Catalog Inventory	24 hours	The frequency at which managed devices report inventory to the *Software Catalog* page.
Metering	4 hours	The frequency at which managed devices report metering information to the appliance. Requires metering to be enabled on devices and applications.
Scripting Update	4 hours	The frequency at which Agents on managed devices request updated copies of scripts that are enabled on managed devices. This interval does not affect how often scripts run.

3. In the *Notify* section, specify the message to use for Agent communications:

Option	Suggested Setting	Notes
Agent Splash Page Message	Default text: `KACE Systems Management Appliance is verifying your PC Configuration and managing software updates. Please Wait...`	The message that appears to users when Agents are performing tasks, such as running scripts, on their devices.

4. In the *Agentless* section, specify communications settings for Agentless devices:

Option	Description
SSH Timeout	The time, in seconds or minutes, after which the connection is closed if there is no activity.
SNMP Timeout	The time, in seconds, after which the connection is closed if there is no activity.
Maximum Attempts	The number of times the connection is attempted.
WinRM Timeout	The time, in seconds or minutes, after which the connection is closed if there is no activity.

5. If the Organization component is not enabled on your appliance, specify *Agent* settings.

NOTE: If the Organization component is enabled on your appliance, *Agent* settings are located on the appliance *General Settings* page.

Option	Description
Last Task Throughput Update	This value indicates the date and time when the appliance task throughput was last updated.

Option	Description
Current CPU Load	The value in this field depicts the load on an appliance at any given time. For the appliance to run normally, the value in this field must be between 0.0 and 10.0.
Task Throughput	The value that controls how scheduled tasks, such as inventory collection, scripting, and patching updates, are balanced by the appliance. **NOTE:** This value can be increased only if the value in the Current CPU Load is not more than 10.0 and the Last Task Throughput Update time is more than 15 minutes.

6. Click **Save**.

   The changes take effect when Agents check in to the appliance.

7. If you have multiple organizations, repeat the preceding steps for each organization.

Related topics

View appliance logs

Configure appliance General Settings with the Organization component enabled

View device inventory and details

You can view the list of devices in inventory on the *Devices* page, and you can view information about any selected device on the *Device Detail* page.

1. Go to the *Device Detail* page:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Inventory**, then click **Devices**.
   c. Click the name of a device.
2. To expand the sections on the *Device Detail* page, click **Expand All** above the *Summary* section.

   The fields that are displayed depend on the type of device and its operating system. For example, if the device is a virtual machine, the *Monitor* field is not displayed, although the *Video Controller* is. In addition, some fields are available for some operating systems but not for others. For example, *System Description* is available for Windows or SNMP devices only.

   To view tables describing the contents of the groups and sections that appear on this page, see Groups and sections of items in device details.

3. **Optional**: If change tracking is enabled for inventory information, click **Show All History** above the *Summary* section to see the history of inventory changes.

Related topics

Configuring history settings

Managing Agent communications

Schedule inventory data collection for managed devices

About the Asset Management component

Viewing information about devices enrolled in KACE Cloud MDM

The appliance displays information about Mac OS X devices that are enrolled in an integrated KACE Cloud Mobile Device Manager (MDM) instance.

The type of information available for such devices depends on whether they have a KACE Agent installed. There are three possible scenarios that determine the type of information collected from Mac OS X devices enrolled in KACE Cloud MDM:

- Hybrid appliance-first device management
- KACE Cloud MDM device management
- Hybrid KACE Cloud MDM-first device management

Hybrid appliance-first device management

1. A Mac OS X device has a KACE Agent installed and configured to connect to the appliance.
2. The device is enrolled in KACE Cloud MDM integrated with the appliance.
3. The appliance recognizes the device as a standard Agent-based device.

KACE Cloud MDM device management

1. A Mac OS X device is enrolled in KACE Cloud MDM integrated with the appliance.
2. KACE Cloud MDM collects inventory information from the device.
3. The appliance recognizes the device as a standard Agentless KACE Cloud MDM device.

Hybrid KACE Cloud MDM-first device management

1. A Mac OS X device is enrolled in KACE Cloud MDM integrated with the appliance.
2. KACE Cloud MDM collects inventory information from the device.
3. The appliance recognizes the device as a standard Agentless KACE Cloud MDM device.
4. A KACE Agent is installed on the device and configured to connect to the appliance.
5. The appliance recognizes the device as a standard Agent-based device.

For complete information about the device fields appearing on the *Device Details* page, see Groups and sections of items in device details.

Groups and sections of items in device details

The *Device Details* page for a device contains inventory information presented in sections that are collected in groups. The extent and focus of information included on the page depends on the device and any subtypes indicated.

NOTE: If you have assigned an Asset Subtype, you can choose whether to show or hide the details that appear for each Device on the *Device Detail* page. For example, for the subtype *Printer*, information that is irrelevant to printers, such as the items *Installed Programs*, *Discovered Software*, and *Metered Software*, could be made hidden. Whole groups can be hidden as well. See Add Asset Subtypes and select Device Detail page preferences.

Scoped users can see the details of all devices, but can only edit the details of those devices that are associated with their role. For more information about user roles, see Add or edit User Roles.

The following groups can appear on the *Device Details* page:

- Summary group
- Inventory Information group
- Software group
- Activities group
- Security group
- Dell Command | Monitor group
- Dell Updates group
- Logs and Diagnostics group
- Asset group

Summary group

Basic device identification information. The items are not separated into sections as in the other groups on the page. The entries that appear on the *Device Detail* page vary depending on the device, operating system (if relevant), connection type, and so on.

Item	Description	Database field
System Name	The hostname or IP address of the device.	NAME
Asset Subtype	The Asset Subtype for this device, if one has been assigned. Asset Subtypes are subcategories of assets that you can add to any Asset Type, including custom Asset Types. This enables you to identify and manage subtypes of assets, such as Device assets that are computers, printers, or routers.	
Asset Location	The location of this asset.	N/A
Assigned To	The device owner. This field is only populated if the device user record exists on the appliance. When you integrate with the KACE Cloud MDM, if the appliance is synchronized with the KACE MDM tenant's Active Directory, the name of the KACE MDM device owner is displayed. For other types of external devices, if the device user record is not found on the appliance, the field is set to *Unassigned*.	N/A
Manual Entry	A field that indicates the inventory information was added manually, either through WSAPI or XML upload. click **Edit** to modify the information.	MANUAL_ENTRY
Device Entry Type	A field that indicates how the device is being managed: *Agent Device*, *Agentless Device*, *Manually Entered Record*, or *Agent/Agentless* (hybrid KACE Cloud MDM inventory). Click **Edit** to change connection protocols.	N/A
System Description	A description of the device, populated by Agentless inventory for Windows and SNMP devices.	SYSTEM_DESCRIPTION

Item	Description	Database field
System Model	The device model.	CS_MODEL
Chassis Type	The type of device, such as desktop or laptop.	CHASSIS_TYPE
Ownership	**KACE MDM devices only**. Indicates the ownership of the device: *Company*, *Personal* or *Unknown*.	OWNERSHIP
IP Address	The IP address of the device.	IP
MAC Address	The device's Media Access Control (MAC) address number.	MAC
RAM Total	The total amount of random-access memory (RAM) on the device.	RAM_TOTAL
Operating System Name	The operating system of the device, such as Windows, Mac OS X®, or Linux.	OS_NAME
Service Pack	The service pack version number (Windows or SUSE Linux Enterprise Server only).	SERVICE_PACK
Uptime Since Last Reboot	The amount of time the device has been running since it was restarted.	UPTIME
Agent Version	The version number of the KACE Agent installed on the device.	CLIENT_VERSION
Device Timezone	The timezone used by the KACE Agent installed on the device.	TZ_AGENT
Source	The source of the collected device details. • **Agent-managed devices**: This field is set to `Agent`. • **Agentless devices**: This field reflects the connection type. For example, `VMware`. • **Agent-managed devices that are also enrolled in KACE Cloud MDM**: This field is set to `Agent/KACE Cloud Mobile Device Manager`. Click the **KACE Cloud Mobile Device Manager** link to see this device in the KACE MDM Cloud inventory.	N/A
User Name	The name of the most recent user who logged in to the device. Some devices might have multiple users.	USER
Agent Connection	The time the agent messaging protocol service on the device connected to the appliance and the current connection status (available for Agent-	KBSYS.SMMP_CONNECTION

Item	Description	Database field
	managed devices only). Connection status information includes: • : An Agent-managed device is connected to the appliance. • : An Agent-managed device with server monitoring enabled is connected to the appliance. • : An Agent-managed device is not connected to the appliance. • : The Agent's activity is suspended on the device using the system tray (Windows) or menu bar (Mac OS) until the indicated time and date. • : A manually added device is connected to the appliance. • : An issue is detected on an Agent-managed device. To find out more about device issues, navigate to the Device Issues page. For more information, see Identify device issues.	
Agentless Connection	The time the Agentless device connected to the appliance and the current connection status (available for Agentless devices only). Connection status information includes: • : Agentless-management is enabled for the device. • : Agentless-management and server monitoring is enabled for the device. • : Agentless management is enabled for the device, but the device is not currently reachable.	N/A
Agentless Connection Method	The protocol, such as SNMP, used to collect inventory information from the device.	N/A
Last Inventory	The time of the most recent inventory report.	LAST_SYNC
Device Created	The date and time that the device's first inventory record was created.	CREATED
Device Modified	The date and time that the device's inventory record was modified.	MODIFIED
Contact	**Printers only**. The contact information for the selected printer, such as an email address. This information is stored in the managed printer's SNMP `sysContact` field.	

Item	Description	Database field
Location	**Printers only**. The location of the selected printer, such as the name of the organization. This information is stored in the managed printer's SNMP `sysLocation` field.	
Volume **n**	The type and size of the disk drive's file system, and amount of space used on the disk drive. To view changes to the drive usage, click **Show Usage History** link in this field. This information is updated when usage increases or decreases by 5% or more. There is one entry for each volume. For VMware® ESXi® host devices, each datastore associated with the ESXi host is listed as a volume.	MACHINE_DISKS
Force Inventory	Click **Force Inventory** to immediately update inventory information for the device and synchronize the device with the appliance. **Force Inventory** is available only if the agent messaging protocol connection to an Agent-managed device is active, or for Agentless devices, if the device is reachable.	N/A
VMware UUID	This field is only visible when you select a VMware device. The UUID is a globally unique identifier for the vCenter Server or the ESXi host.	INSTANCE_UUID
Hyper-V UUID	This field is only visible when you select a Hyper-V device. The UUID is a globally unique identifier for the SCVMM or the Hyper-V server.	INSTANCE_UUID
Managing Virtual Machine Manager	The name of the managing vCenter (VMware devices) or SCVMM (Hyper-V devices). If the managing vCenter or SCVMM is already provisioned by the KACE Agent, its name in this column appears as a hyperlink. When you click the link, the page is updated to display device details for the provisioned virtual machine manager.	N/A
Choose Action	• To upload agent files, click **Choose Action** > **Upload Agent Files (Diagnostic)**. When done, links to uploaded files appear in the *Logs and Diagnostics* group on this page. • To add the device to the KACE Systems Deployment Appliance (SDA) boot action, click **Choose Action** > **Add to SDA Boot Action**. KACE SDA boot actions are used to automate image deployments to target devices. You can only create boot actions from the selected device if a linked KACE SDA exists, and the device has a wired network connection. This command is also available from the **Choose Action** menu on the *Devices* list page. When you click this command, the KACE SDA *Automated Deployment Detail*	N/A

Item	Description	Database field
	page appears. For more information about this page, see the KACE SDA *Administrator Guide*. • To delete the selected device, click **Choose Action** > **Delete**.	
KACE Cloud Mobile Device Manager (MDM) commands	When you integrate with the KACE Cloud MDM and select a KACE Cloud MDM device, an additional set of commands is available in this section. • **Force Inventory**: Requests from the KACE Cloud MDM to initiate a new inventory for the device. When complete, the appliance synchronizes the inventory information. • **Lock**: Blocks access to the selected device. Next time the user interacts with the device, they are prompted to provide the device's passcode. • **Set Passcode**: Allows you to specify a new passcode for the selected device.	N/A

Item	Description	Database field

NOTE: This command is only available for Android devices.

- **Clear Passcode**: Unlocks the selected device. The device remains unlocked until a new passcode is provided.
- **Clear Restrictions**: **Android and iOS devices only.** Removes any settings that limit the selected device's functionality.
- **Unenroll Device**: Un-enrolls the selected device from the KACE Cloud MDM.
- **Factory Reset**: Restores the factory settings on the selected device.
- **Restart Device**: **Android (managed), iOS (supervised), and Mac OS devices only.** Restarts the selected device.
- **Shutdown Device**: **iOS (supervised) and Mac OS devices only**. Turns off the selected device.
- **Enable Remote Desktop**: **Mac OS devices only.** Enables remote desktop connections to the selected device.
- **Disable Remote Desktop**: **Mac OS devices only.** Disables remote desktop connections to the selected device.
- **Set Firmware Password**: **Mac OS devices only.** Allows you to specify a password for the selected device's firmware.
- **Clear Firmware Password**: **Mac OS devices only.** Deletes the password for the selected device's firmware.
- **Rotate BitLocker Recovery Keys** : (For Windows) Rotates the bitlocker recovery keys for the selected Windows device.
- **Run Defender Scan** : (For Windows) Starts a Defender anti-malware scan for the selected Windows devices.
- **Update Defender Signatures** : (For Windows) Updates the Defender signatures for the selected Windows device.
- **Set Windows Key**: (For Windows) Sets the Windows product key for the selected Windows device.

Item	Description	Database field
	TIP: These commands are also accessible from the *Devices* list page, from the **Choose Action** menu, when KACE Cloud MDM bulk actions are enabled. This feature is disabled by default. To enable it, on the *General Settings* page, under *Allowed Bulk Actions*, select the **Enable Bulk KACE Cloud MDM Actions** check box. For more information, see Configure Admin-level or organization-specific General Settings. The **Force Inventory** command appears in the main menu, while the other commands are available in the **KACE Cloud MDM** menu.	
VMware virtual machine commands	If your managed environment includes one or more provisioned VMware virtual machines, you can perform device actions from this page, such as powering virtual machines on or off. These commands are available if the following pre-requisites are met: • The provisioned virtual machines must be running on a provisioned VMware ESXi server version 5.5.x or higher. **NOTE:** Your product license agreement allows administrator to manage a specific number of computers, servers, and assets. Each provisioned VMware ESXi server consumes an agentless license. If you want to use this feature, you must ensure that your product license agreement covers all of your provisioned ESXi hosts. For more information, see http://quest.com/docs/Product_Guide.pdf. To increase your license capacity, visit https://quest.com/buy. • VMware Tools must be installed on the target virtual machines to issue **Shut Down Guest OS** and **Restart Guest OS** commands. The other commands do not require VMware Tools. • User account configured in the inventory must have sufficient administrative-level permissions in order to perform these actions. The following commands are available when you select a provisioned VMware virtual machine. • **Power On**: Powers on the selected virtual machine. If the virtual machine is suspended, this action causes the suspended virtual machine to be powered on. • **Power Off**: Powers off the selected virtual machine. If the virtual machine is a fault-tolerant primary virtual machine, this results in one or more	N/A

Item	Description	Database field
	of the secondary virtual machines being powered off as well. • **Suspend**: Suspends the execution of the selected virtual machine. • **Reset**: Resets the power on the selected virtual machine. If the virtual machine is currently powered on, this action first powers it off, then powers it on. • **Shut Down Guest OS**: Issues a command to the guest operating system on the selected virtual machine to perform a clean shutdown of all services. • **Restart Guest OS**: Issues a command to the guest operating system on the selected virtual machine to perform a reboot. **TIP:** These commands are always available on the *Device Detail* page. They can also appear on the *Devices* list page in the **Choose Action** menu when bulk actions against virtual machines are enabled. This feature is disabled by default. To enable it, on the *General Settings* page, under *Allowed Bulk Actions*, select the **Enable Bulk Virtual Machine Actions** check box. For more information, see Configure Admin-level or organization-specific General Settings. For complete information about these virtual machine actions, refer to your VMware ESXi documentation.	
Hyper-V virtual machine commands	If your managed environment includes one or more provisioned Hyper-V virtual machines, you can perform device actions from this page, such as powering virtual machines on or off. The following commands are available when you select a provisioned Hyper-V virtual machine. • **Power On**: Powers on the selected virtual machine. If the virtual machine is suspended, this action causes the suspended virtual machine to be powered on. • **Power Off**: Powers off the selected virtual machine. If the virtual machine is a fault-tolerant primary virtual machine, this results in one or more of the secondary virtual machines being powered off as well. • **Suspend**: Suspends (pauses) of the selected virtual machine. • **Resume**: Resumes a suspended virtual machine. • **Reset**: Resets the power on the selected virtual machine. If the virtual machine is currently	N/A

Item	Description	Database field
	powered on, this action first powers it off, then powers it on. • **Shut Down Guest OS**: Issues a command to the guest operating system on the selected virtual machine to perform a clean shutdown of all services. • **Restart Guest OS**: Issues a command to the guest operating system on the selected virtual machine to perform a reboot. **TIP:** These commands are always available on the *Device Detail* page. They can also appear on the *Devices* list page in the **Choose Action** menu when bulk actions against virtual machines are enabled. This feature is disabled by default. To enable it, on the *General Settings* page, under *Allowed Bulk Actions*, select the **Enable Bulk Virtual Machine Actions** check box. For more information, see Configure Admin-level or organization-specific General Settings. For complete information about these virtual machine actions, refer to your Hyper-V documentation.	
Chrome device commands	If your managed environment includes one or more provisioned Chrome devices, the following commands are available when you select a Chrome device: • **Move**: Moves a provisioned device to a different organizational unit. • **Disable**: Disables a provisioned device. You can use this command if a device is lost or stolen. • **Re-Enable**: Enables a previously disabled device. • **Deprovision**: Removes all provisioning policies from the device. You typically need to do that for devices that are no longer used in your organization so that you no longer need to manage them. **TIP:** These commands are always available on the *Device Detail* page. They can also appear on the *Devices* list page in the **Choose Action** menu when bulk actions against virtual machines are enabled. This feature is disabled by default. To enable it, on the *General Settings* page, under *Allowed Bulk Actions*, select the **Enable Bulk Chrome OS Actions** check box. For more information, see Configure Admin-level or organization-specific General Settings. For complete information about these Chrome device actions, refer to the Google documentation.	

Item	Description	Database field
Microsoft Defender commands	The following requirements must be met in order for a managed device to have access to these commands: • Agent managed or agentless device • Windows 10 or later, or Windows Server 2016 or later • Powershell is required The following commands are available: • **Perform a Microsoft Defender Quick Scan**: Scans the locations in which malware can be registered, such as registry keys and Windows startup directories. • **Perform a Microsoft Defender Full Scan**: Starts by running a quick scan followed by a scan of all fixed, removable, and network drives, as applicable. • **Update Microsoft Defender Signatures**: Updates the anti-malware definitions. • **Enable Microsoft Defender**: Turn on Microsoft Defender on the selected device. • **Disable Network Traffic**: Disables network traffic to and from the selected device. **TIP:** These commands are also accessible from the *Devices* list page, from the **Choose Action** menu, when Microsoft Defender bulk actions are enabled. This feature is disabled by default. To enable it, on the *General Settings* page, under *Allowed Bulk Actions*, select the **Enable Bulk Microsoft Defender Actions** check box. For more information, see Configure Admin-level or organization-specific General Settings.	

Inventory Information group

Additional details on items in the *Summary* section.

Section or Item	Description	Database field
Hardware	Information about the device's hardware. If change history is enabled for this section, and the information in this section has changed, the **Show Changes** link appears next to the heading. Click **Show Changes** to view only those items that have changed. Click **Hide Changes** to view all items.	
RAM Total	The total amount of random-access memory (RAM) installed on the device.	RAM_TOTAL

Section or Item	Description	Database field
RAM Used	The amount of random-access memory (RAM) in use on the device.	RAM_USED
RAM Maximum	The maximum amount of random-access memory (RAM) that the device can support.	RAM_MAX
System Manufacturer	The device manufacturer.	CS_MANUFACTURER
System Model	The device model.	CS_MODEL
CSP ID Number	The system serial number.	CSP_ID_NUMBER
Asset Tag	**Windows, Chrome and KACE MDM devices only**. The BIOS Asset Tag of a system. An Admin can use a bios utility to set this value on the system.	ASSET_TAG
Domain	The Windows domain to which the device is joined.	CS_DOMAIN
Motherboard Primary Bus	The main bus.	MOTHERBOARD_PRIMARY_BUS
Motherboard Secondary Bus	The peripheral bus.	MOTHERBOARD_SECONDARY_BUS
Processors	The CPU count, type, and manufacturer.	PROCESSORS
Architecture	The architecture of the device operating system, such as x86 or x64.	SYS_ARCH
Virtual Device	Used to identify devices that are virtual, such as devices running on VMware platforms. Not displayed for physical devices, such as laptops and servers.	VIRTUAL
Trusted Platform Module (TPM)	On devices with the TPM dedicated microprocessor installed, displays specifications and information about whether TPM is enabled and activated. See About Dell Data Protection | Encryption (DDP|E) and encryption information in device details.	MACHINE_TPM
Intel AMT Device	On Intel-based Windows devices with Intel AMT technology present, displays information about configuration. See About Intel AMT information in device details.	INTEL_AMT
CD/DVD Drives	The configuration of CD-ROM and DVD-ROM drives installed on the device.	CDROM_DEVICES
Sound Devices	Information about audio devices on the device.	SOUND_DEVICES
Video Controllers	Information about video controllers on the device.	VIDEO_CONTROLLERS

Section or Item	Description	Database field
Monitors	The type and manufacturer of the monitor attached to the device. For virtual devices, this displays monitor information if it is reported by the operating system.	MONITOR
Apple Support Information	Link to the Support page at Apple.	N/A
SMC Version	The System Management Controller version of the device CPU.	BIOS_NAME
Serial Number	The serial number of the device.	BIOS_SERIAL_NUMBER
Boot ROM Version	The Boot ROM or Firmware version of the device.	BIOS_VERSION
Dell Service Information	Information about Dell hardware, including the Service Tag, System Type, Ship Date, Country, and warranty information. This section also includes a *Days Left* column, which indicates the number of days remaining in the warranty period, and *Last Updated* column, which indicates the last time the warranty information was refreshed. To update Dell Service information, click **Refresh**.	DELL_WARRANTY
BIOS Name	The BIOS name.	BIOS_NAME
BIOS Version	The BIOS version.	BIOS_VERSION
BIOS Release Date	The date the BIOS version was released.	BIOS_DATE
BIOS Manufacturer	The BIOS manufacturer.	BIOS_MANUFACTURER
BIOS Description	The BIOS description.	BIOS_DESCRIPTION
BIOS Serial Number	The BIOS serial number.	BIOS_SERIAL_NUMBER
Black Toner - Description	**Printers only**. The make and model of the black toner.	
Black Toner - Maximum Level	**Printers only**. The maximum level of the black toner powder.	
Black Toner - Current Level	**Printers only**. The current level of the black toner powder. If the toner is not installed, a message appears in this field.	
Cyan Toner - Description	**Color printers only**. The make and model of the cyan toner.	

Section or Item	Description	Database field
Cyan Toner - Maximum Level	**Color printers only**. The maximum level of the cyan toner powder.	
Cyan Toner - Current Level	**Color printers only**. The current level of the cyan toner powder. If the toner is not installed, a message appears in this field.	
Magenta Toner - Description	**Color printers only**. The make and model of the magenta toner.	
Magenta Toner - Maximum Level	**Color printers only**. The maximum level of the magenta toner powder.	
Magenta Toner - Current Level	**Color printers only**. The current level of the magenta toner powder. If the toner is not installed, a message appears in this field.	
Yellow Toner - Description	**Color printers only**. The make and model of the yellow toner.	
Yellow Toner - Maximum Level	**Color printers only**. The maximum level of the yellow toner powder.	
Yellow Toner - Current Level	**Color printers only**. The current level of the yellow toner powder. If the toner is not installed, a message appears in this field.	
Volume **n**	The type and size of the disk drive's file system, and amount of space used on the disk drive. To view changes to the drive usage, click **Show Usage History** link in this field. This information is updated when usage changes by plus or minus 5%. There is one entry for each volume.	MACHINE_DISKS
Lenovo Service Information	**Lenovo devices only**. Information about the selected Lenovo device. This section is populated when you provide the manufacturer's API keys on the *General Settings* page. For more information, see Configure appliance General Settings with the Organization component enabled.	
	Product: The name of the selected Lenovo device.	PRODUCT
	Purchased: The date when the selected Lenovo device is purchased.	PURCHASED
	Shipped: The date when the selected Lenovo device is shipped.	SHIPPED
	In Warranty: Indicates if the selected Lenovo device is covered by the warranty (*Yes* or *No*).	IN_WARRANTY

Section or Item	Description	Database field
	Country: The country where the selected Lenovo printer is purchased.	COUNTRY
	UpgradeUrl: The URL containing upgrade information.	UPGRADE_URL
	Last Updated: The time stamp of when the device information was last updated.	
	Id: The warranty ID.	ID
	Type: The warranty type: *UNKNOWN*, *BASE*, *UPGRADE*, *EXTENDED* or *INSTANT*.	TYPE
	Start Date: The warranty start date.	START_DATE
	End Date: The warranty end date.	END_DATE
	Name: The warranty name.	
	Description: The warranty description, as applicable.	DESCRIPTION
Printers	The printers that the device is configured to use.	PRINTERS
Network Interfaces	The type of network interface, such as Ethernet card or Bluetooth adapter, and details like IP address, whether DHCP (Dynamic Host Configuration Protocol) is enabled or disabled for the associated IPv4 (Internet Protocol version 4).	MACHINE_NICS
SNMP Data	The results of a SNMP Full Walk of data in the MIB (management information base) on a device, if you set up the *Authenticated* device discovery type to perform a Full Walk. This section does not appear if discovery was made with a Bulk GET.	
MAC Address	The device's wireless MAC address.	MAC_ADDRESS
DHCP	An indicator of whether DHCP is enabled for the IPv4 address associated with this network interface.	
IPv6 Host Configuration	A list containing one or more IPv6 ((Internet Protocol version 6) addresses available on the network interface. For each listed item, this section displays its full IPv6 address and the number of bits in the IPv6 address prefix. An IPv6 prefix typically consists of 64 bits.	
DNS Hostname	The host name associated with this network interface.	

Section or Item	Description	Database field
Wi-Fi	**KACE MDM devices only**. The IP or MAC address of the device.	
Chrome OS	Chrome-related information. **NOTE:** Chrome values are in the MACHINE_CHROMEOS_DETAIL table, not the MACHINE table.	N/A
Directory API ID	The unique ID of the Chrome device.	DEVICE_ID
Status	The status of the Chrome device: ACTIVE, DEPROVISIONED, INACTIVE, RETURN_APPROVED, RETURN_REQUESTED, SHIPPED, UNKNOWN.	STATUS
Support End Date	The final date the device will be supported. This is applicable only for those devices purchased directly from Google.	SUPPORT_END_DATE
Custom User	The user of the device as noted by the administrator.	ANNOTATED_USER
Custom Location	The address or location of the device as noted by the administrator.	ANNOTATED_LOCATION
Order Number	The device's order number. Only devices directly purchased from Google have an order number.	ORDER_NUMBER
Chrome Version	The Chrome device's operating system version.	OS_VERSION
Platform Version	The Chrome device's platform version.	PLATFORM_VERSION
Firmware Version	The Chrome device's firmware version.	FIRMWARE_VERSION
Boot Mode	The boot mode for the device.	BOOT_MODE
Organizational Unit	The full parent path with the Google organization unit's name associated with the device.	ORG_UNIT_PATH
Auto-Update Expiration	The date and time until which the device receives automatic updates.	AUTO_UPDATE_EXPIRATION
Mobile Information	Information from devices managed by KACE Mobile Device Manager (KMDM), and Workspace ONE®	N/A
UDID	The device’s Unique Device Identifier. For iOS devices only.	UDID
Modem Firmware	The mobile device's firmware version.	FIRMWARE_VERSION

Section or Item	Description	Database field
Device type	**DMM devices only**. The type of mobile device. Examples include iPhone, iPad, iPod, Android Phone, and Android Tablet.	DEVICE_TYPE
ICCID	**KACE MDM and DMM devices only**. The unique serial number for the device's SIM card.	ICCID
IMEI	**KACE MDM and DMM devices only**. International Mobile Equipment Identity number for the device.	IMEI
Voice Roaming Enabled	**KACE MDM Android phones only**. An indicator of whether the selected KACE MDM Android phone has voice roaming enabled.	VOICE_ROAMING_ENABLED
Data Roaming Enabled	**KACE MDM Android phones only**. An indicator of whether the selected KACE MDM Android phone has data roaming enabled.	DATA_ROAMING_ENABLED
MEID	**KACE MDM devices only**. The Mobile Equipment Identifier. This is the unique identifier of the selected mobile device.	MEID
Phone Number	**DMM devices only**. Phone number associated with the device.	PHONE_NUMBER
Mobile Operator	**KACE MDM and DMM devices only**. The mobile network carrier.	CARRIER
Bluetooth MAC Address	**DMM devices only**. Media access control address for Bluetooth on the device.	BLUETOOTH_MAC
Battery Level	**KACE MDM and DMM devices only**. Amount of battery charge at last update, in percent.	BATTERY_LEVEL
Last Check-in	The time stamp of when the device information was last updated.	LAST_CHECK_IN
Last Enrollment Time	The date and time the device was last enrolled with the Google Admin console.	LAST_ENROLLMENT_TIME
Enrolled	**KACE MDM and Workspace ONE devices only**. The date and time the device was last enrolled with KACE MDM or Workspace ONE console.	IS_ENROLLED
Supervised	**KACE MDM iOS devices only**. An indicator of whether the selected KACE MDM iOS device is supervised. This is the highest level of control on an iOS device.	IS_SUPERVISED
Lost Mode	**KACE MDM iOS supervised devices only**. An indicator of whether the selected KACE MDM iOS	IS_LOST

Section or Item	Description	Database field
	device is in Lost mode. The Lost mode prevents a device from being unlocked by a third party.	
Encrypted	**KACE MDM devices only**. An indicator of whether the selected KACE MDM iOS device is in Encrypted mode.	IS_ENCRYPTED
Locator Service Enabled	**KACE MDM iOS devices only**. An indicator of whether the selected KACE MDM iOS device is has the Locator Service enabled. This service retrieves the device location information, if the device is responding.	LOCATOR_SERVICE_ENABLED
Activation Lock Enabled	**KACE MDM iOS devices only**. An indicator of whether the activation lock is enabled on the selected KACE MDM iOS device. This feature prevents anyone else from using an iOS device if it is lost or stolen.	ACTIVATION_LOCK_ENABLED
Rooted	**KACE MDM Android devices only**. An indicator of whether the OS of the selected KACE MDM Android device is unlocked.	IS_ROOTED
Compliant	**Workspace ONE devices only**. Indicates if the device meets pre-configured Workspace ONE compliance rules.	IS_COMPLIANT
Current Mobile Network	**Workspace ONE devices only**The name of the mobile network associated with the Workspace ONE device.	N/A
Activation Lock Bypass Code	**KACE MDM iOS DEP-managed devices only**.The bypass code that can be used as the device password, when activation lock is enabled.	ACTIVATION_LOCK_BYPASS_CODE
Allow Supervised Activation Lock	**KACE MDM iOS DEP-managed devices only**. Indicates if activation lock is enabled for the device. Activation lock allows users to bypass the password and log in to the device with the activation lock bypass code.	ACTIVATION_LOCK_ALLOWED
DEP Managed	**KACE MDM iOS devices only**. Indicates if the device is managed by the Apple Device Enrollment Program (DEP).	IS_DEP_MANAGED
DEP Profile	**KACE MDM iOS DEP-managed devices only**. The name of the DEP profile associated with the device.	DEP_PROFILE
DEP Profile Assigned By	**KACE MDM iOS DEP-managed devices only**. The name of the user account that assigned the DEP profile to the device.	DEP_ASSIGNED_BY

Section or Item	Description	Database field
DEP Profile Assigned Date	**KACE MDM iOS DEP-managed devices only**. The date when the DEP profile is assigned to the device.	DEP_ASSIGNED_DATE
DEP Profile Status	**KACE MDM iOS DEP-managed devices only**. The management status of the device: • **Assigned**: Apple DEP received a profile and it is ready to be assigned to the device. • **Empty**: profile is not assigned to the device. • **Pushed**: A profile is delivered to the activated device. • **Removed**: A profile was assigned to the device but has been removed. When the device reactivates, KACE MDM will no longer manage the device.	DEP_PROFILE_STATUS
Device Configured	**KACE MDM iOS DEP-managed devices only**.	IS_DEP_CONFIGURED
Do Not Disturb	Indicates if the device is in Do Not Disturb mode.	DO_NOT_DISTURB_ENABLED
Exchange Device ID	The Microsoft Exchange ID assigned to the device.	EAS_DEVICE_ID
First Enrolled	The date when the device was enrolled in KACE MDM.	ENROLLMENT_DATE
iCloud Enabled	**KACE MDM iOS devices only**. Indicates if cloud is enabled on the devices.	ICLOUD_ENABLED
Last iCloud Backup	**KACE MDM iOS devices only**. The date when Apple iCloud was last backed up on the device.	ICLOUD_LAST_BACKUP
Logged into iTunes	**KACE MDM iOS devices only**. Indicates if the device is logged in to iCloud.	IS_ITUNES_ACCOUNT_ACTIVE
Wi-Fi Received	**KACE MDM Android devices only**. The number of bytes the device received through a Wi-Fi network.	WIFI_BYTES_RECV
Wi-Fi Sent	**KACE MDM Android devices only**. The number of bytes the device sent through a Wi-Fi network.	WIFI_BYTES_SENT
WWAN Received	**KACE MDM Android devices only**. The number of bytes the device received through a mobile network.	WWAN_BYTES_RECV
WWAN Sent	**KACE MDM Android devices only**. The number of bytes the device sent through a mobile network.	WWAN_BYTES_SENT
Agent	Agent-related information.	N/A

Section or Item	Description	Database field
Agent Version	The version number of the KACE Agent installed on the device.	CLIENT_VERSION
Connected	The time the agent messaging protocol service on the device connected to the appliance.	CONNECT_TIME
Disconnected	If disconnected, the time the agent messaging protocol service on the device disconnected from the appliance.	DISCONNECT_TIME
KACE ID	The character string used to identify the device in the appliance database.	KUID
Database ID	The unique number used to identify the device in the appliance database.	ID
Manual Entry	A field that indicates the inventory information was added manually, either through WSAPI or XML upload.	MANUAL_ENTRY
Device Entry Type	A field that indicates how the device is being managed: *Agent Device*, *Agentless Device*, or *Manually Entered Record*. Click **Edit** to change connection protocols.	N/A
Last Inventory	The time of the most recent inventory report.	LAST_INVENTORY
Last Sync	For Agent-managed devices, the time the device last checked in to the appliance. For Agentless devices, the time the appliance last connected to the device and collected inventory.	LAST_SYNC
Last Agent Update	The time of the most recent update to the KACE Agent, if any.	LAST_CLIENT_UPDATE
Konductor Tasks	The status of tasks that are currently running, or that are scheduled to run, on Agent-managed devices. This section displays the following information about each task: • **Task Type**: The type of task. Depending on appliance configuration, task types include alerts, inventory, kbot, krash upload, and scripting updates. • **Start Time**: The start time of the task. • **Completed**: The completion time of the task. • **Next Scheduled**: The next scheduled run time for the task. • **Timeout**: The time limit for completing the task. • **Priority**:The importance or rank of the task.	N/A

Section or Item	Description	Database field
	This information also appears on the *Agent Tasks* list page. For more information, see View Agent task status.	
Quarantine	Information related to the KACE Agent authentication.	N/A
Quarantine Record	A link to the quarantine details for this Agent. For more information, see Registering KACE Agent with the appliance.	KUID
Approved Time	The date and time the KACE Agent is authenticated by the appliance.	APPROVED_TIME
Token Used	If the KACE Agent used a token to register with the appliance, this field contains the token name and a link to the token details.	TOKEN_ID
Approved By	If the KACE Agent connected to the appliance after being granted access by the appliance administrator, this field contains the name of the administrative user that approved the agent's connection.	APPROVED_BY
User	Information related to the device user.	N/A
User Logged	The user currently logged in to the device. This entry includes the username and the domain to which the user belongs.	USER_LOGGED
User Fullname	The full name of the user who owns the device.	USER_FULLNAME
User Name	The name of the current user.	USER_NAME
User Domain	The domain to which the user belongs.	USER_DOMAIN
Operating System	Information about the device's operating system.	N/A
Name	The operating system of the device, such as Windows, Mac OS X, or Linux.	OS_NAME
Service Pack	The service pack version number (Windows or SUSE Linux Enterprise Server only).	SERVICE_PACK
Operating System Version	The version number of the operating system.	OS_VERSION
Operating System Build Version	The build number of the operating system.	OS_BUILD
Number	The number of the operating system.	OS_NUMBER

Section or Item	Description	Database field
Operating System Architecture	The architecture of the device operating system, such as x86 or x64.	OS_ARCH
Domain	The Windows domain to which the device is joined.	CS_DOMAIN
Operating System Installed On	The date the operating system was installed.	OS_INSTALLED_DATE
Last Startup	The length of time the operating system has been running.	LAST_REBOOT
Uptime Since Last Reboot	The amount of time the device has been running since it was restarted.	UPTIME
System Directory	The location of the system directory.	SYSTEM_DIRECTORY
Registry Size	The size of the registry.	REGISTRY_SIZE
Registry Maximum Size	The maximum size of the registry.	REGISTRY_MAX_SIZE
Pagefile Size	The current size of the Windows Pagefile.	PAGEFILE_SIZE
Pagefile Max Size	The maximum size of the Windows Pagefile.	PAGEFILE_MAX_SIZE
IE Version	The version of Internet Explorer installed on the device.	IE_VERSION
Edge Version	The version of Microsoft Edge installed on the device.	EDGE_VERSION
WMI Status	The status of the Windows Management Instrumentation (WMI) service (Windows Devices only).	WMI_STATUS
Drive Encryption	Information on encryption if a DDP|E client has been installed on a device, as well as BitLocker or FileVault2. See About Dell Data Protection | Encryption (DDP|E) and encryption information in device details.	
Drive Encryption Summary	Identifies encryption technology in place, and whether the encryption is enabled.	N/A
Dell Data Protection | Encryption (DDP|E)	Configuration and status information about DDP|E.	N/A
BitLocker	Configuration and status information about Windows BitLocker.	N/A

Section or Item	Description	Database field
FileVault	Configuration and status information about Mac OS X FileVault 2.	N/A
Location	Information from devices managed by Workspace ONE or KACE MDM Cloud.	
Address	The street address of the selected device.	STREET_ADDRESS
City	The city where the selected device is located.	LOCALITY
State/Province	The state or province in which the selected device is located.	REGION
Country	The country where the device is located.	COUNTRY
Latitude	The latitude of the device detected during the last update.	LATITUDE
Longitude	The longitude of the device detected during the last update.	LONGITUDE
Last Update	The time stamp of when the device information was last updated.	LAST_UPDATE
Notes	Any additional information you want to provide.	NOTES
Virtual Machines	When an ESXi host or a Hyper-V server is selected, this group lists the virtual machines associated with the selected device. Some of the information in this list is only available if VMware tools/Microsoft Integration services are installed on the virtual machines. If some columns are not populated, this may be due to missing VMware tools or Microsoft Integration services.	
Name	The name of the virtual machine.	NAME
Hostname	The host name assigned to the virtual machine. If a virtual machine is already provisioned by the KACE Agent, its name in this column appears as a hyperlink. When you click the link, the page is updated to display device details for the provisioned virtual machine.	HOSTNAME
IP Address	The primary IP address assigned to the virtual machine.	IP

Section or Item	Description	Database field
State	Indicates if the virtual machine is running. Possible values: • **0 - Running**: Virtual machine is running normally. • **1 - Shutting down**: Virtual machine has a pending shutdown command. • **2 – Resetting**: Virtual machine has a pending reset command. • **3 – Pending standby**: Virtual machine has a pending standby command. • **4 – Not running**: Virtual machine is not running. • **5 – Unknown**: Virtual machine information is not available.	MACHINE_VIRTUAL_STATE
Status	The virtual machine status. Possible values: • **0 – OK**: No problems. • **1 – Warning**: Possible problem. • **2 – Error: Definite problems**. • **3 – Unknown**: Status is unknown.	MACHINE_VIRTUAL_STATUS
Hardware Version	The hardware version of a virtual machine reflects the virtual machine's supported virtual hardware features.	HARDWARE_VERSION
Hypervisors	When a vCenter or a SCVMM environment is selected, this group lists the hypervisors managed by vCenter or SCVMM.	
Hostname	The host name assigned to the ESXi host or Hyper-V server. If an ESXi or or Hyper-V device is already added to the inventory, its name in this column appears as a hyperlink. When you click the link, the page is updated to display device details for the selected device.	N/A
Platform	The platform and version of the associated ESXi or Hyper-V hypervisor.	PLATFORM
IP Address	The IP address assigned to the ESXi host.	N/A
Virtual Machines	The number of virtual machines on the ESXi or Hyper-V hypervisor.	N/A
System Serial Number	The serial number of the device hosting the ESXi or Hyper-V hypervisor.	N/A
Status	The ESXi host status.	N/A

Section or Item	Description	Database field
SDA Deployment Information	When you select a device deployed from the KACE System Deployment Appliance (SDA), this group displays the deployment details.	
Deployment Time	The time when the deployment is successfully completed.	SDA_DEPLOYMENT_TIME
Deployment Type	The type of the deployment, such as Scripted Installation, System Image, or Custom Deployment.	SDA_DEPLOYMENT_TYPE
Deployment Name	The name of the deployment, as specified in the KACE SDA.	SDA_DEPLOYMENT_NAME
Deployment URL	The URL to the deployment on the associated KACE SDA.	SDA_DEPLOYMENT_URL
Deployment ID	The ID of the deployment on the KACE SDA.	SDA_SCRIPTED_INSTALLATION_ID
SDA Name	The host name or IP address of the KACE SDA.	SDA_NAME
SDA URL	The URL of the KACE SDA.	SDA_URL
Batteries	This group displays battery information for Windows, Linux and MacOS Agent- and Agentless-managed devices.	
Charge	The percentage of the current battery capacity.	CHARGE_PERCENT
Chemistry	**Windows and Linux devices only**. The battery type, such as Lithium Ion, and so on.	CHEMISTRY
Current Capacity (mWh)	The current battery capacity.	CURRENT_CAPACITY
Design Capacity (mWh)	The maximum capacity of battery by design.	DESIGN_CAPACITY
Full Charge Capacity (mWh)	Current maximum capacity of battery. This value degrades over time.	FULL_CHARGE_CAPACITY
Health (%)	The percentage of the current battery capacity compared to its maximum designed capacity.	HEALTH_PERCENT
Manufacturer	The battery manufacturer.	MANUFACTURER
Name	The battery name or model.	NAME
Plugged In	An indicator of whether the battery is currently plugged into a power source.	PLUGGED_IN

Section or Item	Description	Database field
Recharge Count	**MacOS devices only**. The number of times the battery has been recharged.	RECHARGE_COUNT
Serial Number	The serial number of the battery.	SERIAL
Time Remaining (Minutes)	The number of minutes after which the battery becomes discharged. When the battery is plugged in, this field is blank.	TIME_REMAINING

Software group

Details on the applications installed on the device, including patching information, running processes, and startup programs.

Section	Description	Database field
Installed Programs	A list of the software installed on the device. If change history is enabled for this section, and the information in this section has changed, the **Show Changes** link appears next to the heading. Click **Show Changes** to view only those items that have changed. Click **Hide Changes** to view all items.	N/A
Discovered Software	Discovered applications are executables in the appliance inventory that match the definitions of applications in the Software Catalog. You can enable metering for Discovered applications and suites, mark them as Not Allowed, and add license information for them. In addition, the Discovered application list can be exported in CSV format. You can export the Discovered application list, the Uncataloged list, and the Locally Cataloged list; you cannot export the entire Software Catalog.	N/A
Metered Software	Applications for which metering has been enabled.	N/A
Custom Inventory Fields	A list of Custom Inventory fields for this device, along with the field name and value.	N/A
Uploaded Files	The files that have been uploaded to the appliance from this device using the *upload a file* script action.	N/A
Patches Reported Installed in Software Inventory	Microsoft patches that have been installed on the device. If change history is enabled for this section, and the information in this section has changed, the **Show Changes** link appears next to the heading. Click **Show Changes** to view only those items that have changed. Click **Hide Changes** to view all items.	N/A
Running Processes	A list of processes running on the device. If change history is enabled for this section, and the information in this section has changed, the **Show Changes** link appears next to the heading. Click **Show Changes** to view only those items that have changed. Click **Hide Changes** to view all items.	N/A
Startup Programs	A list of startup programs on the device.	N/A

Section	Description	Database field
	If change history is enabled for this section, and the information in this section has changed, the **Show Changes** link appears next to the heading. Click **Show Changes** to view only those items that have changed. Click **Hide Changes** to view all items.	
Services	A list of services that are running on the device. If change history is enabled for this section, and the information in this section has changed, the **Show Changes** link appears next to the heading. Click **Show Changes** to view only those items that have changed. Click **Hide Changes** to view all items.	N/A

Activities group

Information about actions to be performed on the device.

Section	Description	Database field
Monitoring	Information related to server monitoring, if enabled and if the device's operating system is supported. If the operating system is not supported, that fact is stated in a message. If the device is eligible for monitoring but does not have monitoring enabled, the **Enable Monitoring** button appears.	N/A
Active/Paused	Whether monitoring is enabled for this device.	N/A
Profiles	Any alert criteria profiles that are assigned to this device.	N/A
Maintenance Windows	Any Maintenance Windows that are assigned to this device.	N/A
Level/Alert	Alerts that are active for this device, with icons indicating the level of alert.	N/A
Labels	The labels assigned to this device. Labels are used to organize and categorize inventory and assets.	N/A
Failed Managed Installations	A list of Managed Installations that have failed to install. To access details of the Managed Installations, click the **Managed Installation Detail** link.	N/A
Managed Install List	A list of Managed Installations that are scheduled to be sent to the device the next time it connects with the appliance.	N/A
Service Desk Tickets	A list of the tickets associated with this device. These can either be tickets assigned to the device owner or tickets submitted by the device owner. To view ticket details, click the ticket ID (for example, TICK:0032).	N/A
SNMP Inventory Configurations	A list of SNMP Inventory Configurations associated with this device. To access details of the configurations, or	N/A

Section	Description	Database field
	to add configurations, click **Manage Associated SNMP Configurations**.	

Security group

Information related to patching and device vulnerabilities.

Section	Description	Database field
Patching Detect/ Deploy Status	A list of the patches detected and deployed on the device. If patch attempts have been made, but they have failed, you can click **Reset Tries** to reset the number of patch attempts to the maximum allowed.	N/A
Threat Level 5 List	Threats that are harmful to applications, processes, startup items, or services on the device.	N/A
Windows Feature Update Status	A list of the Windows Feature Update tasks detected and deployed on the device. If updates attempts have been made, but they have failed, you can click **Reset Tries** to reset the number of patch attempts to the maximum allowed.	
Linux Package Repository Information	A list of URL to the device-associated Linux package repositories.	N/A
Linux Package Upgrades Status	A list of the patches detected and deployed on the device. If patch attempts have been made, but they have failed, you can click **Reset Tries** to reset the number of patch attempts to the maximum allowed.	N/A
Microsoft Defender	A list of the Microsoft Defender components and their properties, including its summary, antimalware, antispyware, and antivirus, antivirus network inspection, real-time protection, and tamper protection.	N/A
Microsoft Defender Threat History	A list of the threats detected by Microsoft Defender. For each threat, the list displays its name, the date and time it was first detected, the severity, whether the threat is quarantined, and if the threat is launched and active. For additional details, click a threat, and in the dialog box that appears, you can review the threat category, type, launch status, detection source, and the affected files.	N/A

Dell Command | Monitor group

Additional inventory information about selected Dell client systems using Dell Command | Monitor.

Section	Description	Database field
Alerts	DCM log entries. These can indicate hardware errors detected by firmware.	N/A

Section	Description	Database field
Hardware	Collected information that includes detailed battery specs and usage data, service processor presence and configuration, memory inventory, and attached Dell monitors.	N/A

For classes and properties queried by the appliance using Dell Command | Monitor, see .

Dell Updates group

Information regarding updates and inventory (for Dell devices only).

Section	Description	Database field
Dell Updates Detect/ Deploy Status	A list of the Dell Updates detected and deployed on the device, and any related schedules. If update attempts have been made, but they have failed, you can click **Reset Tries** to reset the number of update attempts to the maximum allowed.	N/A

Logs and Diagnostics group

Information related to appliance records.

- **Management Service Logs**: The primary role of appliance Management Service is to run the offline KScripts. The Management Service logs display the steps performed by Management
- Service to run the offline KScripts. These steps include, downloading dependencies and validating the KBOTS file. Any error in the execution of offline KScript is logged in the Management Service logs.
- **Bootstrap Logs**: The appliance sends a bootstrap request to get inventory information for devices that have checked in for the first time. The logs related to this request are displayed in Bootstrap logs.
- **Client Logs**: The appliance sends a request to the Agent to get inventory information periodically. A script runs on the device, then sends the inventory information to the appliance and inventory is uploaded to the appliance. The Agent logs display these actions.
- **Scripting Updater**: A request is initiated periodically from the device to get the latest information related to the changes in offline KScripts. Scripting Updater logs display this information.
- **Agentless Inventory Status Messages**: The log displays messages related to collecting and submitting inventory data from Agentless-managed devices.
- Splashtop streamer logs: Splashtop-related log files are uploaded to the server. Reviewing these logs helps identify, analyze, and resolve remote control failures efficiently.

Section	Description	Database field
Agent Logs	The logs for the KACE Agent.	N/A
Agent Diagnostic Files	Files uploaded by selecting **Choose Action** > **Upload Agent Files** on this page.	N/A
User Console Installation Logs	Details about **User Console** packages installed on this device.	N/A
Scripting Logs	Scripts, such as Configuration Policy scripts, that have run on this device, along with the available status of any scripts in progress.	N/A

Section	Description	Database field
Server-side Device Log Data	Log entries for the selected device. This section shows the last five entries of each related log, allowing you to troubleshoot any existing issues.	N/A
Device Activity	**Chrome devices only**. It shows the date the device was last active, the length of time the device was active for, and the activity history. Each entry in the activity history shows the date and length or each user session.	N/A

Asset group

This section displays the details of the Asset associated with this device. Clicking the **Edit this Asset** link enables you to edit the asset information.

Section	Description	Database field
Asset Information	Details such as the date and time the record was created and last modified; the Asset Type, such as device; and the name of the asset.	N/A
Barcodes	Barcodes associated with this asset, if they exist.	N/A
Related Assets	Assets that are related to this asset, such as parent or child assets.	N/A
Task History	A list of tasks that have run on the device.	N/A

About Dell Data Protection | Encryption (DDP|E) and encryption information in device details

If devices in the network have the DDP|E client installed, the appliance can collect status and configuration information and display it on the *Device Detail* page.

Registry key needed to be set on Windows DDP|E client

A requirement for the appliance being able to collect detailed inventory from Windows DDP|E clients is to set the `DumpXmlInventory` key in the client.

```
Key: HKLM\SYSTEM\CurrentControlSet\services\DellMgmtAgent\Parameters
DWORD Value: DumpXmlInventory
Data: 0x1
```

This registry value causes DDP|E to write an `inventory.xml` file to the target device, which is then parsed by inventory. See Add a Dump Inventory registry key to permit inventory collection on Windows DDP|E client devices.

This requirement applies only to Windows.

Dell Data Protection | Encryption (DDP|E)

DDP|E consists of applications that enable a user to:

- Detect data security risks on desktops, laptops, and external media.
- Protect data on these devices by enforcing access control policies, authentication, and encryption of sensitive data.
- Manage data centrally with policies using collaborative tools that integrate into existing user directories.
- Support key and data recovery, automatic updates, and tracking for protected devices.

Table 11. Supported OSs for DDP|E

Operating system	Versions
Windows	7, 8, 8.1
Mac OS X	10.7.5, 10.8.3–10.8.5, 10.9.2–10.9.3

Table 12. DDP|E information displayed on the Device Detail page

Item	Description	MACHINE_DDPE Database field
Unique ID	An identification of the DDP|E client used by the DDP|E server.	MCID
Agent Version	Version of DDP|E client installed.	AGENT_VERSION
Server Hostname	Hostname of the DDP|E server managing this DDP|E client.	SERVER_HOSTNAME
Protection Status	Example values are *Protected* and *Unprotected*. Values of *Locked* or *Unknown* might indicate a problem.	PROTECTION_STATUS
Last Inventory Generated	Timestamp of when the last DDP|E client inventory occurred. Not to be confused with K1 inventory.	PROTECTION_STATUS_UPDATED

Table 13. DDP|E Volume information displayed on the Device Detail page

Item	Description	MACHINE_DDPE_VOLUME Database field
Device	Name of the device/volume as reported by the operating system.	DEVICE_ID
Protection Status	Indication of the current level/status of DDP|E protection on the DDP|E client.	PROTECTION_STATUS
Protection Reason	Manner of protection used on the DDP|E client. The option is typically *VendorProtected*, which indicates DDP|E or BitLocker.	PROTECTION_REASON

BitLocker

BitLocker is a full disk encryption feature included with Windows.

Table 14. Supported OSs for BitLocker

Operating system	Versions
Windows	Vista, 7 (Enterprise and Ultimate)
Windows	8, 8.1 (Pro and Enterprise)
Windows server	2008, 2008 R2, 2012, 2012 R2

Table 15. BitLocker information displayed on the Device Detail page

		MACHINE_BITLOCKER_VOLUME
Item	**Description**	**Database field**
Device ID	Unique identifier for the volume on the system.	DEVICE_ID
Persistent Volume ID	A persistent identifier for the volume on the system.	PERSISTENT_VOLUME_ID
Protection status	Denotes whether BitLocker is protecting the volume. • Protection Off • Protection On • Protection Unknown	PROTECTION_STATUS
Metadata Version	Possible values: • 0 • 1 • 2	VERSION
Encryption Method	Type of encryption used. For example, *AES-128*. Possible values: • None • AES-128 with Diffuser • AES-256 with Diffuser • AES-128 • AES-256 • Encrypted • Unknown	SELF_ENCRYPTION_DRIVE _ENCRYPTION_METHOD (self-encrypting drives only) ENCRYPTION_METHOD (software-based encryption only)

Item	Description	MACHINE_BITLOCKER_VOLUME Database field
Hardware Encryption Status	**NOTE:** The Hardware Encryption Status property is supported on Windows 8 and higher systems. Possible values: • Unknown • Not Supported • No Protection • Uses Software • Uses Hardware	HARDWARE_ENCRYPTION_STATUS
Lock Status	Possible values: • Unknown • Unlocked • Locked	LOCK_STATUS
Conversion Status	Status of the conversion. Possible values: • Unknown • Fully Decrypted • Fully Encrypted • Encryption In Progress • Decryption In Progress • Encryption Paused • Decryption Paused	CONVERSION_STATUS
Encryption Percentage	The extent of conversion, shown as a percentage.	ENCRYPTION_PERCENTAGE
Wiping Status	Status of any wiping of free space. Possible values: • Unknown • Free Space Not Wiped • Free Space Wiped • Free Space Wiping In Progress • Free Space Wiping Paused	WIPING_STATUS
Wiping Percentage	The extent of free space wiping, shown as a percentage.	WIPING_PERCENTAGE

Item	Description	MACHINE_BITLOCKER_VOLUME Database field
Key Protectors	Key protectors in place. Possible values: • Unknown • Trusted Platform Module (TPM) • External Key • Numerical Password • TPM and PIN • TPM and Startup Key • TPM and PIN and Startup Key • Public Key • Passphrase • TPM Certificate • CryptoAPI Next Generation (CNG) Protector	KEY_PROTECTORS

FileVault 2

FileVault 2 is a full disk encryption feature included with Mac OS X.

Table 16. Supported OSs for FileVault 2

Operating system	Versions
Mac OS X	10.8, 10.9, 10.10

Table 17. FileVault 2 information displayed on the Device Detail page

Item	Description	MACHINE_FILEVAULT_VOLUME Database field
Enabled	Indicates if FileVault is enabled.	IS_ENABLED
Personal Recovery Key	Indicates the existence of a Personal Recovery Key.	HAS_PERSONAL_RECOVERY_KEY
Institutional Recovery Key	Indicates the existence of a corporate-provisioned X.509-based asymmetric key pair.	HAS_INSTITUTIONAL_RECOVERY_KEY
Authorized Users	A list of accounts that can unlock the drive in EFI.	AUTHORIZED_USERS
Conversion Status	The status of the encryption process. Examples include *Pending Conversion*, *Converting*, *Encryption Paused*, and *Complete*.	CONVERSION_STATUS
Conversion Percentage	The extent of conversion, shown as a percentage.	CONVERSION_PERCENTAGE

Item	Description	MACHINE_FILEVAULT_VOLUME Database field
Encryption Status	Status of the encryption. For example, *Locked* or *Unlocked*.	ENCRYPTION_STATUS
Encryption Type	Type of encryption used. For example, *AES-XTS*.	ENCRYPTION_TYPE
Device	Unique identifier for the volume on the system.	DEVICE_ID
Version		VERSION

Trusted Platform Module (TPM)

TPM is a dedicated microprocessor that secures hardware by integrating cryptographic keys into devices.

Table 18. Supported OSs for TPM

Operating system	Versions
Windows	Vista, 7, 8, 8.1
Windows Server	2008, 2008 R2, 2012, 2012 R2

Table 19. TPM information displayed on the Device Detail page

Item	Description	MACHINE_TPM Database field
Manufacturer	Manufacturer of the TPM chip.	MANUFACTURER_ID_TEXT
Manufacturer Version	Version of the TPM chip.	MANUFACTURER_VERSION
Manufacturer Version Info	Additional version information that is specific to the manufacturer.	MANUFACTURER_VERSION_INFO
Specification Version	The version of the Trusted Computing Group (TCG) specification that the TPM supports.	SPECIFICATION_VERSION
Physical Presence Version	The version of the Physical Presence Interface that the device supports. The Physical Presence Interface is a communication mechanism that runs device operations that require physical presence.	PHYSICAL_PRESENCE_VERSION_INFO
TPM Enabled	Step 1 of TPM initialization.	IS_TPM_ENABLED
TPM Activated	Step 2 of TPM initialization.	IS_TPM_ACTIVATED
TPM Owned	Step 3 of TPM initialization.	IS_TPM_OWNED

Add a Dump Inventory registry key to permit inventory collection on Windows DDP|E client devices

If `DumpXmlInventory` is absent on a Windows DDP|E client, the appliance cannot get access to the inventory .xml file in order to collect the relevant field information.

Dell Data Protection | Encryption is installed on the Windows device. Go to http://www.dell.com/support/home/us/en/19/product-support/product/dell-data-protection-encryption/drivers.

The procedure for adding the key is different for Agent-managed devices and Agentless-managed devices.

- Add the DumpXmlInventory registry key to an Agent-managed Windows device
- Add the DumpXmlInventory registry key to an Agentless-managed Windows device

Add the DumpXmlInventory registry key to an Agent-managed Windows device

You must add `DumpXmlInventory` to a Windows DDP|E client before the appliance can collect field information from that client's inventory.xml file.

For Agent-managed Windows devices, you can use a default offline KScript from the appliance scripting feature to set the "dump inventory" registry key. This key is necessary for the DDP|E agent to write the detailed inventory XML data to the appliance file system.

NOTE: After you set the registry key, the DDP|E service requires a full policy update schedule before the appliance is able to collect inventory.

1. Go to the *Script Detail* page for the *K1000 Enable Detailed DDPE Inventory (Windows)* script.
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Scripting**, then click **Scripts**.
    c. From the list, select **KACE SMA Enable Detailed DDPE Inventory (Windows)**.
2. In the *Configure* tab, specify script settings:

Option	Description
Name	*KACE SMA Enable Detailed DDPE Inventory (Windows)*, the name of this default script.
Enabled	Select this check box to run the script on the target devices. Do not enable a script until you are finished testing it and are ready to run it. Enable the script on a test label before you enable it on all devices.
Type	The script type is **Offline KScripts**.
Status	Indicates the readiness of the script to be rolled out to the network. Set the status to **Production**.
Description	Contains the brief description of the actions the default script performs.
Notes	Any additional information you want to provide.

3. In the *Deploy* tab specify deployment options:

Option	Description
All Devices	Deploy to all devices. Clear the check box to limit the deployment to specific labels or devices.
Restrict to Labels	Limit deployment to devices that belong to specified labels. To select labels, click **Edit**, drag labels to the *Limit Deployment to* window, then click **OK**. If you select a label that has a Replication Share or an alternate download location, the appliance copies digital assets from that Replication Share or alternate download location instead of downloading them directly from the appliance. **NOTE:** The appliance uses a Replication Share before it uses the KACE Alt Location.
Devices	Limit deployment to one or more devices. To find devices, begin typing in the field.
Operating Systems	The operating systems on which the application runs. Applications are deployed only to devices with the selected operating systems. 1. Click **Manage Operating Systems**. 2. In the **Operating Systems** dialog box that appears, select the OS versions in the navigation tree, as applicable. You have an option to select OS versions by their family, product, architecture, release ID, or build version. You can choose a specific build version, or a parent node, as needed. Selecting a parent node in the tree automatically selects the associated child nodes. This behavior allows you to select any future OS versions, as devices are added or upgraded in your managed environment. For example, to select all build current and future versions associated with the Windows 10 x64 architecture, under **All** > **Windows** > **Windows 10**, select **x64**.

4. In the *Schedule* tab, specify run options:

Option	Description
None	Run in combination with an event rather than on a specific date or at a specific time.
Every n hours	Run at a specified interval.
Every day/specific day at HH:MM	Run daily at a specified time, or run on a designated day of the week at a specified time.
Run on the nth of every month/ specific month at HH:MM	Run on the same day every month, or a specific month, at the specified time.
Run on the nth weekday of every month/specific month at HH:MM	Run on the specific weekday of every month, or a specific month, at the specified time.

Custom	Run according to a custom schedule.
	Use standard 5-field cron format (extended cron format is not supported):
	`* * * * *`
	`| | | | +————————day of week (0-6)(Sun=0)`
	`| | | +————————month (1-12)`
	`| | +————————day of month (1-31)`

Option	Description

	`| +————————hour (0-23)`
	`+————————minute (0-59)`
	Use the following when specifying values:
	• **Spaces ( )**: Separate each field with a space.
	• **Asterisks (*)**: Include the entire range of values in a field with an asterisk. For example, an asterisk in the hour field indicates every hour.
	• **Commas (,)**: Separate multiple values in a field with a comma. For example, `0,6` in the day of the week field indicates Sunday and Saturday.
	• **Hyphens (-)**: Indicate a range of values in a field with a hyphen. For example, `1-5` in the day of the week field is equivalent to `1,2,3,4,5`, which indicates Monday through Friday.
	• **Slashes (/)**: Specify the intervals at which to repeat an action with a slash. For example, `*/3` in the hour field is equivalent to `0,3,6,9,12,15,18,21`. The asterisk (`*`) specifies every hour, but `/3` restricts this to hours divisible by 3.
	Examples:
	• `15 * * * * Run 15 minutes after every hour every day`
	• `0 22 * * * Run at 22:00 every day`
	• `0 0 1 1,6 * Run at 00:00 on January 1 and June 1`
	• `30 8,12 * * 1-5 Run weekdays at 08:30 and 12:30`
	• `0 2 */2 * * Run every other day at 02:00`

View Task Schedule	Click to view the task schedule. The *Task Schedule* dialog box displays a list of scheduled tasks. Click a task to review the task details. For more information, see View task schedules.

5. Skip the *Dependencies* and *Tasks* tab.
6. Do one of the following:
   - **Click Run Now to immediately push the script to all devices.**

     Use this option with caution. See Using the Run and Run Now commands.
   - **Click Save.**

Add the DumpXmlInventory registry key to an Agentless-managed Windows device

You must add `DumpXmlInventory` to a Windows DDP|E client before the appliance can collect field information from that client's inventory.xml file.

For an Agentless-managed Windows device, the process requires that you create a new Group Policy Object on a Windows Server 2008 or 2012 device so that you can deploy the registry setting to multiple devices in a domain.

1. On a Windows Server 2008 or 2012 device, open the *Group Policy Management Console*.
2. Right-click **Group Policy Objects** and click **New**.
3. Provide a description name for the new GPO (for instance, Dell Data Protection | Encryption: Inventory Registry Setting) and click **OK**.
4. Right-click the new GPO and click **Edit**.
5. Browse to **Computer Configuration** > **Preferences** > **Windows Settings** > **Registry**.
6. Right-click **Registry** and select **New** > **Registry Item**.
7. On the *General* tab, select **Update** in the *Action* drop-down menu.
8. Select **HKEY_LOCAL_MACHINE** in the *Hive* drop-down list.
9. Specify a *Key Path* of `SYSTEM\CurrentControlSet\services\DellMgmtAgent\Parameters`.
10. Specify a *Value* name of DumpXmlInventory.
11. Select **REG_DWORD** in the *Value type* drop-down list.
12. Specify 1 in the *Value* data field.
13. Select the *Hexadecimal* option in the *Base* group, and click **OK**.
14. Close the *Group Policy Management Editor*.

You can now link this new group policy object to a specific domain, Organizational Unit, and so on.

IMPORTANT: You should test the GPO on a specific computer or set of computers before deploying it to all systems.

About Intel AMT information in device details

On Intel-based Windows devices with Intel AMT technology present, the appliance can display information about the AMT configuration.

Intel AMT is hardware-based technology for remotely managing Intel-based computer devices. Intel AMT is a feature of Intel® Core™ processors with Intel® vPro™ technology.

NOTE: The data collection discussed here is separate from the vPro and AMT data that the appliance collects using Dell Command | Monitor. See .

Intel AMT resources and appliance requirements

For information from the Dell Tech Center, go to http://en.community.dell.com/techcenter/enterprise-client/w/wiki/7537.dell-command-intel-vpro-out-of-band. For information and download link for the Intel Setup and Configuration Software (SCS), which contains the components required to configure Intel AMT, go to http://www.intel.com/content/www/us/en/software/setup-configuration-software.html.

In order for the appliance to get access to the complete inventory information on an AMT device, the device must have the Intel Management Engine installed. For driver downloads from Intel, go to https://downloadcenter.intel.com/search?keyword=intel+management+engine.

Intel AMT information

Table 20. Intel AMT information displayed on the Device Detail page

Item	Description	MACHINE_INTEL_AMT Database field
SKU	The Stock Keeping Unit of the device. Possible values are: • Full AMT Manageability • Standard Manageability	SKU
Status	Indicates whether AMT is configured on the device.	STATE IS_AMT_CONFIGURED
Configuration Mode	The current configuration mode of the AMT device. Possible values are: • SMB Mode • Enterprise Mode • None	CONFIGURATION_MODE
Control Mode	The current Control Mode of the AMT device. Possible values are: • Client control Mode • Admin Control Mode • None	CONTROL_MODE
Firmware Version	The version of firmware in the AMT device.	FW_VERSION
MEI Driver	Indicates if the MEI driver is installed and working, and if so, the version of the driver.	IS_MEI_ENABLED MEI_VERSION

Finding and managing devices

Use Advanced Search, labels, and alerts to find and manage devices in inventory.

Finding devices in inventory

Advanced Search enables you to specify values for any field present in the inventory record and search the entire inventory for those values.

This type of search is useful when you want to find devices with specific characteristics, such as a particular BIOS version, MAC address, or operating system. See Searching at the page level with advanced options.

You can also run a simple search to quickly find a specific device. For example, you can look for a device whose barcode contains specific characters.

Using alerts to find devices

You can configure alerts to automatically send email messages to administrators when devices meet the criteria you select. For example, if you want to notify administrators when devices approach disk space limits, you can set up email alerts based on disk usage. See Add notification schedules from the Reporting section.

Filtering devices by Organizational Unit

To filter devices based on Organizational Units found in LDAP or Active Directory servers, you can use LDAP Labels. See About LDAP Labels.

Labeling devices to group them

You can use manual labels and Smart Labels to group devices. Doing so makes it possible to perform actions, such as updating software, on devices as a group.

To enable the metering of Software Catalog applications, you must apply a metering-enabled label to the devices on which the applications are installed. For more information about metering, see Using software metering.

Add, apply, and remove manual device labels

You can add manual labels and apply them to, or remove them from, devices. Manual labels remain associated with devices until the labels are manually removed from devices.

1. Go to the *Devices* list:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Inventory**, then click **Devices**.
2. Select the check boxes next to one or more devices.
3. Select **Choose Action** > **Add Label**.
4. In the *Add Label* text box, enter a name for the label.

    TIP: Avoid using backslashes (\) in label names. If you need to use a backslash in a label name, add a second backslash (\\) to escape it.

5. Click **Add Label**.
6. To apply an existing label:
    a. Select the check box next to one or more devices.
    b. Select **Choose Action** > **Apply Labels**.
    c. Drag labels into *Apply these labels*, then click **Apply Labels**.

    The label appears next to the device name on the *Devices* list.
7. To remove a manual label:
    a. Select the check box next to one or more devices.
    b. Select **Choose Action** > **Remove Label** > **Label_Name**.

    The label is removed from the devices.

Using Smart Labels for devices

Use Smart Labels to find and label devices automatically based on specified criteria.

For example, to track laptops in a specific office, you could create a label called “San Francisco Office,” and create a Smart Label based on the IP address range or subnet for devices located in the San Francisco office. Whenever a device that falls within the IP address range is inventoried, the Smart Label “San Francisco Office” is automatically applied. When the device leaves the IP address range, and is inventoried again, the label is automatically removed.

Smart Labels are applied to and removed from managed devices when the appliance processes device inventory. So if you create a Smart Label that enables metering on devices, it might take time for the Smart Label to be applied to devices and for devices to report metering information. Metering is enabled for devices that match the Smart Label criteria only after devices are inventoried and the Smart Label is applied.

For more information, see Managing Smart Labels.

The following table lists examples of useful Smart Labels that can be applied to devices based on inventory attributes:

Sample Label Name	Sample Criteria
Win7 Low Disk	Windows 7 devices with less than 1 GB of free hard disk space
WS2012 No 2916993	Windows Server 2012 devices without Hotfix 2916993 installed
Building 3	Devices in an IP address range known to originate in Building 3
CN Sales	Devices whose device name contains the word **sales**

Run actions on devices

You can use Device Actions to run actions on devices remotely, provided that those programs are installed on the remote devices.

You have created Device Actions from which to choose. For information on adding or editing Device Actions, see Configure appliance General Settings without the Organization component.

NOTE: This feature is only supported on Windows devices. The Windows device you are running the device action from must have the KACE Agent version 9.0 or later agent installed and connected.

NOTE: When you initiate device through the agent, the action executable must be placed in your `%PATH%`. The agent is 32-bit, so on 64-bit Windows devices, use `%windir%/System32` as an alias to the `%windir%/Wow64` directory. If you need to run a program that's located in the `%windir%/System32` directory on a 64-bit Windows system, you must use the `%windir%/SysNative` virtual directory. You can either add `%windir%/SysNative` to your `%PATH%` environment variable or provide a fully-qualified path by prepending `%windir%/SysNative` to your executable when defining your machine action.

1. Go to the *Device Detail* page for a device:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Inventory**, then click **Devices**.
    c. On the *Devices* list, in the row that contains the required device, select the check box.
2. Select an action in the *Actions* drop-down list.

NOTE: If no Device Actions have been created, the *Actions* drop-down list does not appear.

TIP: Assigning devices to a user (**Choose Action > Assign To**) causes all of the assigned devices to appear listed for the selected user on the *My Devices* page in the **User Console**. When the user attempts to download and install software, they can select a target device, as required.

View devices that have been added manually

Devices that have been added manually appear on the *Devices* list along with other managed devices. You can use Advanced Search to filter the *Devices* list to show only those devices that have been added manually.

1. Go to the *Devices* list:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Inventory**, then click **Devices**.
2. To filter the list to show only those devices that have been added manually:
    a. Click the **Filter** tab above the list on the right to display the *Filter* panel.
    b. Specify the criteria required to find devices that have been added manually:

Option	Criteria
Field Name	Device Identity Information: Inventory Type
Operator	is
Value	Choose one of the following: • **Wsapi Agent**: Inventory uploaded through the API. • **XML Import**: Inventory uploaded on the *Software Detail* page.

    c. Click **Search**.

Devices that have been added manually are displayed.

Delete devices from inventory

If you have unused or obsolete devices in inventory, you can delete them manually. This deletion prevents the devices from being counted toward the number of devices you are allowed to manage through your Quest KACE license.

1. Go to the *Devices* list:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Inventory**, then click **Devices**.
2. Select the check box next to one or more devices.
3. Select **Choose Action** > **Delete**, then click **Yes** to confirm.

Registering KACE Agent with the appliance

The appliance uses a registration process to prevent unauthorized access to its resources. Only authenticated KACE Agents can establish a successful connection.

Any Agents that attempt to connect to the appliance are placed on a quarantine list. If an Agent has a valid token, the appliance authenticates the Agent and automatically grants access to the appliance. Agents that do not have a token remain in the quarantine until a system administrator approves their connection request.

You can create and manage Agent tokens, and manage requests from quarantined Agents to connect to the appliance.

Manage KACE Agent tokens

KACE Agent tokens enable the appliance to authenticate and register Agents, allowing them to access the appliance resources.

Each token can be associated with one or more Agents. Use the *Agent Token Detail* page to create or modify Agent tokens. This page also identifies all devices that used a specific token to connect to the appliance, and allows you to download Agent installers that include the selected token.

Any Agents that do not have a valid token must be approved by the appliance administrator in order to establish a successful connection. For more information, see Review quarantined KACE Agents.

1. Do one of the following:
   - **Log in to the appliance Administrator Console, `https://appliance_hostname/admin`. Or, if *Show organization menu in admin header* is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.**
   - **Log in to the appliance System Administration Console, `https://appliance_hostname/system`, or select System from the drop-down list in the top-right corner of the page.**

   The *Dashboard* or *System Dashboard* page appears.
2. Go to the *Agent Token Detail* page:
   a. On the left navigation bar, click **Settings**, then click **Agent Tokens**.

   The *Agent Tokens* page appears, displaying the list of all Agent tokens. For each token, it shows a token status, the name of the user who created it, expiration date (if applicable), the number of times the token is used to register an Agent device with the appliance, and the usage limit (if applicable).
3. On the *Agent Tokens* list page that appears, complete one of the following steps:
   - **To create a new Agent token, click Choose Action > New.**

     TIP: To delete or revoke one or more tokens, select them in the list, and use the applicable commands from the **Choose Action** menu. You can also perform this action on the *Agent Token Detail* page.
   - **To edit an existing Agent token, click the token name in the list.**
4. On the *Agent Token Detail* page that appears, under *Configuring*, provide the following information:

Option	Description
Name	The name of the Agent token. Choose a name that you can easily recognize and associate with a specific agent, platform, or purpose.
Expires	If you want this token to be valid for a limited time, select **Enable Expiration**, and specify the expiration date and time, as required. To change the specified date and time, click **Clear**, and provide the new expiration deadline.
Organization	The name of the organization that uses this token. You can select one specific organization, or apply to all organizations by selecting *All Orgs*. **NOTE:** This field only appears if you are using the **System Administration Console**.

5. If you want to specify the number of times the token can be used to register one or more agents with the appliance, under *Use Limit*, select **Enable Use Limit**, and in the field that appears, specify the maximum use count.

Unless an agent's history is deleted from the appliance, the agent registers with the appliance only once, so this number represents the total number of times one or more agents can register with the appliance.

6. Click **Save**.

   If you created a new Agent token, the page displays some additional sections: *Information*, *Agent Token Bundle Installers*, **and** *Token Usage by Machines*, **and** *Token Usage by Provisioning Schedules*.

7. **Optional**. Review the contents of the following sections:

Section	Description
Information	General information about the Agent token, such as when it was created, last modified, the name of the user who created it, its status, and the token string. To copy the token string to clipboard, in the *Token* field, click the icon. You can specify the token string while installing the KACE Agent on a target device. For more information about agent installation, see Manually deploying the KACE Agent.
Agent Token Bundle Installers	Links to KACE Agent installers for each supported operating system. Each installer bundle includes this Agent token.
Token Usage by Machines	A list of devices in the appliance inventory that use this Agent token, and the date and time the appliance administrator approved access for each device.
Token Usage by Provisioning Schedules	A list of provisioning schedules that use this Agent token. For each entry, the list indicates the IP range and whether the schedule is enabled.

Review quarantined KACE Agents

The appliance keeps track of any agents that request a connection to the appliance.

In a default view, the *Quarantine* list page only shows the Agents that are waiting for registration. You can use it to review and register applicable Agents. To display already connected Agents, simply change the list filter.

NOTE: On the *Quarantine* list page, the *Zone* column shows each agent as *Internal* or *External*. If you configure your firewall to map port 443 externally to port 52230 of the appliance, Agents that connect through the firewall to port 443 show up as External on this page. Agents that connect directly to the appliance's port 443 appear as Internal. This feature is optional, but you can use it, for example, if the appliance is hosted in a perimeter network. For more details. see https://go.kace.com/to/k1000-external-agent-port.

Agents that include a valid token are automatically connected. For more information about tokens, see Manage KACE Agent tokens.

1. Go to the *Quarantine* list page by doing one of the following:

   - **If your appliance has the Organization component enabled, and you want to access a System-level quarantine list:**

     Log in to the appliance System Administration Console, `https://`**appliance_hostname**`/system`, or select **System** from the drop-down list in the top-right corner of the page. Then select **Organizations** > **Quarantine**.
     A System-level quarantine list includes the Agents associated with all organizations managed by the appliance.

   - **If your appliance does not have the Organization component enabled, or if you want to access an organization-level quarantine list, log in to the appliance Administrator Console, `https://`appliance_hostname`/admin`. Or, if the** *Show organization menu in admin header* **option is**

enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information. Then select Inventory > Quarantine.

An organization-level quarantine list includes only the Agents associated with the selected organization.

The *Quarantine* list page appears. By default, the list uses the *Awaiting Action* filter, showing only those Agents that require approval. You can apply different filters to display *All Items*, and *Approved* or *Blocked Agents*. When you display the *Approval Status* column you can see which agents are *Approved*, *Blocked*, and *Awaiting Action*.

2. Review the items in the list and approve any Agents, as required.

   To approve one or more Agents, select them in the list, and click Choose Action > Approve. You can also block or delete Agents, as required. Blocking a quarantined agent only removes it from the *Awaiting Action* view on the *Quarantine* list page. You can block an agent that you do not want to consider approving, in general. To remove a blocked agent from all views, you may want to delete it. A blocked agent reappears on the *Awaiting Action* view if it attempts a re-connection. For example, if you see a suspicious host name coming from an external agent, you can either block or delete that agent. Blocked status is intended to be a permanent list of blocked devices that stay hidden from Awaiting Action view, that are not intended to be approved at any point.

3. To find out more about a quarantined Agent:
   a. Click the Agent's name in the list.
   b. On the *Quarantine Detail* page that appears, review the Agent's details.

      This page shows the details about the selected KACE Agent, such as the name of the device on which the Agent is installed, the device's MAC address, and so on. If the Agent used a token to connect to the appliance, the token name appears on the page. This page also allows you to approve, block, or delete Agents.

   c. When done, click **Cancel**.
4. **System-level Agents only**. If you want to associate a System-level Agent with a specific organization, select it in the list and click **Choose Action** > **Assign to Organization** > **<*organization name*>**

   The selected Agent record now appears in the organization-level *Quarantine* list page, allowing the organization's administrator to review and register this Agent, as applicable. If an Agent is approved without being assigned to an organization, Organization filters are used to assign the agent to an organization after its first inventory.

Provisioning the KACE Agent

Agent provisioning is the task of installing the KACE Agent on devices you want to add to appliance inventory using the Agent.

About the KACE Agent

The KACE Agent is an application that can be installed on devices to enable inventory reporting and other device management features.

Agents that are installed on managed devices communicate with the appliance through an agent messaging protocol. Agents perform scheduled tasks, such as collecting inventory information from, and distributing software to, managed devices. Communication between an Agent and the appliance occurs over a proprietary KACE tunnel which is encrypted using the TLS 1.3 protocol. The agent sends and receives unencrypted data through the TLS 1.3-encrypted KACE tunnel.

Agentless management is available for devices that cannot have Agent software installed, such as printers and devices with operating systems that the Agent does not support. See Using Agentless management.

Tracking changes to Agent settings

If History subscriptions are configured to retain information, you can view the details of the changes made to settings, assets, and objects.

This information includes the date the change was made and the user who made the change, which can be useful during troubleshooting. See About history settings.

Methods for provisioning the KACE Agent

You have a number of ways to deploy the KACE Agent to the devices you want to manage.

- **Provision using the Agent Provisioning Assistant**: You can use the Agent Provisioning Assistant to perform provisioning for devices with Windows, Mac OS X, and Linux operating systems. Within the Assistant, you can choose between using the appliance GPO Provisioning Tool for deploying the Agent to Windows devices, or using Onboard Provisioning for deploying the Agent to Windows, Mac OS X, or Linux devices.

  The GPO Provisioning Tool is recommended for Windows devices because using the tool minimizes the pre-configuration that must happen on the target device. It requires an Active Directory environment. The onboard provisioning approach requires you to perform client-side configuration on the devices to be managed before you can start provisioning.

- **Provision using manual deployment**: Manual deployment is useful when automated Agent provisioning is not practical or when you want to deploy the KACE Agent using email or logon scripts.

Related topics

Provisioning the KACE Agent using the GPO Provisioning Tool for Windows devices

Provisioning the KACE Agent using onboard provisioning

Manually deploying the KACE Agent

Enabling file sharing

To provision Agent software, you must enable file sharing.

If the Organization component is enabled on your appliance, see Enable file sharing at the System level. Otherwise, see Enable file sharing without the Organization component enabled.

Enable file sharing at the System level

If the Organization component is enabled on your appliance, you must enable file sharing at the System level to provision the Agent.

NOTE: If the Organization component is not enabled on your appliance, follow the instructions in Enable file sharing without the Organization component enabled.

1. Go to the *Security Settings* page:
   a. Log in to the appliance System Administration Console, `http://`**appliance_hostname**`/system`, or select **System** from the drop-down list in the top-right corner of the page.
   b. On the left navigation bar, click **Settings**, then click **Control Panel**.
   c. On the *Control Panel*, click **Security Settings**.
2. In the *Samba* tab, specify the following settings:

Option	Description
For appliances with the Organization component enabled: **Enable Organization File Shares**	Use the appliance's client share to store files, such as files used to install applications on managed devices. The appliance's client share is a built-in Windows file server that the provisioning service can use to assist in distributing the Samba client on your network. Quest recommends that this file server only be enabled when you perform application installations on managed devices.
Require NTLMv2 authentication	Enable NTLMv2 authentication for the appliance files shares. When this setting is enabled, managed devices connecting to the appliance File Shares require support

Option	Description
to appliance file shares	for NTLMv2 and authenticate to the appliance using NTLMv2. Even though NTLMv2 is more secure than NTLM and LANMAN, non-NTLMv2 configurations are more common and this option is usually turned off. Enabling this option disables **lanman auth** and **ntlm auth** on the Samba server. NTLMv2 Levels 1-4 are supported. If you need NTLM v2 Level 5, consider manually provisioning the KACE Agent. See Manually deploying the KACE Agent.
Require NTLMv2 to off-board file shares	Force certain appliance functions that are supported through the Samba client, such as Agent Provisioning, to authenticate to offboard network file shares using NTLMv2. Even though NTLMv2 is more secure than NTLM and LANMAN, non-NTLMv2 configurations are more common and this option is usually disabled. Enabling this option enables the **client ntlmv2 auth** option for Samba client functions.

3. Click **Save**.
4. If prompted, restart the appliance.

When the appliance restarts, enable file sharing at the organization level. See Enable organization-level file sharing with the Organization component enabled.

Enable organization-level file sharing with the Organization component enabled

If the Organization component is enabled on your appliance, you must enable file sharing at the organization level to provision the Agent.

Verify that organization file shares are enabled. For instructions, see Enable file sharing at the System level.

1. Go to the Admin-level *General Settings* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Settings**, then click **Control Panel**.
    c. On the *Control Panel*, click **General Settings**.
2. Select **Enable File Sharing** in the *File Sharing* tab.

    If File Shares are disabled, you must enable them at the System level. See Configure security settings for the appliance.

3. **Optional**: Enter a password for the File Share User.
4. Click **Save**.
5. If prompted, restart the appliance.
6. If you have multiple organizations, repeat the preceding steps for each organization.

Enable file sharing without the Organization component enabled

If the Organization component is not enabled on your appliance, you must enable file sharing in the appliance security settings to provision the Agent.

1. Go to the *Security Settings* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Settings**, then click **Control Panel**.
    c. On the *Control Panel*, click **Security Settings**.
2. In the *File Sharing* tab, select **Enable File Sharing**.
3. **Optional**: Select authentication options:

Option	Description
Require NTLMv2 to authenticate appliance file shares	Enable NTLMv2 authentication for the appliance files shares. When this setting is enabled, managed devices connecting to the appliance File Shares require support for NTLMv2 and authenticate to the appliance using NTLMv2. Even though NTLMv2 is more secure than NTLM and LANMAN, non-NTLMv2 configurations are more common and this option is usually turned off. Enabling this option disables **lanman auth** and **ntlm auth** on the Samba server. NTLMv2 Levels 1-4 are supported. If you need NTLM v2 Level 5, consider manually provisioning the KACE Agent. See Manually deploying the KACE Agent.
Require NTLMv2 authentication to off-board file shares	Force certain appliance functions that are supported through the Samba client, such as Agent Provisioning, to authenticate to offboard network file shares using NTLMv2. Even though NTLMv2 is more secure than NTLM and LANMAN, non-NTLMv2 configurations are more common and this option is usually disabled. Enabling this option enables the **client ntlmv2 auth** option for Samba client functions.

4. Click **Save**.
5. If prompted, restart the appliance.

Provisioning the KACE Agent using the GPO Provisioning Tool for Windows devices

Of the methods for provisioning the Agent on Windows devices, Quest recommends the GPO Provisioning Tool because using the tool minimizes the pre-configuration that must happen on the target devices.

The GPO Provisioning Tool uses Active Directory® and Group Policy to distribute the installation settings and to perform the installation of the Agent. The tool creates a GPO, or modifies a pre-existing GPO to install the KACE Agent when a device authenticates with Active Directory.

The first time a target device refreshes Group Policy after the tool has completed the creation or modification process, a new Group Policy client-side extension dll is registered on the devices applying this GPO. Then the next time that the device refreshes Group Policy, Windows triggers the newly registered client-side extension to install the KACE Windows Agent.

For the Quest Knowledge Base article that contains the link to download the GPO Provisioning Tool, go to https://support.quest.com/kb/133776.

Prepare to use the GPO Provisioning Tool for Agent deployment

Before you can use the GPO Provisioning Tool to deploy Agents to Windows devices, you must ensure that your system is configured to use the tool.

The following system requirements are necessary for using the GPO Provisioning Tool:

- **Windows 7 and higher**: **Remote Server Administration Tools** (RSAT) enables IT administrators to remotely manage roles and features in Windows Server 2016, Windows Server 2012 R2, or Windows Server 2012, from a computer that is running Windows 8.1, Windows 8, or Windows 7.

  Go to 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 or higher Active Directory Functional Level**.
- **Distribution Share**: Make sure to use a share that everyone can access. For example, do not place the `.msi` file on the NETLOGON share, because not every user can reach that share and the lack of access will cause your upgrade to fail in the future. This location should be a permanently accessible share. The installer is an MSI (Microsoft Installer) file. To uninstall or upgrade software, MSI needs access to the `.msi` file. If it is not accessible, `msiexec` will not uninstall.

Provision KACE Agents using the appliance GPO Provisioning Tool

You can install the KACE Agent on a single device, or on multiple devices by using the appliance GPO Provisioning Tool, starting within the Agent Provisioning Assistant. You can use this method to provision Windows devices.

- You have an Active Directory environment.
- You have appropriate access to set up software installations.
- You have met the system requirement spelled out in Prepare to use the GPO Provisioning Tool for Agent deployment.

To complete this task, you leave the appliance to work in the Windows Group Policy Management Console or the Windows Administrative Tools using the appliance GPO Provisioning Tool before returning to the appliance.

1. Go to the Agent Provisioning Assistant:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Settings**, then click **Provisioning**.
    c. On the *Provisioning* panel, click **Agent Provisioning Assistant**.

    The *Agent Provisioning Assistant: Step 1 of 3* page appears.
2. Select the check box for *Provisioning Using Windows Group Policy (recommended)*, and click **Next** to display the *Agent Provisioning Assistant: Step 2 of 3* page.
3. Click the link to the Knowledge Base article about using the appliance GPO Provisioning Tool for Agent deployment at https://support.quest.com/kb/133776.

The Knowledge Base article provides a link to download the MSI for the GPO Provisioning Tool.

Installing and starting the tool requires leaving the appliance interface.

4. Download the MSI, and start it to install the tool.
5. Start the installed tool from the **Start** menu.

The deployment wizard leads you through steps to configure and apply a GPO for software deployment. Where possible, the wizard attempts to use defaults that reduce the amount of configuration required.

NOTE: Only GPOs for which you have permission to **edit** are displayed in the tool.

6. Return to the *Agent Provisioning: Step 2 of 3* page in the appliance when you have completed working in the tool, and click **Next**.
7. Click **Finish** on the *Agent Provisioning: Step 3 of 3* page.

Agents are installed on the client devices after the Group Policy is refreshed on those devices. Depending on the environment, this installation takes place either when the device reboots, or after a 90-minute refresh cycle occurs for the Group Policy.

Go to the *Devices* page to keep track of the progress of devices having the agents installed and checked in.

Provisioning the KACE Agent using onboard provisioning

You can install the KACE Agent on multiple devices by specifying a range of IP addresses as targets for deployment (onboard provisioning). Windows, Mac OS X, and Linux devices can be targets for onboard provisioning.

After you have prepared each of your target client devices, you use the Agent Provisioning Assistant in the appliance to identify the devices and set up a provisioning schedule.

Preparing to install the KACE Agent

Before you install the KACE Agent on devices using onboard provisioning, you must verify system requirements, enable file sharing, and prepare devices.

For information on file sharing, see Enabling file sharing.

Verifying system requirements for the KACE Agent installation

Before you install the KACE Agent on devices, verify that the required ports are accessible, and that managed devices meet system requirements.

Managed devices must meet the following system requirements and be able to access the required ports:

- See the *Technical Specifications* available on the product documentation page: https://support.quest.com/kace-systems-management-appliance/technical-documents.
- See Verifying port settings, NTP service, and website access.

Prepare Windows devices to have the Agent installed

Before you install the KACE Agent on Windows devices, you must configure file sharing and User Account Control (UAC) properly.

- **Prepare a Windows 7 or Windows 8 device**

  Provide Administrator credentials for each device. To install the KACE Agent on multiple devices, the Administrator credentials must be the same for all devices.

  To configure User Account Control (UAC), do one of the following:

  # Set **User Account Control: Run all administrators in Admin Approval Mode** to **Disabled**. This option is recommended, because it is more secure and can be centrally configured using GPO. To find this setting, open the **Group Policy** (type secpol.msc into the *Search programs and files* field under the **Start** menu), then go to **Local Policies** > **Security Options**. Restart the device after applying the settings.
  # Disable UAC. On Windows 7, go to **Control Panel** > **System and Security** > **Action Center** > **Change User Account Control Settings**. On Windows 8, go to **Control Panel** > **System and Security** > **Administrative Tools** > **Local Security Policy**, then in *Security Options* in the *Local Policies* section choose **Disabled** for each of the items labeled *User Account Control*.

  On the *Advanced Sharing Settings* page, enable network discovery and file and printer sharing.

- **Prepare Windows Firewall**

  If Windows Firewall is enabled, you must enable File and Print Sharing in the *Exceptions* list of the Firewall Configuration. For instructions, see the Microsoft Support website.

- **Verify port availability**

  Verify the availability of ports 139 and 445.

  The appliance verifies the availability of ports 139 and 445 on target devices before attempting to run any remote installation procedures.

  NOTE: On Windows devices, ports 139 and 445, File and Print Sharing, and Administrator credentials are required only during Agent installation. You can disable access to these ports and services after installation if necessary. The Agent uses port 443 for ongoing communications.

  NOTE: After installation, the Agent runs within the context of the Local System Account, which is a built-in account used by Windows operating systems.

Install the KACE Agent on a device or multiple devices

You can install the KACE Agent on a single device, or on multiple devices by specifying a range of IP addresses as targets for installation, using the Agent Provisioning Assistant. You can use this method to provision Windows, Mac, or Linux devices.

- You have prepared all the target devices. See Preparing to install the KACE Agent.
- You have information for the administrator account that has the necessary privileges to install Agents on the target devices.

With the Agent Provisioning Assistant, you can create provisioning schedules to specify how and when to install the KACE Agent on devices in your network. Provisioning according to a schedule is useful to help ensure that devices in an IP address range have the Agent installed.

Provisioning schedules configure the appliance to periodically check devices in a specified IP address range and install, reinstall, or uninstall the KACE Agent as needed.

For provisioning Windows devices, you can also use the appliance GPO Provisioning Tool. Using the tool minimizes the pre-configuration that must happen on the target device. See Provisioning the KACE Agent using the GPO Provisioning Tool for Windows devices.

1. Go to the Agent Provisioning Assistant:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Settings**, then click **Provisioning**.
    c. On the *Provisioning* panel, click **Agent Provisioning Assistant**.

    The *Agent Provisioning Assistant: Step 1 of 3* **page appears.**
2. Select *Provisioning Using IP Range (Windows, Mac, Linux)* and click **Next** to display the *Provisioning Schedule Detail* page.
3. In the *Configure* section, name the schedule, enable provisioning, and provide platform information:

Option	Description
Name	A unique name that identifies this configuration. The name appears on the *Provisioning Schedules* page.
Enabled	Enable provisioning schedules. Schedules run only if this check box is selected.
Install/Uninstall	Indicates whether the provisioning schedule deals with installing or uninstalling Agents.
Agent Token	The token the Agent uses to connect to the appliance. Select an existing Agent token or add a new one: 1. Select *Add Agent Token*. 2. In the *Add Agent Token* dialog box, provide the following information: # **Name**: # **Enable Expiration**: If you want this token to be valid for a limited time, select this check box, and specify the expiration date and time, as required. To change the specified date and time, click **Clear**, and provide the new expiration deadline. # **Enable Use Limit**: If you want to specify the number of times the token can be used to register one or more agents with the appliance, select this check box, and in the field that appears, specify the maximum use count. Unless an agent's history is deleted from the appliance, the agent registers with the appliance only

Option	Description
	once, so this number represents the total number of times one or more agents can register with the appliance. 3. Click **Save**. If you do not select an Agent token, when the Agent connects to the appliance for the first time, it remains in the quarantine list until the appliance administrator approves its connection request. For more information, see Registering KACE Agent with the appliance.
Credentials	Separate rows for the credentials needed to connect to the device and run commands for the particular platform targeted by the schedule. The first column contains the operating system. The second column contains the Agent Version in place for installation. The third column contains a drop-down list from which to select existing credentials. You can select **Add new credential** to add credentials not already listed. See Add and edit User/Password credentials.

4. In the *Deploy* section, identify the devices to be included in the schedule:

Option	Description
Target IP addresses or hostnames	A comma-separated list of the IP addresses or host names of the target devices. Use hyphens to specify individual IP address class ranges. **TIP:** The appliance supports both IPv6 (Internet Protocol version 6) and IPv4 addresses. The **Help me pick devices** link enables you to add devices to the *Target IP addresses or Hostnames* list: • **Provisioning IP Range**: Use hyphens to specify individual IP address class ranges. For example: # **IPv6**: fdef:22b9:e8ae:14a9::1a0:f000-f0aa # **IPv4**: 192.168.2-5.1-200 After specifying a range, click **Add All** • **Select Devices from Discovery**: This drop-down list is populated from the **Discovery Results**. To filter the contents, start typing in the field. After selecting a device, click **Add All**.

5. Set the time for the schedule to run.

Option	Description
None	Run in combination with an event rather than on a specific date or at a specific time.
Every n hours	Run at a specified interval.
Every day/specific day at HH:MM	Run daily at a specified time, or run on a designated day of the week at a specified time.
Run on the nth of every month/ specific month at HH:MM	Run on the same day every month, or a specific month, at the specified time.

Option	Description
Run on the nth weekday of every month/specific month at HH:MM	Run on the specific weekday of every month, or a specific month, at the specified time.

Custom	Run according to a custom schedule.
	Use standard 5-field cron format (extended cron format is not supported):
	`* * * * *`
	`| | | | +----------day of week (0-6)(Sun=0)`
	`| | | +-----------month (1-12)`
	`| | +-----------day of month (1-31)`
	`| +-----------hour (0-23)`
	`+-----------minute (0-59)`
	Use the following when specifying values:
	• **Spaces ( )**: Separate each field with a space.
	• **Asterisks (*)**: Include the entire range of values in a field with an asterisk. For example, an asterisk in the hour field indicates every hour.
	• **Commas (,)**: Separate multiple values in a field with a comma. For example, `0,6` in the day of the week field indicates Sunday and Saturday.
	• **Hyphens (-)**: Indicate a range of values in a field with a hyphen. For example, `1-5` in the day of the week field is equivalent to `1,2,3,4,5`, which indicates Monday through Friday.
	• **Slashes (/)**: Specify the intervals at which to repeat an action with a slash. For example, `*/3` in the hour field is equivalent to `0,3,6,9,12,15,18,21`. The asterisk (`*`) specifies every hour, but `/3` restricts this to hours divisible by 3.
	Examples:
	• `15 * * * * Run 15 minutes after every hour every day`
	• `0 22 * * * Run at 22:00 every day`
	• `0 0 1 1,6 * Run at 00:00 on January 1 and June 1`
	• `30 8,12 * * 1-5 Run weekdays at 08:30 and 12:30`
	• `0 2 */2 * * Run every other day at 02:00`

View Task Schedule	Click to view the task schedule. The *Task Schedule* dialog box displays a list of scheduled tasks. Click a task to review the task details. For more information, see View task schedules.

6. **Optional**: Use *Advanced* settings to:
   - # Customize the ports the appliance uses to deploy the Agent.
   - # Designate an alternative download location for the Agent installer.

NOTE: Newer versions of MS Windows such as Windows 10 do not support downloading files from file shares which prevents alternate location WinRM provisioning to work as expected.

Specify the WinRM port used for agent provisioning on Windows devices. For those schedules using a legacy method to provision Windows devices, you have an option to change it to WinRM. For more information about WinRM configuration, see https://support.quest.com/kb/260699/agent-provisioning-with-winrm.

Choose the level of information to display in the log. To see only the most important messages, select *Critical*. To see all messages, select *Debug*. Other options include *Error*, *Warning*, *Notice*, and *Info*.

Specify the device that you want to use as a relay for agentless device inventory. A relay device that is used during discovery as a relay is used for agentless inventory, when a new device is provisioned automatically from discovery results. For more information, see Add a Discovery Schedule to perform a quick "what and where" scan of your network.

Enable a complete uninstall of the Agent. Selecting *Remove KUID during uninstall* results in an existing Agent being removed from the device before the Agent is installed again. In this case, the appliance generates a new KUID for the asset, and it appears as a new device in the appliance.

7. Click **Run now** to display the *Provisioning Schedules* page and the new configuration.

   The appliance saves the configuration with the name you supplied, and then runs the configuration against the targeted IP addresses.

The *Provisioning Schedules* page displays the progress of the successful installations after the schedule's start time.

Related topics

Power-on the appliance and log in to the Administrator Console

Provisioning the KACE Agent using the GPO Provisioning Tool for Windows devices

Manually deploying the KACE Agent

Managing provisioning schedules

To streamline the Agent installation process, you can add provisioning schedules that specify how and when to install the KACE Agent on devices. You can add, view, edit, run, duplicate, and delete provisioning schedules.

View, run, edit, or duplicate provisioning schedules

You can view provisioning schedule status and other details on the *Provisioning Schedules* page. From this page you can also run and edit provisioning schedules as needed.

When you duplicate provisioning schedule, its properties are copied into the new configuration. If you are creating a configuration that is similar to an existing configuration, starting with a duplicated schedule can be faster than creating a configuration from scratch.

1. Go to the *Provisioning Schedules* list:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Settings**, then click **Provisioning**.
   c. On the *Provisioning Panel*, click **Schedules**.

The list displays the following columns:

Option	Description
Name	The name of the provisioning schedule (links to the *Provisioning Schedule Detail page*).

Option	Description
Targeted	The total number of target devices in the configuration (links to the *Provisioning Results* page).
Running	The total number of target devices on which provisioning is running (links to the *Provisioning Results* page).
Pending	The total number of target devices on which provisioning has not yet started (links to the *Provisioning Results* page).
Succeeded	The total number of target devices on which provisioning has succeeded (links to the *Provisioning Results* page).
Failed	The total number of target devices on which provisioning has failed (links to the *Provisioning Results* page).
Success Rate	The total number of target devices on which provisioning has succeeded as a percentage.
IP Range	The IP address range of the target device.
Schedule	The specified provisioning schedule. For example: Every**n** minutes, Every **n** hours, or Never.
Enabled	Whether the configuration is enabled or disabled. A check mark indicates that the provisioning schedule is enabled.

2. Run provisioning schedules:
    a. Select the check boxes for the schedules that you want to run.
    b. Select **Choose Action** > **Run Now**.
3. Edit schedules:
    a. Click the name of a schedule.
    b. Edit the provisioning schedule on the schedule's *Provisioning Schedule Detail* page, and click **Save**.

    See Install the KACE Agent on a device or multiple devices.
4. Duplicate schedules:
    a. Click the name of a schedule.
    b. In the *Advanced* section, click **Duplicate** to display the *Provisioning Schedules* page with the new schedule listed as **Copy of Schedule Name**.

Delete provisioning schedules

You can delete provisioning schedules when you want to remove schedules from the appliance.

When provisioning schedules are deleted, results associated with those schedules are also deleted. Devices provisioned using the schedules, however, are not removed from inventory.

1. Go to the *Provisioning Schedules* list:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Settings**, then click **Provisioning**.

c. On the *Provisioning Panel*, click **Schedules**.

2. Select the check box next to one or more schedules.
3. Select **Choose Action** > **Delete**, then click **Yes** to confirm.

View provisioning results

You can view the results of actions performed by provisioning schedules.

1. Go to the *Provisioning Schedules* list:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Settings**, then click **Provisioning**.
   c. On the *Provisioning Panel*, click **Schedules**.
2. Click a link in the *Running, Pending, Succeeded, or Failed* column.

The *Provisioning Results* page appears with the following information:

Item	Description
Status	The status of the Agent connection to the appliance: : An Agent-managed device is connected to the appliance. : An Agent-managed device is not connected to the appliance.
Schedule Name	The name of the provisioning schedule.
IP Address	The IP address of the target device.
Hostname	The hostname of the target device. Click the **Remote Connection** button to open a Remote Desktop Connection to the target device (Microsoft Edge only):
Result	The status of the most recent provisioning attempt.
Action	**I** indicates a successful installation. **U** indicates a successful uninstallation.
Error	The failure error, such as TCP ports not accessible.
Last Run	The last time the schedule ran.

3. To view additional information about a target device, click its **IP Address**.

   The *KACE Agent Provisioning* page appears.

   This page displays the results of the most recent provisioning run and includes information such as the IP address, port configuration, and the logs of each provisioning step.
4. To view inventory information, click the **[computer inventory]** link next to the **MAC address**.

NOTE: The **[computer inventory]** link appears only if the provisioning process can match the MAC address of the target device with the current inventory data. See Managing MIA devices.

Managing Agent communications

Communications between the appliance and Agents installed on managed devices include inventory reports, alerts, patches, scripts, and crash logs. You can configure and view communications that are queued, or pending.

Configure Agent communication and log settings

Agents installed on managed devices periodically check in to the appliance to report inventory, update scripts, and perform other tasks.

You can configure the Agent settings, including the interval at which the Agents check in, messages displayed to users, and log retention time, as described in this section. If you have multiple organizations, you configure Agent settings for each organization separately.

1. Do one of the following:
   - **If the Organization component is enabled on your appliance, log in to the appliance System Administration Console, `https://appliance_hostname/system`, or select System in the drop-down list in the top-right corner of the page next to the login information. Then click Organizations. To display the organization's information, click the organization's name.**

     On the *Organization Detail* page that appears, locate the *Communication and Agent Settings* section.
   - **If the Organization component is not enabled on your appliance, log in to the appliance Administrator Console, `https://appliance_hostname/admin`. Then select Settings > Provisioning., and click Communication Settings on the *Provisioning* panel.**

     The *Communication Settings* page appears.
2. Specify the following settings in Agent tab:

NOTE: To reduce the load on the appliance, limit the number of Agent connections to 500 per hour. The number of connections that appears next to the inventory, scripting, and metering intervals, applies to the current organization only. If the Organization component is enabled on your appliance, the total number of Agent connections for all organizations should not exceed 500 per hour.

Option	Suggested Setting	Notes
Enable Agent Logging	Enabled	Whether the appliance stores scripting results provided by Agents installed on managed devices. Agent logs can consume as much as 1GB of disk space in the database. If disk space is not an issue, enable *Agent Logging* to keep all log information for Agent-managed devices. These logs can be useful during troubleshooting. To save disk space, and enable faster Agent communication, disable *Agent Logging*.
Agent Debug Trace	Enabled	If selected, this option allows you to record the Agent's debug trace. This information allows administrators to monitor the Agent's performance, and to diagnose common problems.
Agent Inventory	12 hours	The frequency at which Agents on managed devices report inventory. This information is displayed in the *Inventory* section.
Agentless Inventory	1 Day	The frequency at which Agentless devices report inventory. This information is displayed in the *Inventory* section.
Catalog Inventory	24 hours	The frequency at which managed devices report inventory to the *Software Catalog* page.

Option	Suggested Setting	Notes
Metering	4 hours	The frequency at which managed devices report metering information to the appliance. Requires metering to be enabled on devices and applications.
Scripting Update	4 hours	The frequency at which Agents on managed devices request updated copies of scripts that are enabled on managed devices. This interval does not affect how often scripts run.
Max Download Speed	As required	The maximum download speed, as required. Choose from the available options.
Konea Connection Timeout	80 seconds	Configurable konea tunnel timeout check for bootup MI.
Enable Wait for Bootup Tasks	Disabled	If selected, this option stops the agent from executing bootup tasks.
Enable Wait for Login Tasks	Disabled	If selected, this option stops the agent from executing login tasks.

3. In the Agent Settings tab in the*Agent Status Icon Settings* section, specify the following settings:

Option	Suggested Setting	Notes
Agent Status Icon On Device	Enabled	If selected, this option allows you to display the agent status on managed devices.
Enable Agent Snooze on Device	Enabled	If selected, this option allows you to suspend the agent's activity on managed devices using the system tray (Windows) or menu bar (Mac OS). **NOTE:** Some critical background tasks are still allowed to run, including inventory, replication tasks, and urgent alerts.
Agent Snooze Max Count (per day)	1 snooze	The maximum number of times you can snooze the agent each day on managed devices.
Agent Status Icon Shortcuts	As required	Use this section to display links in the KACE Agent menu on agent-managed devices. You can specify up to ten links. Standard Uniform Resource Identifier (URI) links are supported, such as `https`, `ssh`, and `ftp` URLs. To add a link: 1. Click +. 2. In the *Display Name* column, type the text that you want to display in the menu. For example, *My FTP link*.

Option	Suggested Setting	Notes
		3. In the URL column, type the fully qualified URL address. For example, `https://www.quest.com/`. The URL supports the following replacement variables: # $(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) For complete information about these and other replacement variables, see Token replacement variables. You can use the column headings to sort the list. In the KACE Agent menu, the links appear in the order they are listed on this page.

NOTE: Any changes that you make in this section take effect only after the KACE Agent on the managed device reconnects to the appliance, either by restarting each individual agent, or the appliance.

4. In the *Notify* tab, specify the message to use for Agent communications:

Option	Suggested Setting	Notes
Agent Splash Page Message	Default text: `KACE Systems Management Appliance is verifying your PC Configuration and managing software updates. Please Wait...`	The message that appears to users when Agents are performing tasks, such as running scripts, on their devices.
Agent Splash Bitmap	As required	The path to an existing .bmp file that you want to use as the splash logo.
Disable Bootup Splash	Disabled	If selected, this option stops the agent from displaying the boot-up splash logo.
Disable Login Splash	Disabled	If selected, this option stops the agent from displaying the login splash logo.

5. In the *Agentless Settings* tab, specify communications settings for Agentless devices:

Option	Description
SSH Timeout	The time, in seconds, after which the connection is closed if there is no activity.
SNMP Timeout	The time, in seconds, after which the connection is closed if there is no activity.

Option	Description
Retry Attempts	The number of times the connection is attempted.
WinRM Timeout	The time, in seconds, after which the connection is closed if there is no activity.
VMware Timeout	The amount of time in seconds to wait for a connection to the VMware vSphere API service running on a VMware host.

6. If the Organization component is not enabled on your appliance, specify *Agent Tasks* settings.

   NOTE: If the Organization component is enabled on your appliance, these *Agent Tasks* settings are located on the appliance System Administration Console *General Settings* page.

Option	Description
Last Task Throughput Update	This value indicates the date and time when the appliance task throughput was last updated.
Current CPU Load	The value in this field depicts the load on an appliance at any given time. For the appliance to run normally, the value in this field must be between 0.0 and 10.0.
Task Throughput	The value that controls how scheduled tasks, such as inventory collection, scripting, and patching updates, are balanced by the appliance. **NOTE:** This value can be increased only if the value in the Current CPU Load is not more than 10.0 and the Last Task Throughput Update time is more than 15 minutes.

7. In the *Duplicate Machine Detection Settings (Advanced)* section, configure the following options to prevent duplicate device records

   When the appliance receives inventory from a device without an existing inventory record (which is determined by the use of a new/unknown KUID), it scans the device's properties that you select in this section to determine whether this is a new device or an existing one. If it determines that the device belongs to an existing inventory record, it merges the new device record with the existing one.

Option	Description
Required to match an existing machine record	Select one or more of the following check boxes to indicate which device properties you want the appliance to use to identify potentially duplicated devices. • **Machine Name** • **BIOS Serial Number** • **Manufacturer** • **Operating System Family**
MAC Addresses	Specify the number of MAC addresses that are associated with the machine record that you to match with the existing device records.

8. Click **Save**.

   The changes take effect when Agents check in to the appliance.

9. If you have multiple organizations, repeat the preceding steps for each organization.

Related topics

View appliance logs

Configure appliance General Settings with the Organization component enabled

View Agent task status

You can view the status of tasks that are currently running, or that are scheduled to run, on Agent-managed devices.

1. Go to the appliance *Control Panel*:
   - **If the Organization component is not enabled on the appliance, log in to the appliance Administrator Console, `https://appliance_hostname/admin`, then select Settings > Control Panel.**
   - **If the Organization component is enabled on the appliance, log in to the appliance System Administration Console, `https://appliance_hostname/system`, or select System in the drop-down list in the top-right corner of the page, then select Settings > Control Panel.**
2. On the left navigation bar, click **Support** to display the *Support* page.
3. In the *Troubleshooting Tools* section, click **Display Agent task status** to display the *Agent Tasks* page.

   By default, *In Progress* tasks are listed. To view other tasks, select different filtering options in the *View By* drop-down list, which appears above the list on the right. Task information includes:

Column	Description
Device Name	The name of the device that is the target of the task.
Type	The type of task. Depending on appliance configuration, task types include alerts, inventory, kbot, krash upload, and scripting updates.
Started	The start time of the task.
Completed	The completion time of the task.
Next Run	The next scheduled run time for the task.
Run Time	How long it took to run the task.
Timeout	The time limit for completing the task.
Priority	The importance or rank of the task.

   The options displayed depend on type of tasks available on your appliance. Typical options include:

   # **Ready to Run (connected)**: Tasks that are connected through the messaging protocol and about to run.
   # **Ready to Run**: Tasks that are queued to run when an messaging protocol connection is established.
   # **Longer than 10 minutes**: Tasks that have been waiting longer than 10 minutes for a protocol connection.
4. To view details about a device, click its name in the *Device Name* column.

   The *Device Detail* page appears.

View the Agent Command Queue

The Agent Command Queue list shows messages, such as pop-ups and alerts, that have been queued for distribution from the appliance to Agent-managed devices.

1. Go to the appliance *Control Panel*:
   - **If the Organization component is not enabled on the appliance, log in to the appliance Administrator Console, `https://appliance_hostname/admin`, then select Settings > Control Panel.**
   - **If the Organization component is enabled on the appliance, log in to the appliance System Administration Console, `https://appliance_hostname/system`, or select System in the drop-down list in the top-right corner of the page, then select Settings > Control Panel.**
2. On the left navigation bar, click **Support** to display the *Support* page.
3. In the *Troubleshooting Tools* section, click **View Agent command queue** to display the *Agent Command Queue* page.

   Pending messages appear in this queue only during continuous connection between the Agent and the appliance.

   NOTE: Pending alerts appear on the *Agent Command Queue* page even if there is no connection between the Agent and the appliance.

   The *Agent Command Queue* page contains the following fields:

Option	Description
Device Name	The name of the device. Click a name to view device details.
Type [Plug-in, Source]	The type of message, such as *Run Process*.
Command	The content and information contained in the message.
Expiration	The date and time when the message expires, also called *Keep Alive* time. Messages are deleted from the queue automatically when they expire.
Status	The status of the message, such as *Completed* or *Received*.

Related topics

Broadcasting alerts to managed devices

Delete messages from the Agent command queue

You can delete messages that are no longer needed from the Agent command queue.

1. Go to the appliance *Control Panel*:
   - **If the Organization component is not enabled on the appliance, log in to the appliance Administrator Console, `https://appliance_hostname/admin`, then select Settings > Control Panel.**
   - **If the Organization component is enabled on the appliance, log in to the appliance System Administration Console, `https://appliance_hostname/system`, or select System in the drop-down list in the top-right corner of the page, then select Settings > Control Panel.**
2. On the left navigation bar, click **Support** to display the *Support* page.
3. In the *Troubleshooting Tools* section, click **View Agent command queue** to display the *Agent Command Queue* page.
4. Select the check box next to one or more messages.
5. Select **Choose Action > Delete**, then click **Yes** to confirm.

Updating the KACE Agent on managed devices

The appliance automatically checks with Quest for KACE Agent updates at approximately 03:40 every day. In addition, the appliance checks Quest for Agent updates whenever the appliance is rebooted.

When Agent updates are available, they are automatically downloaded to the appliance, provided that the appliance is connected to the Internet, and an alert appears on the *Home* page of the appliance **Administrator Console**. Until you configure deployment settings, however, Agent updates are not automatically deployed to managed devices. Click the link in the alert to configure deployment settings.

In addition, you can check for Agent software updates, obtain Agent updates manually, and configure Agent update settings any time. Obtaining updates manually is useful if your appliance is not connected to the Internet.

View KACE Agent updates

You can view KACE Agent updates in the **Administrator Console**.

1. Go to the appliance *Control Panel*:
   - **If the Organization component is not enabled on the appliance, log in to the appliance Administrator Console, `https://appliance_hostname/admin`, then select Settings > Control Panel.**
   - **If the Organization component is enabled on the appliance, log in to the appliance System Administration Console, `https://appliance_hostname/system`, or select System in the drop-down list in the top-right corner of the page, then select Settings > Control Panel.**
2. On the left navigation bar, click **Appliance Updates**.

   The *Appliance Updates* page appears. The current Agent bundle appears in the *Agent* section.
3. **Optional**: To check for updates: In the *Agent* section, click **Check for Update**.

   The appliance checks for updates, and the results appear on the *Logs* page.

Configure Agent update settings

After Agents are installed on devices, they are designed to update themselves automatically based on the Agent update settings you choose on the *Update Agent Settings* page. This is true regardless of the provisioning methods used to deploy the Agents, including appliance provisioning, GPO wizard, other GPO deployments, or image deployment.

If you have multiple organizations, you configure Agent update settings for each organization separately.

1. Go to the *Update Agent Settings* page:

a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
b. On the left navigation bar, click **Settings**, then click **Provisioning**.
c. On the *Provisioning Panel*, click **Agent Update from KACE**.

If a new Agent update is available, it appears in the *Available Agent Bundle* section.

2. Click **Apply** in the *Available Agent Bundle* section.

The new Agent version number appears in the *Advertised Updates* section, and the *Enabled* check box in the *Agent Settings* section is cleared, disabling automatic updates. This enables you to test the updates on selected devices before deploying them system-wide.

3. View or specify the following Agent update settings:

Option	Description
Enabled	Deploy the update to the selected appliance devices during the next scheduled inventory interval. Clear the check box to prevent updates from being installed.
Modified	Read-only: The time the most recent Agent bundle was downloaded.
All Devices	Deploy the update to all devices that have the KACE Agent installed. If this option is selected, the *Devices* and *Labels* elements do not appear on the page.
Devices	Update only specific devices. Select the device names in the drop-down list that appears when you click in the field, or type the first few characters of a device name to sort the list. For example, type Dev to list matching device names such as Device-1, Device-2, and so on. This option is not available when you select **All Devices**.
Restrict to Labels	Display the *Edit Labels* dialog. Search for and select labels, and update devices assigned to the selected labels. This option is not available when you select **All Devices**.
Notes	Any additional information you want to provide.

4. Click **Save**.

The update is deployed to the selected devices during the next scheduled inventory interval. If you use Replication Shares, and failover to the appliance is not selected, Agents are updated after the Replication Shares are updated.

5. If you limited deployment to specified devices for testing, select additional devices in the *Agent Settings* section of the *Update Agent Settings* page when your testing is complete.

The update is deployed to the selected devices during the next scheduled inventory interval.

6. If you have multiple organizations, repeat the preceding steps for each organization.

Related topics

Setting up and using labels to manage groups of items

Upload Agent updates manually

In most cases, Agent updates are automatically downloaded to the appliance when they become available. However, you can download updates from Quest and manually upload Agent updates to the appliance as needed. This is useful if your appliance is not connected to the Internet, or if Agent updates are available but have not yet been downloaded to the appliance automatically.

To download Agent updates from Quest, you must obtain customer login credentials by contacting **Quest Support** at https://support.quest.com/contact-support.

1. To manually check for updates, go to the appliance *Control Panel*:
   - **If the Organization component is not enabled on the appliance, log in to the appliance Administrator Console, `https://appliance_hostname/admin`, then select Settings > Control Panel.**
   - **If the Organization component is enabled on the appliance, log in to the appliance System Administration Console, `https://appliance_hostname/system`, or select System in the drop-down list in the top-right corner of the page, then select Settings > Control Panel.**
2. On the left navigation bar, click **Appliance Updates** to display the *Appliance Updates* page.

   The version of the current Agent bundle appears in the *Agent* section.
3. Click **Check for Agent Updates** in the *Agent* section.

   The appliance checks for updates, and the results appear on the *Logs* page.
4. To obtain updates:
   a. Log in to the Quest Support site using your customer login credentials:

      https://support.quest.com/kace-systems-management-appliance/download-new-releases.

   b. Download the Agent update bundle and save the file locally.
5. Go to the *Update Agent Settings* page:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Settings**, then click **Provisioning**.
   c. On the *Provisioning Panel*, click **Agent Update from KACE**.
6. Do one of the following:
   - **If a new update appears in the *Available Agent Bundle* section, click Apply.**
   - **If you manually downloaded an update, go to the *Manually Upload Agent Bundle* section, click Browse or Choose File, locate the file that you downloaded, then click Upload.**

   The new Agent version number appears in the *Advertised Updates* section, and the *Enabled* check box in the *Agent Settings* section is cleared, disabling automatic updates. This enables you to test the updates on selected devices before deploying them system-wide.
7. Specify deployment options In the *Agent Settings* section. See Configure Agent update settings.
8. If you have multiple organizations, repeat 6 and 7 for each organization.

Manually deploying the KACE Agent

Manual deployment is useful when automated Agent provisioning is not practical or when you want to deploy the KACE Agent using email, logon scripts, GPO (Group Policy Objects), or Active Directory.

- **Email**: To deploy KACE Agents through email, you would send an email to your users that contains one of the following:
  # The Agent installation file.
  # A link to the appliance where the Agent file can be downloaded.
  # A web location where the required installation file can be downloaded.
- **Logon scripts**: Logon scripts enable you to deploy the KACE Agent when users log on to a device. If you use logon scripts, you would upload the appropriate file in an accessible directory and create a logon script to retrieve it.

Obtaining Agent installation files

Agent installation files are available on the appliance.

You can find the KACE Agent installers for Windows, Mac OS X, and Linux devices on the appliance in the following directory:

`\\`**appliance_hostname**`\client\agent_provisioning`

NOTE: File sharing must be enabled to access the installers. See Enable file sharing at the System level.

The appliance uses a registration process, allowing authenticated KACE Agents to connect to the appliance, either by associating a token with an Agent, or having an appliance administrator approve a connection request. Agent installers obtained this way do not include a valid token. You can pass the agent token to the installer manually using one of the following options:

- **Windows devices:**
  # Use the following parameters when starting the installer: `HOST=<appliance_hostname> TOKEN=<agent_token>`, or:
  # Manually change the installation file name using the following syntax: `AMPAgent-xx.xx.xx-x86_<appliance_hostname>+<agent_token>.msi`
- **Non-Windows devices**:
  # Use the `KACE_HOST` and `KACE_TOKEN` environment variables to specify the appliance host name and agent token before you run the installation file, or:
  # Manually change the installation file name using the following syntax: `<agent_installation_filename>_<appliance_hostname>+<agent_token>.<extension>`

If you do not specify a valid token string during the Agent installation, any connection requests result in the Agent being quarantined.

Alternatively, you can download Agent token installer bundles for your operating system from the *Agent Token Detail* page. For complete information, see Registering KACE Agent with the appliance.

Manually deploying the KACE Agent on Windows devices

You can manually deploy the KACE Agent on Windows devices using the installation wizard or from the command line on devices.

When you install the Agent manually, the Agent executable files must be installed in the following locations:

- Windows 32-bit devices: `C:\Program Files\Quest\KACE\`
- Window 64-bit devices: `C:\Program Files (x86)\Quest\KACE\`

The Agent configuration files, logs, and other data are stored in:

- Windows 32-bit devices: `C:\Documents and Settings\All Users\Quest\KACE`
- Window 64-bit devices: `C:\ProgramData\Quest\KACE`

Manually deploy the KACE Agent on Windows devices using the installation wizard

You can manually deploy the KACE Agent on Windows devices by running the installation wizard on devices.

1. Go to the shared directory of the appliance:

\\appliance_hostname\client\agent_provisioning\windows_platform

2. Copy the `ampagent-x.x.xxxxx-x64.msi` file to the device.
3. Double-click the file to start the installation and follow the instructions in the installation wizard.
4. If you want to register the agent with the appliance:

   # Use the following parameters when starting the installer: `HOST=<appliance_hostname> TOKEN=<agent_token>`, or:

   # Manually change the installation file name using the following syntax: `AMPAgent-xx.xx.xx-x86_<appliance_hostname>+<agent_token>.msi`

   You can obtain the agent token string from the *Agent Token Detail* page. For more details, see Registering KACE Agent with the appliance.

The device information appears in the appliance **Inventory** within a few minutes. See Managing applications on the Software page.

Manually deploy the KACE Agent on Windows devices using the Command line

There are several ways to deploy the Agent from the command line on Windows devices.

For example:

- In a batch file as part of a logon script that runs the installer (`msiexec`) and sets various parameters, such as the value of the host.
- Set an environment variable for the server name then run the installer.
- Change name of the installer, which automatically sets the server name during the installation.

The following table shows command line parameters used to deploy the Agent.

Table 21. Command line parameters for the Agent

Description	Parameter
Windows Installer Tool	`msiexec` or `msiexec.exe`

Install flag	`/i`
	Example:
	`msiexec /i ampagent-6.x.xxxxx-x64`

Uninstall flag	`/x`
	Example:
	`msiexec /x ampagent-6.x.xxxxx-x64`

Silent install	`/qn`
	Example:
	`msiexec /qn /i ampagent-6.x.xxxxx-x64`

Log verbose output	`/L*v log.txt`
	Example:
	`msiexec /qn /L*v C:\temp\log.txt /i ampagent-6.x.xxxxx-x64`

Auto set hostname: Rename the installation file to the name of the server	`rename agent_installer.msi_hostname.msi` **Example**:

Description	Parameter
name, which automatically sets the hostname	`msiexec /qn /i ampagent-6.x.xxxxx-x64_kace_sma.example.com.msi`
Set properties	`PROPERTY=value` (Must use ALL CAPS) **Example**: `msiexec /qn /i ampagent-6.x.xxxxx-x64.msi HOST=kace_sma.example.com`

Set server name	`set KACE_SERVER=kace_sma_name`
	Must be followed by an `msiexec` call to install
	Example:
	`set KACE_SERVER=kboxmsiexec /i ampagent-6.x.xxxxx-x64`

Prevent the installation of logon or bootup hooks, and preserve existing userinit.exe files	`NOHOOKS=1`
	Example:
	`msiexec /qn /i ampagent-6.x.xxxxx-x64.msi HOST=kace_sma.example.com NOHOOKS=1`

Install the Agent but do not start the service. This enables the Agent to be imaged and cloned to other devices	`CLONEPREP=yes/no`
	Example:
	`msiexec /qn /i ampagent-6.x.xxxxx-x64.msi HOST=kace_sma.example.com CLONEPREP=yes`

Set the debug level for the Agent when it generates logs	`DEBUG=true/all`
	Example:
	`msiexec /qn /i ampagent-6.x.xxxxx-x64.msi HOST=kace_sma.example.com DEBUG=true`

Force the Agent to communicate through HTTPS only. It cannot fall back to HTTP if HTTPS is unavailable	`SSLREQUIRED=true`
	Example:
	`msiexec /qn /i ampagent-6.x.xxxxx-x64.msi HOST=kace_sma.example.com SSLREQUIRED=true`

The system looks for the value of **host** in these locations in the order shown:

1. The installer file
2. The `HOST` property value
3. `KACE_SERVER` (environment variable)
4. The `amp.conf` file

If you want to register the agent with the appliance:

- Use the following parameters when starting the installer: `HOST=<appliance_hostname> TOKEN=<agent_token>`, or:
- Manually change the installation file name using the following syntax: `AMPAgent-xx.xx.xx-x86_<appliance_hostname>+<agent_token>.msi`

You can obtain the agent token string from the *Agent Token Detail* page. For more details, see Registering KACE Agent with the appliance

CAUTION: If you leave the host value empty, you must set the environment variable. Otherwise, the Agent will not connect to the appliance. Quest recommends that you use the fully qualified domain name as the hostname.

Manage the KACE Agent on Windows devices using the Windows system tray

You can view the status of the KACE Agent, force inventory, and display agent information using the Windows system tray.

To access the KACE Agent status using the system tray, you must enable the **Agent Status On Device** option in the *Agent and Communication Settings* section. For more information, see Configure Agent communication and log settings.

1. On the device where the KACE Agent is running, in the Windows system tray, click .

   The indicator in the bottom-right corner of the icon indicates if the agent status:

   # : The agent is connected to the appliance.
   # : The agent is snoozed.
   # : The agent has pending actions.
   # : The agent is disconnected from the appliance.

2. To find out if the agent is connected to the appliance, observe the Status icon in the menu.

   This is the same indicator that appears on the Agent icon, that tells you whether the agent is connected, snoozed, has pending actions, or disconnected from the appliance, as described above.

3. To run the device inventory, click **Inventory** in the menu.
4. To restart the agent, click **Restart Agent** in the menu.
5. To temporarily suspend the agent's activity during a specific time period, click **Snooze Agent**, and select a time period in the menu. You can snooze the agent for 15 minutes, 30 minutes, one hour, or two hours.

   NOTE: You can only snooze the agent if the **Agent Snooze on Device** option is enabled in the *Agent and Communication Settings* section on the appliance, and if the maximum number of snoozes is not reached. For more information, see Configure Agent communication and log settings.

   Snoozing an agent does not stop any ongoing agent processes on the device. It only prevents the agent from starting a new process. If an agent snooze is not possible, for example, due to configuration, an error message appears.

6. To install the patches downloaded to the Agent device, click **Deploy staged patches**.

   NOTE: This menu item only appears when a Detect, Stage and On-demand Deploy patch or Windows Feature schedule downloads all applicable patches to the Agent device. For more information, see Configure patch schedules.

7. To access any agent-related links, click **Shortcuts** in the menu, and then click a link, as applicable. Any standard Uniform Resource Identifier (URI) links are supported, such as `https`, `ssh`, and `ftp` URLs.

   This menu item only appears when your system administrator specifies one or more links. For more information, see Configure Agent communication and log settings.

   The link causes the OS to launch the application associated with the selected resource. For example, to open an HTTP link, your system opens the link in the default browser.

8. To find out more information about the agent application, click **About**.

Manually deploying and upgrading the KACE Agent on Linux devices

You can manually deploy or upgrade the KACE Agent on Linux devices as needed.

Manually deploy the KACE Agent on Linux devices

You can manually deploy the KACE Agent on Linux devices by copying the Agent installation files to the devices and running installation commands.

1. Copy the KACE Agent installation file to the device.

   See Obtaining Agent installation files.

2. If you want to register the agent with the appliance:

   # Use the `KACE_HOST` and `KACE_TOKEN` environment variables to specify the appliance host name and agent token before you run the installation file, or:

   # Manually change the installation file name using the following syntax:
   `<agent_installation_filename>_<appliance_hostname>+<agent_token>.<extension>`

   You can obtain the agent token string from the *Agent Token Detail* page. For more details, see Registering KACE Agent with the appliance.

3. Open a terminal window from **Applications** > **System Tools**.
4. At the command prompt, set the name of the server and install the Agent:

   ```
   sudo KACE_SERVER=kace_sma_name rpm -Uvh ampagent-x.x.xxxxx-x.i386.rpm
   ```

   The Agent is installed in the following directories:

   # `/opt/quest/kace/bin/` where the Agent executable files are installed.

   # `/var/quest/kace/` where the Agent configuration, logs, and other data is stored.

The device information appears in the appliance **Inventory** within a few minutes. See Managing applications on the Software page.

Deploy the KACE Agent on Linux devices at startup or login

You can schedule the Agent to be deployed when users start or log in to Linux devices.

- Set the name by adding the following command to the root directory:

  ```
  export KACE_SERVER=kace_sma_name
  ```

  The `export` call must precede the call to the installer. For example: `export KACE_SERVER=kace_sma_name rpm -Uvh kace_sma_agent-12345.i386.rpm`

  The system looks for the value of **host** in these locations in the order shown:

  1. The installer file
  2. `KACE_SERVER` (environment variable)
  3. The `amp.conf` file

  If you want to register the agent with the appliance:

  # Use the `KACE_HOST` and `KACE_TOKEN` environment variables to specify the appliance host name and agent token before you run the installation file, or:

  # Manually change the installation file name using the following syntax:
  `<agent_installation_filename>_<appliance_hostname>+<agent_token>.<extension>`

  You can obtain the agent token string from the *Agent Token Detail* page. For more details, see Registering KACE Agent with the appliance

  CAUTION: If you leave the host value empty, you must set the environment variable. Otherwise, the Agent does not connect to the appliance. Quest recommends that you use the fully qualified domain name as the hostname.

Upgrade the KACE Agent on Linux devices

You can manually upgrade the KACE Agent on Linux devices by running commands on the devices.

1. Copy the KACE Agent installation file to the device. See Obtaining Agent installation files.
2. If you want to register the agent with the appliance:

   # Use the `KACE_HOST` and `KACE_TOKEN` environment variables to specify the appliance host name and agent token before you run the installation file, or:

   # Manually change the installation file name using the following syntax:
   `<agent_installation_filename>_<appliance_hostname>+<agent_token>.<extension>`

   You can obtain the agent token string from the *Agent Token Detail* page. For more details, see Registering KACE Agent with the appliance.

3. Open a terminal window from **Applications** > **System Tools**.
4. At the command prompt, enter:

   ```
   rpm -uvh kace_sma_agent-linux_buildnumber.rpm
   ```

Performing Agent operations on Linux devices

You can run commands on Agent-managed Linux devices to perform various Agent operations.

Start and stop the Agent on Linux devices

You can run commands on Linux devices to start and stop the Agent. This procedure is useful in troubleshooting Agent-related issues.

1. Open a terminal window from **Applications** > **System Tools**.
2. To start the Agent, enter:

   ```
   /opt/quest/kace/bin/AMPTools start
   ```

3. To stop the Agent, enter:

   ```
   /opt/quest/kace/bin/AMPTools stop
   ```

Manually remove the Agent from Linux devices

You can remove the Agent from Linux devices manually by running commands on the devices.

1. Open a terminal window from **Applications** > **System Tools**.
2. At the command prompt, enter:

   ```
   sudo rpm -e ampagent
   ```

3. **Optional**: Remove the `kace` directory:

   ```
   rm -rf  /var/quest/kace/
   ```

Verify that the Agent is running on Linux devices

You can run a command on Linux devices to determine whether the Agent is running.

1. Open a terminal window from **Applications** > **System Tools**.
2. At the command line prompt, enter:

   ```
   ps aux | grep AMPAgent
   ```

   This output indicates that the process is running:

```
root 6100 0.0 3.9 3110640 20384 ? Ssl Mar03 0:00 /opt/quest/kace/bin/AMPAgent
--daemon
```

View the Agent version on Linux devices

You can run a command on Linux devices to verify the version of the Agent installed on those devices.

1. Open a terminal window from **Applications** > **System Tools**.
2. At the command prompt, enter:

   `rpm -q ampagent`

   The version number is displayed.

Collecting inventory information

You can manually collect inventory on Linux devices by forcing inventory updates.

See Forcing inventory updates.

Manually deploying and upgrading the KACE Agent on Mac devices

You can manually deploy or upgrade the Agent on Mac devices as needed.

This section provides information for manually deploying the KACE Agent on Mac OS X devices. Additional options are described in Use shell scripts to deploy the KACE Agent.

NOTE: Some commands must be run as **root**.

NOTE: Proceed with `su` or `sudo` as required.

Deploy or upgrade the KACE Agent to Mac devices using the Agent installer

You can manually deploy the KACE Agent on Mac devices by copying the Agent installation files to the devices and running the installer.

1. Copy the KACE Agent installation file to the device.

   See Obtaining Agent installation files.

2. If you want to register the agent with the appliance:

   # Use the `KACE_HOST` and `KACE_TOKEN` environment variables to specify the appliance host name and agent token before you run the installation file, or:

   # Manually change the installation file name using the following syntax:
   `<agent_installation_filename>_<appliance_hostname>+<agent_token>.<extension>`

   You can obtain the agent token string from the *Agent Token Detail* page. For more details, see Registering KACE Agent with the appliance.

3. Double-click **ampagent-x.x.build_number.dmg**.
4. Double-click **AMPAgent.pkg**.
5. Follow the instructions in the installer.

   Be sure to enter the name of your appliance.

The installer creates the following directories on your device:

- `/Library/Application Support/Quest/KACE/bin` where the Agent executable files are installed.
- `/Library/Application Support/Quest/KACE/data/` where the Agent configuration, logs, and other data is stored.

Deploy the Agent to Mac devices using the terminal window

You can manually deploy the KACE Agent on Mac devices by copying the Agent installation files to the devices and running commands.

1. Copy the KACE Agent installation file to the device.

   See Obtaining Agent installation files.

2. If you want to register the agent with the appliance:

   # Use the `KACE_HOST` and `KACE_TOKEN` environment variables to specify the appliance host name and agent token before you run the installation file, or:

   # Manually change the installation file name using the following syntax:
   `<agent_installation_filename>_<appliance_hostname>+<agent_token>.<extension>`

   You can obtain the agent token string from the *Agent Token Detail* page. For more details, see Registering KACE Agent with the appliance.

3. Open a terminal window from **Applications** > **Utilities**.
4. At the command prompt, enter the following commands to set the name of the server and install the Agent:

   `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'
   ```

Use shell scripts to deploy the KACE Agent

You can run shell scripts to deploy the Agent to Mac devices.

When using shell scripts to deploy the Agent, you can use the following command line options:

- `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'`

> **NOTE:** The export call must proceed the install call. For example: `sudo export KACE_SERVER=kace_sma_name installer -pkg '/Volumes/Dell KACE/AMPAgent.pkg' -target /`

The system looks for the value of **host** in these locations in the following order shown:

1. The installer file
2. `KACE_SERVER` (environment variable)
3. The `amp.conf` file

If you want to register the agent with the appliance:

- Use the `KACE_HOST` and `KACE_TOKEN` environment variables to specify the appliance host name and agent token before you run the installation file, or:
- Manually change the installation file name using the following syntax:
  `<agent_installation_filename>_<appliance_hostname>+<agent_token>.<extension>`

You can obtain the agent token string from the *Agent Token Detail* page. For more details, see Registering KACE Agent with the appliance

For information about using shell scripts and command lines, go to http://developer.apple.com.

CAUTION: If you leave the host value empty, you must set the environment variable. Otherwise, the Agent will not connect to the appliance. Quest KACE recommends that you use the fully qualified domain name as the hostname.

Performing other Agent operations on Mac devices

You can run commands on Agent-managed Mac devices to perform various operations.

Start or stop the Agent on Mac devices

You can run commands on Mac devices to start and stop the Agent. This procedure is useful in troubleshooting Agent-related issues.

1. Open a terminal window from **Applications** > **Utilities**.
2. Type the following:

   ```
   cd "Library/Application Support/Quest/KACE/bin"
   ```

3. To start the Agent, enter:

   ```
   ./AMPTools start
   ```

4. To stop the Agent, enter:

   ```
   ./AMPTools stop
   ```

Manually remove the Agent from Mac devices

You can remove the Agent from Mac devices manually by running commands on the devices.

1. Open a terminal window from **Applications** > **Utilities**.
2. Type the following:

   ```
   sudo "/Library/Application Support/Quest/KACE/bin/AMPTools" uninstall
   ```

The Agent is removed.

Verify that the Agent is running on Mac devices

You can run a command on Mac devices to determine whether the Agent is running.

1. Open a terminal window from **Applications** > **Utilities**.
2. Enter the following command:

   ```
   ps aux | grep AMPAgent
   ```

   This output indicates that the process is running:

   ```
   root 2159 0.0 1.1 94408 12044 p2 S 3:26PM 0:10.94 /Library/Application Support/
   Quest/KACE/AMPAgent
   ```

Verify the version of the Agent on Mac devices

You can run a command on Mac devices to verify the version of the Agent installed on those devices.

1. Open a terminal window from **Applications** > **Utilities**.
2. Enter the following command:

   ```
   cat /Library/Application\ Support/Quest/KACE/data/version
   ```

   The version number is displayed.

Collecting inventory information from Mac devices

You can manually collect information from Mac devices by forcing inventory updates.

See Forcing inventory updates.

Manage the KACE Agent on Mac devices using the menu bar

You can view the status of the KACE Agent, force inventory, and display agent information using the Mac menu bar.

To access the KACE Agent status using the Mac menu bar, you must enable the **Agent Status On Device** option in the *Agent and Communication Settings* section. For more information, see Configure Agent communication and log settings.

1. On the device where the KACE Agent is running, in the Mac menu bar, click .

   The indicator in the bottom-right corner of the icon indicates if the agent status:

   # : The agent is connected to the appliance.
   # : The agent is snoozed.
   # : The agent has pending actions.
   # : The agent is disconnected from the appliance.

   The agent menu appears.
2. To find out if the agent is connected to the appliance, observe the Status icon in the menu.

   This is the same indicator that appears on the Agent icon, that tells you whether the agent is connected, snoozed, has pending actions, or disconnected from the appliance, as described above.
3. To run the device inventory, click **Inventory** in the menu.
4. To restart the agent, click **Restart Agent** in the menu.
5. To temporarily suspend the agent's activity during a specific time period, click **Snooze Agent**, and select a time period in the menu. You can snooze the agent for 15 minutes, 30 minutes, one hour, or two hours.

   NOTE: You can only snooze the agent if the **Agent Snooze on Device** option is enabled in the *Agent and Communication Settings* section on the appliance, and if the maximum number of snoozes is not reached. For more information, see Configure Agent communication and log settings.

   Snoozing an agent does not stop any ongoing agent processes on the device. It only prevents the agent from starting a new process. If an agent snooze is not possible, for example, due to configuration, an error message appears.
6. To access any agent-related links, click **Shortcuts** in the menu, and then click a link, as applicable. Any standard Uniform Resource Identifier (URI) links are supported, such as `https`, `ssh`, and `ftp` URLs.

   This menu item only appears when your system administrator specifies one or more links. For more information, see Configure Agent communication and log settings.

   The link causes the OS to launch the application associated with the selected resource. For example, to open an HTTP link, your system opens the link in the default browser.
7. To find out more information about the agent application, click **About**.
8. To remove the agent application from the Mac menu bar, click **Quit**.

The agent icon is removed from the menu bar. To display it again, log off, then log on. Alternatively, you can install the agent again from the `Application` directory.

Viewing information collected by the Agent

You can view inventory information collected by the Agent on the *Device Detail* page.

See Managing inventory information.

Using Agentless management

Use Agentless device management if you want to manage devices without the need to deploy and maintain the KACE Agent software on those devices.

About Agentless device management

Agentless device management is a method of managing devices without the need to deploy and maintain the KACE Agent software on those devices.

Agentless management uses SSH, SNMP, and other methods to connect to Agent-intolerant devices, such as printers, network devices, and storage devices, and report the collected inventory information to the appliance **Administrator Console**. Using Agentless management is useful for operating system versions and distributions that are not supported by the KACE Agent, and where Agentless management is preferred over installing the Agent.

There are some differences between the features that are supported for Agent devices and Agentless devices. See Features available for each device management method.

Operating systems supported by Agentless management

Agentless management supports a variety of device operating systems.

The following table shows the device operating systems that are supported by Agentless management:

Operating system
CentOS
Chrome OS
Debian
Fedora
FreeBSD
Mac OS X
Oracle Enterprise Linux
Red Hat Enterprise Linux*
SUSE*

Operating system
Solaris
Ubuntu*
Windows
Windows Server

*Most recent versions can also be managed with the KACE Agent.

NOTE: For non-computer devices such as assets, or devices without operating systems that Agentless management supports, you can map SNMP (Simple Network Management Protocol) OIDs (Object Identifiers) to particular fields in the inventory table. As a result, you can identify specific devices to be inventoried so that you can expand the inventory of Agentless-managed devices. See Using SNMP Inventory Configurations to identify specific SNMP objects and non-computer devices to add to inventory.

About enabling Agentless management on Agent-managed devices

Agentless management can be enabled for any discovered device, including devices that have the KACE Agent installed.

However, using both methods for managing a single device is not recommended. If both methods are enabled for a device, both the device, and its software, appear twice on inventory lists. As a result, it is better to not to enable Agentless management on Agent-managed devices.

Managing Agentless devices

To manage devices without installing KACE Agent software, you can enable Agentless management using Discovery information or by entering device connection details manually.

Features available to Agentless devices differ from those features available to Agent-managed devices. See Features available for each device management method.

Enable Agentless management using Discovery information

You can enable Agentless management using Discovery information.

1. Go to the *Discovery Results* list:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Inventory**, then click **Discovery Results**.
2. Select the check box next to one or more devices.
3. Select **Choose Action** > **Provision** > **Agentless: Automatic**.

Agentless management is enabled for the selected devices and one of the following icons appears next to the device names:

: Agentless management is enabled for the device.

: Agentless management is enabled for the device, but the device is not currently reachable.

Depending on the device, the appliance uses various connection types to run commands on the selected devices, obtain inventory information, and display that information on the *Device Detail* page. Information is updated according to the inventory schedule for Agentless devices. See:

Managing inventory information

Schedule inventory data collection for managed devices

Enable Agentless management by entering device information manually

You can enable Agentless management by entering device information manually.

You can choose from the following connection types: SSH, SNMP, WinRM, and VMware. WinRM is the connection type to use for Windows devices.

1. Go to the *Devices* list:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Inventory**, then click **Device**s.
2. Select **Choose Action** > **New** > **Agentless Device** to display the *Agentless Device Connection Details* page.
3. Provide information according to the type of connection.

- **To set up SSH connections with devices, provide the following information:**

Option	Description
Name	The hostname or IP address of the device.
Asset Subtype	The asset subcategory, if applicable. This information enables you to identify and manage subtypes of assets, such as Device assets that are computers, printers, routers, and Software assets that run on Windows, Mac, or Linux systems in the inventory. See About Asset Subtypes, custom fields, and device detail preferences. **NOTE:** In a default installation, Device Assets include two Asset Subtypes for printer devices: *Laser Printer: Color* and *Laser Printer: Monochrome*. Each of these subtypes provides a common set of fields that apply to most printers. The appliance also comes with a set of printer templates for typical SNMP-enabled printer models, based on these Asset Subtypes. You can edit these templates or add new ones, as needed. When you apply a printer template to a device, the data defined in the template, such as toner levels or descriptions, is collected for the printer in the next inventory cycle. For more information, see About printer templates.
Connection Type	The connection method to use to connect to the device and obtain inventory information, in this case, SSH.
Port	The port number the appliance uses to connect to the device. No input is required for the following the default port number (22).
Credentials	The details of the service account required to connect to the device and run commands. Select existing credentials from the drop-down list, or select **Add new credential** to add credentials not already listed. See Add and edit User/Password credentials.
Sudo Password	The name of a service user account with permission to connect to devices. Using a service account and Sudo Password is useful when you want to avoid using root

Option	Description
	credentials to access devices. On some devices, however, higher privileges enable the appliance to retrieve more detailed inventory information.
Operating System	The operating system of the device.
Shell	The shell to use during connections. See Shell support for SSH connections.
Log Level	The level of information to display on the *Device Detail* page. To see only the most important messages, select **Critical**. To see all messages, select **Debug**.
Enable Inventory	The inventory collection option. If this option is selected, the appliance collects inventory information for the device according to the Agentless device inventory schedule. If this option is cleared, inventory information is not collected. In both cases, however, Agentless devices are counted.
DNS Server	The hostname of the DNS server to use when identifying the device hostname and other information. Providing the DNS server information enables the appliance to match the device to existing inventory information during updates. If the appliance cannot detect the device due to changes made to its hostname or IP address, inventory fails.
Relay Device	The name of the device that you want to use as a relay for agentless device inventory. A relay device that is used during discovery as a relay is used for agentless inventory, when a new device is provisioned automatically from discovery results. You can select a relay device on the *Discovery Schedule Detail* page. For more information, see Add a Discovery Schedule to perform a quick "what and where" scan of your network.

- **To set up SNMP connections with devices, provide the following information:**

Option	Description
Name	The hostname or IP address of the device.
Asset Subtype	The asset subcategory, if applicable. This information enables you to identify and manage subtypes of assets, such as Device assets that are computers, printers, or routers, and Software assets that run on Windows, Mac, or Linux systems in the inventory. See About Asset Subtypes, custom fields, and device detail preferences. **NOTE:** In a default installation, Device Assets include two Asset Subtypes for printer devices: *Laser Printer: Color* and *Laser Printer: Monochrome*. Each of these subtypes provides a common set of fields that apply to most printers. The appliance also comes with a set of printer templates for typical SNMP-enabled printer models, based on these Asset Subtypes. You can edit these templates or add new ones, as needed. When you apply a printer template to a device, the data defined in the template, such as toner levels or descriptions, is collected for the printer in the next inventory cycle. For more information, see About printer templates.
Connection Type	The connection method to use to connect to the device and obtain inventory information, in this case, SNMP.

Option	Description
	SNMP (Simple Network Management Protocol) is a protocol for monitoring managed devices on a network. To enable SNMP, port 161 must be open on the appliance and on the device. SNMP scan results include all SNMP capable devices. Remote shell extensions enable the appliance to connect, run commands, and capture information that can be managed as inventory. For more information about SNMP options, see Add a Discovery Schedule for SNMP-enabled non-computer devices.
SNMP Version	The version of SNMP to use for connections. SNMPv1 and SNMPv2c do not use authentication or encryption. SNMP v3 uses authentication and encryption algorithms to increase the security of SNMP communications. When you configure the SNMP v3 options, the appliance performs an SNMP v3 scan on selected devices. If that scan fails, the appliance attempts an SNMP v1 scan using the specified **Public String**
Credentials	The details of the service account required to connect to the device and run commands using SNMP v3. Select existing credentials from the drop-down list, or click **Add new credential** to add credentials not already listed. Credentials are not required for SNMPv1 and SNMPv2c. See Add and edit User/Password credentials.
Inventory Configurations	One or more inventory configurations for the new SNMP agentless device, such as *Brother Laser Printer: Color*, and others.
Inventory Type	The method used to collect inventory information. • **Inventory**: Collect a subset of device information, such as the IP Address, MAC Address, and device name. • **Inventory/Walk**: Conduct a full SNMP walk to collect inventory information. The full walk results appear on the *Device Detail* page. **NOTE:** SNMP inventory walk does not support non-English characters on Windows devices. If it encounters non-English characters, the SNMP inventory process reports an error and stops loading inventory information.
Log Level	The level of information to display on the *Device Detail* page. To see only the most important messages, select **Critical**. To see all messages, select **Debug**.
Enable Inventory	The inventory collection option. If this option is selected, the appliance collects inventory information for the device according to the Agentless device inventory schedule. If this option is cleared, inventory information is not collected. In both cases, however, Agentless devices are counted.
DNS Server	The hostname of the DNS server to use when identifying the device hostname and other information. Providing the DNS server information enables the appliance to match the device to existing inventory information during updates. If the appliance cannot detect the device due to changes made to its hostname or IP address, inventory fails.
Relay Device	The name of the device that you want to use as a relay for agentless device inventory. A relay device that is used during discovery as a relay is used for agentless inventory, when a new device is provisioned automatically from discovery results. You can

Option	Description
	select a relay device on the *Discovery Schedule Detail* page. For more information, see Add a Discovery Schedule to perform a quick "what and where" scan of your network.

- **To set up WinRM connections with devices, provide the following information:**

Option	Description
Name	The hostname or IP address of the device.
Asset Subtype	The asset subcategory, if applicable. This information enables you to identify and manage subtypes of assets, such as Device assets that are computers, printers, or routers, and Software assets that run on Windows, Mac, or Linux systems in the inventory. See About Asset Subtypes, custom fields, and device detail preferences. **NOTE:** In a default installation, Device Assets include two Asset Subtypes for printer devices: *Laser Printer: Color* and *Laser Printer: Monochrome*. Each of these subtypes provides a common set of fields that apply to most printers. The appliance also comes with a set of printer templates for typical SNMP-enabled printer models, based on these Asset Subtypes. You can edit these templates or add new ones, as needed. When you apply a printer template to a device, the data defined in the template, such as toner levels or descriptions, is collected for the printer in the next inventory cycle. For more information, see About printer templates.
Connection Type	The connection method to use to connect to the Windows device and obtain inventory information, in this case, WinRM.
Port	The port number the appliance uses to connect to the device. No input is required for the following default port number: 5985.
Credentials	The details of the service account required to connect to the device and run commands. Select existing credentials from the drop-down list, or select **Add new credential** to add credentials not already listed. See Add and edit User/Password credentials.
Require Kerberos	If selected, Kerberos is required for authentication. NTLM will not be used as an alternative when Kerberos is unavailable. Using Kerberos requires DNS Lookup to be enabled in the same discovery configuration. The DNS Server is also required in the local appliance network settings.
Log Level	The level of information to display on the *Device Detail* page. To see only the most important messages, select **Critical**. To see all messages, select **Debug**.
Enable Inventory	The inventory collection option. If this option is selected, the appliance collects inventory information for the device according to the Agentless device inventory schedule. If this option is cleared, inventory information is not collected. In both cases, however, Agentless devices are counted.
DNS Server	The hostname of the DNS server to use when identifying the device hostname and other information. Providing the DNS server information enables the appliance to match the device to existing inventory information during updates. If the appliance

Option	Description
	cannot detect the device due to changes made to its hostname or IP address, inventory fails.
Inventory Hyper-V or Virtual Machine Manager	Select this option to allow the appliance to import a Microsoft Hyper-V or System Center Virtual Machine Manager infrastructure using agentless management. For more information about this feature, see Add a Discovery Schedule for a Microsoft Hyper-V or System Center Virtual Machine Manager.
Relay Device	The name of the device that you want to use as a relay for agentless device inventory. A relay device that is used during discovery as a relay is used for agentless inventory, when a new device is provisioned automatically from discovery results. You can select a relay device on the *Discovery Schedule Detail* page. For more information, see Add a Discovery Schedule to perform a quick "what and where" scan of your network.

- **To set up a VMware® device, provide the following information:**

Option	Description
Name	The host name or IP address of the ESXi host or the vCenter Server.
Asset Subtype	The asset subcategory, if applicable. This information enables you to identify and manage subtypes of assets, such as VMware devices. For example, hypervisors (ESXi hosts). See About Asset Subtypes, custom fields, and device detail preferences.
Connection Type	The connection method to use to connect to the VMware device and obtain inventory information.
VMware Type	The VMware device type: **ESXi** or **vCenter Server**. **NOTE:** vCenter Server devices do not count against the total number of device licenses. That is because these device instances are only used to establish relationships between the vCenter Servers, ESXi hosts, and the virtual machines running on them.
Credentials	The details of the service account required to connect to the device and run commands. Select existing credentials from the drop-down list, or select **Add new credential** to add credentials not already listed. An account with read-only access can be used. See Add and edit User/Password credentials.
Log Level	The level of information to display on the *Device Detail* page. To see only the most important messages, select **Critical**. To see all messages, select **Debug**.
Enable Inventory	The inventory collection option. If this option is selected, the appliance collects inventory information for the device according to the Agentless device inventory schedule. If this option is cleared, inventory information is not collected. In both cases, however, Agentless devices are counted.
DNS Server	The hostname of the DNS server to use when identifying the device hostname and other information. Providing the DNS server information enables the appliance to match the device to existing inventory information during updates. If the appliance

Option	Description
	cannot detect the device due to changes made to its hostname or IP address, inventory fails.

4. Click **Test Connection**.

   The connection status appears.

5. Click **Save**.

   The Agentless device is added. If *Enable Inventory* is selected, inventory information is updated according to the Agentless device inventory schedule. See Schedule inventory data collection for managed devices.

Shell support for SSH connections

Operating systems vary in their support of shells used for SSH connections between the appliance and managed devices.

The following table shows the shells available for SSH connections for each operating system.

Table 22. Shell support for SSH connections by operating system

Operating system	Default shell	Supported shells
CentOS	bash	bash, sh
Debian Linux	bash	bash, sh
Fedora	bash	bash, sh
FreeBSD	csh	bash, csh, sh
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

Edit Agentless device connection details or delete Agentless devices

You can edit the device connection details for Agentless devices and you can delete Agentless devices as needed.

1. Go to the *Devices* list:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.

b. On the left navigation bar, click **Inventory**, then click **Device**s.

2. Click the name of an Agentless device that was entered manually to display the *Device Detail* page.
3. In the *Summary* section, click **Edit** in the *Device Entry Type* row to display the *Agentless Device Connection Details* page.
4. Do one of the following:

   - **Modify the connection details as needed, then click Save. See Enable Agentless management by entering device information manually.**
   - **To delete the device, click Delete.**
   - **For Agentless devices enrolled in KACE Cloud Mobile Device Managed (MDM), to remove the device's association with KACE Cloud MDM and revert to Agent-only inventory records, click Remove Agentless Integration.**

Using SNMP Inventory Configurations to identify specific SNMP objects and non-computer devices to add to inventory

You can identify specific SNMP (Simple Network Management Protocol) objects and non-computer devices to be inventoried so that you can expand or limit the inventory to fit your needs. In addition, the appliance enables you to map SNMP OIDs (Object Identifiers) to particular fields in the appliance inventory table, using Asset Subtypes.

IMPORTANT: For SNMP devices, you must assign the appropriate Asset Subtype when the device is configured. You cannot add or change SNMP Asset Subtypes after they have been configured.

SNMP is one of the possible methods that appliance Agentless Inventory uses to extract data for inventory and integration into the appliance. The appliance uses the RFC1213 MIB (Management Information Base) as the primary data gathering layer, because it contains data that is specific to all SNMP-capable devices. All SNMP-capable devices expose RFC1213 data. For more information, go to http://tools.ietf.org/html/rfc1213.

With the appliance SNMP inventory configuration feature, you can define an additional set of OIDs to be collected during inventory beyond the standard RFC1213 data. This enables instant extensibility and robustness to what would otherwise be limited in terms of the amount of data that could be gathered from each device.

Related Topics

About Asset Subtypes, custom fields, and device detail preferences

Obtain a list of object identifiers (OIDs) using the Administrator Console

If you do not have a vendor-provided management information base (MIB) or a generally available MIB for an object, you can obtain a list of object identifiers by using the appliance to probe the object.

You can define an additional set of OIDs to be collected during inventory beyond the standard RFC1213 data, which expands the amount of data that can be gathered from each device. To find these OIDs, you can use a MIB browser on MIBs you have obtained elsewhere. With the appliance, you can perform an SNMP full walk either through device discovery or device inventory if you do not have access to a MIB otherwise.

1. Perform an SNMP full walk for an object.

   - **Scan using a Discovery Schedule. See Discovering devices on your network.**
   - **Scan using inventory data collection. See Schedule inventory data collection for managed devices.**

2. Go to the *Device Detail* page for the scanned object:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Inventory**, then click **Device**s.

c. Click the name of the object on the *Devices* list page.

3. Click **SNMP Data** in the *Inventory* section to display the results of the full walk.
4. Collect the relevant OIDs from the list.

Map the OIDs to fields in the appliance inventory table so that their information can be integrated into inventory. See Map Object Identifiers to fields in the inventory table.

Map Object Identifiers to fields in the inventory table

You can map SNMP (Simple Network Management Protocol) OIDs (Object Identifiers) to particular fields that you have created as Asset Subtypes. You can use the resulting SNMP Inventory Configurations to expand your inventory information to include data from non-computer devices.

- You have identified the relevant OIDs to be contained in the configuration:
  - # You have used a MIB browser on a vendor-supplied Management Information Base.
  - # You have performed an SNMP Full Walk on a target object with the appliance, and have reviewed the OIDs displayed in **SNMP Data** of the *Inventory Information* section of the object's *Device Detail* page. See Discovering devices on your network.
- You have created appropriate Asset Subtypes for the non-computers devices you want to manage in inventory. See Add Asset Subtypes and select Device Detail page preferences.

The *SNMP Inventory Configurations* list page provides you with the tool to create new mappings or manage existing ones.

After you have determined the OID data you want to collect, you select a subtype for the device from categories that are the same as those on the *Device Detail* page. You then select a property of that category, the result of which maps the OID to a field in the inventory table. The SNMP object appears in the device inventory after the next scan.

For example, if you had a printer in inventory, added manually or through a discovery schedule, you could use an SNMP Inventory Configuration to have the printer report cartridge ink levels to the appliance. In this case, you would use an Asset Subtype of *Printer* that you have created as a subtype of device, with a field named *Toner Level*.

1. Go to the *SNMP Inventory Configurations* list page:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Inventory**, then click **SNMP Inventory Configurations**.
2. Select **Choose Action** > **New**.
3. Type a name for the configuration in the *Name* field.

   IMPORTANT: For SNMP devices, you must assign the appropriate Asset Subtype when the device is configured. You cannot add or change SNMP device subtypes after they have been configured.
4. Select an Asset Subtype that identifies the type of device you want to inventory.
5. Map an OID to an appliance inventory field:
   a. Click the Add button: +.

      A new row appears under the headings.
   b. Enter the OID in the text box under *Object Identifier (OID)*.
   c. Select a category from the drop-down list under *Category*.

      The categories match those identified on the *Asset Subtype Detail* page.
   d. Select a property from the drop-down list under *Property*.

      The properties that appear are dependent on the subtype and the category you selected.
   e. Click **Save** at the end of the row.
6. Map as many additional OIDs as you want for your purposes, and click **Save** at the bottom left of the page.

Apply the configuration to an object. See Apply an SNMP Inventory Configuration to a device.

Apply an SNMP Inventory Configuration to a device

You can apply an SNMP Inventory Configuration to a device so that the additional data can be collected during the next scan for that device.

You have created the configuration. See Map Object Identifiers to fields in the inventory table.

NOTE: You can apply SNMP Inventory Configurations only to SNMP-managed Agentless devices.

1. Go to the *Devices* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Inventory** to display the *Devices* page.
2. Select the check boxes next to one or more devices.
3. Select **Choose Action** > **Apply SNMP Configurations** to display the *Apply SNMP Configurations* dialog.
4. Drag the configurations you want to apply into the *Apply these SNMP configurations* box.

   You can search for a particular configuration by starting to type its name into the *Search SNMP Configurations* field.
5. Click **Apply SNMP Configurations**.

   The *Devices* list page reappears after the configuration is applied.

The information appears for the device after the next regularly scheduled reporting time or forced inventory update.

Related topics

Schedule inventory data collection for managed devices

Forcing inventory updates

About printer templates

The appliance also comes with a set of printer templates for typical SNMP (Simple Network Management Protocol) printer models. You can apply these SNMP configurations to printer devices, as needed.

The *SNMP Inventory Configurations* list page displays the available printer templates. When you apply a printer template to a device, the data defined in the template, such as toner levels or descriptions, is collected for the printer in the next inventory cycle.

A default installation includes a set of templates for the following laser printers, with two variation for each brand to accommodate monochrome and color printers: Brother, Canon, HP, Lexmark, and Xerox.

You can edit or create these templates, as needed. To create or edit a printer template, you must have the relevant SNMP OIDs (Object Identifiers) for the fields that exist as the associated Asset Subtypes. The appliance comes with two Asset Subtypes that capture printer-specific fields such as toner levels: *Laser Printer: Color* and *Laser Printer: Monochrome*. For more information about mapping OIDs, see Map Object Identifiers to fields in the inventory table. For details about Asset Subtypes and to find out how they relate to SNMP configurations, see About Asset Subtypes, custom fields, and device detail preferences.

Adding devices manually in the Administrator Console or by using the API

You can add devices to inventory manually, either within the **Administrator Console** or by using the inventory API (application programming interface).

Adding devices manually is useful when you want to track device information, but you do not want to manage devices by installing the KACE Agent or using Agentless management.

Inventory for manual devices must be updated or uploaded manually. The appliance does not receive scheduled inventory updates from manual devices.

About managing devices

Managing devices is the process of using the appliance to collect and maintain information about devices on your network and performing tasks such as monitoring device status, creating reports, and so on.

To add devices to the appliance inventory, you can:

- **Install the KACE Agent on devices**. Devices are automatically added to inventory after the Agent is installed on them and the Agent reports inventory to the appliance. See Provisioning the KACE Agent.
- **Enable Agentless management for devices**. Agentless management is especially useful for devices that cannot have the KACE Agent installed, such as devices with unsupported operating systems. See Managing Agentless devices.
- **Upload inventory information for devices manually**. See Adding devices manually in the Administrator Console or by using the API.

NOTE: Your product license agreement entitles you to manage a specified number of devices that are classified as Managed Computers, Chromebooks & Network Devices, and Monitored Computers. Devices count toward these limits even if such devices are MIA (missing in action) or no longer in use. However, devices that are added to inventory manually, or through the API, do not count toward license limits. See View product licensing information.

For information about the features available to devices, see Features available for each device management method.

Tracking changes to inventory settings

If History subscriptions are configured to retain information, you can view the details of the changes made to settings, assets, and objects.

This information includes the date the change was made and the user who made the change, which can be useful during troubleshooting. See About history settings.

About inventory change history

Change history for devices begins when there is a change to the information collected during the first report.

The first time a managed device reports inventory to the appliance, the information is considered to be a baseline report. As such, it is not recorded in the change history.

Add devices manually with the Administrator Console

You can add devices to the appliance inventory manually by entering device information on the *Device Detail* page.

Once created, manual records are not touched or modified by the appliance or Agents. Subsequently, the fields in a manual record can only be updated manually by an administrator.

1. Go to the *Devices* list:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.

b. On the left navigation bar, click **Inventory**, then click **Device**s.

2. Select **Choose Action** > **New** > **Manual Device** to display the *Device Detail* page.
3. Do one of the following:

   - **Under *Import device.xml*, click Choose File to find and import an XML file that includes device inventory information. See Valid XML schema for Windows and Upload an XML file using the Administrator Console.**

     In the *Summary* section, enter a *Name* for the device, then skip to step 10.

   - **In the *Summary* section, provide the following information:**

Item	Description	Database field
System Name	The hostname or IP address of the device.	NAME
System Description	A description of the device.	SYSTEM_DESCRIPTION
Model	The device model.	CS_MODEL
Chassis Type	The type of device, such as desktop or laptop.	CHASSIS_TYPE
IP Address	The IP address of the device.	IP
MAC	The device's Media Access Control (MAC) address number.	MAC
OS Name	The operating system of the device, such as Windows, Mac OS X, or Linux.	OS_NAME
Service Pack	The service pack version number (Windows only).	SERVICE_PACK
Device Timezone	The KACE Agent installed on the device uses this timezone.	TZ_AGENT
User	A user associated with this device.	USER
Domain	The domain of the device.	CS_DOMAIN
Notes	Any additional information you want to provide.	NOTES

4. In the *Hardware* section, provide the following information:

Item	Description	Database field
RAM Maximum	The maximum amount of random-access memory (RAM) available.	RAM_MAX
RAM Total	The total amount of random-access memory (RAM) on the device.	RAM_TOTAL
RAM Used	The amount of random-access memory (RAM) in use on the device.	RAM_USED

Item	Description	Database field
System Manufacturer	The device manufacturer.	CS_MANUFACTURER
System Model	The device model.	CS_MODEL
Service Tag	Information used to identify device service.	SERVICE_TAG
Asset Tag	Information used to identify device hardware.	ASSET_TAG
Motherboard Primary Bus	The main bus.	MOTHERBOARD_PRIMARY_BUS
Motherboard Secondary Bus	The peripheral bus.	MOTHERBOARD_SECONDARY_BUS
Architecture	The architecture of the device operating system, such as x86 or x64.	SYS_ARCH
Virtual Device	Used to identify devices that are virtual, such as devices running on VMware platforms. Not displayed for physical devices, such as laptops and servers.	VIRTUAL
Processors	The CPU count, type, and manufacturer.	PROCESSORS
CD/DVD Drives	The configuration of CD-ROM and DVD-ROM drives installed on the device.	CDROM_DEVICES
Sound Devices	Information about audio devices on the device.	SOUND_DEVICES
Monitors	The type and manufacturer of the monitor attached to the device. This field is not displayed for virtual devices.	MONITOR
Video Controllers	Information about video controllers on the device.	VIDEO_CONTROLLERS
BIOS Name	The BIOS name.	BIOS_NAME
BIOS Release Date	The date the BIOS version was released.	BIOS_RELEASE_DATE
BIOS Version	The BIOS version.	BIOS_VERSION
BIOS Manufacturer	The BIOS manufacturer.	BIOS_MANUFACTURER
BIOS Description	The BIOS description.	BIOS_DESCRIPTION
BIOS Identification Code	The BIOS identification code.	BIOS_IDENTIFICATION_CODE

Item	Description	Database field
BIOS Serial Number	The BIOS serial number.	BIOS_SERIAL_NUMBER

5. In the *Printers* section, specify printer information related to the device.
6. In the *Agent* section, specify the version number of the KACE Agent installed on the device.
7. In the *User* section, provide user information.

Item	Description	Database field
User Logged	The user currently logged in to the device. This entry includes the username and the domain to which the user belongs.	USER_LOGGED
User Fullname	The full name of the user who owns the device.	USER_FULLNAME
User Domain	The domain to which the user belongs.	USER_DOMAIN
Last User	The name of the most recent user who logged in to the device. Some devices might have multiple users.	USER

8. In the *Operating System* section, provide information about the operating system installed on the device.

Item	Description	Database field
Operating System Version	The version number of the operating system.	OS_VERSION
Operating System Build Version	The build number of the operating system.	OS_BUILD
Number	The number of the operating system.	OS_NUMBER
Operating System Major Version	The number that identifies the major version of the operating system.	OS_MAJOR
Operating System Minor Version	The number that identifies the minor version of the operating system.	OS_MINOR
Minor Version (2)	Additional operating system version information.	OS_MINOR2
Internet Explorer Version	The version of Internet Explorer installed on the device.	IE_VERSION
.NET Versions	The version or versions of .NET installed on the device.	DOT_NET_VERSIONS
Operating System Architecture	The architecture of the device operating system, such as x86 or x64.	OS_ARCH
Operating System OS Name	The name of the device operating system.	OS_NAME

Item	Description	Database field
Edge Version	The version of Microsoft Edge installed on the device.	EDGE_VERSION
Family	The product family of the operating system.	OS_FAMILY
Service Pack		
Operating System Installed On	The date the operating system was installed.	OS_INSTALLED_DATE
Last Startup	The last time the operating system was turned off.	LAST_REBOOT
Last System Shutdown	The last time the operating system was turned off.	LAST_SHUTDOWN
Uptime Since Last Reboot	The length of time the operating system has been running.	LAST_REBOOT
Domain	The domain of the device.	CS_DOMAIN
System Directory	The location of the system directory.	SYSTEM_DIRECTORY
Registry Size	The size of the registry.	REGISTRY_SIZE
Registry Maximum Size	The maximum size of the registry.	REGISTRY_MAX_SIZE
WMI Status	The status of the Windows Management Instrumentation (WMI) service (Windows Devices only).	WMI_STATUS

9. Click **Save**.

   The manual device icon appears in the device's **Status** column on the *Devices* page: . Inventory for manual devices must be updated manually.

Adding devices manually using the API

You can add devices to the appliance manually by creating an XML file and uploading that file to the appliance using the API (application programming interface). Adding devices in this way is useful for devices that might not be able to run the KACE Agent for security reasons, and devices that cannot connect to the LAN (Local Area Network) to report inventory.

The XML file you create can be modeled on the sample script in this section.

Devices that are added to inventory through the API do not count toward the license limit. See View product licensing information.

Application inventory that is uploaded through the API is displayed on the *Software page*, but it is not displayed on the *Software Catalog* page. See:

- Managing applications on the Software page
- Managing Software Catalog inventory

NOTE: The inventory API supports HTTP and HTTPS communications, depending on your appliance configuration. To upload inventory information, use the following URL: `http://`**appliance_hostname**`/service/wsapi.php`, where **appliance_hostname** is the host name of your appliance.

Submit inventory information using the API

To submit inventory using the API, you first need to generate an XML file that contains the inventory information.

For examples, see:

- Valid XML schema for Windows
- Example using the XML schema for Windows devices
- Valid XML schema for Linux and Mac devices

After you generate an XML file with the expected content, you can submit inventory using the API.

1. (Required) Request a session key:

   Submit `keyreq=true` in the body of the request to get a session string in response.

2. (Required) Construct the authentication token:
   a. Construct the `auth` string as:

      `session_string + '|' + MD5 of API password`

   b. Run MD5 on the `auth` string.
3. (Required for new devices) Request a device UUID:

   Submit `req=newuuid&key=$auth` in the body of the request to get a UUID in response.

4. (Required) Submit inventory XML data:

   Submit `req=loadxml&key=$auth&KUID=$uuid&version=6.0` in the `GET` line and inventory XML in the body of the request.

   See Sample Perl script.

Sample Perl script

You can use Perl scripts to upload XML files with device inventory information to the appliance.

The following is a sample Perl script that uploads a user-created XML file to the appliance. For information about using this script, contact **Quest Support** at 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";
```

Valid XML schema for Windows

Files used to upload inventory information for Windows devices must conform to valid XML schemas.

The following is an example of a valid XML schema for Windows devices.

```
<?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>
```

Example using the XML schema for Windows devices

You can view an example of a file that conforms to the valid XML schema for Windows devices.

The following is an example of valid XML that uses the schema in Valid XML schema for Windows.

```
<?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>konea.exe</NAME>
    <COMMAND_EXE>C:\Program Files (x86)\Quest\KACE\konea.exe</COMMAND_EXE>
    <COMMAND_ARGS/>
    <FILE_INFO>
      <FILE_NAME>konea.exe</FILE_NAME>
      <FILE_DESCRIPTION>konea</FILE_DESCRIPTION>
      <FILE_VERSION>255.239.6</FILE_VERSION>
      <PRODUCT_NAME>KACE Agent</PRODUCT_NAME>
      <PRODUCT_VERSION>255.239.6</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>
```

Valid XML schema for Linux and Mac devices

Files used to upload inventory information for Linux and Mac devices must use valid XML schemas.

The following is an example of an XML schema for Linux and Mac devices.

```
<?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>
```

Upload an XML file using the Administrator Console

You can upload an XML file that contains device inventory information using the **Administrator Console**. This type of information is referred to as manual inventory information.

The KACE Agent is installed on the device that is having its inventory information added.

You create the XML file on the device to be inventoried, then move to the appliance to upload the file.

Manual inventory information appears on the *Software* page but it does not appear on the *Software Catalog* page. See:

- Managing applications on the Software page
- Managing Software Catalog inventory

1. Generate an XML file that contains the information.
    a. On a device where the KACE Agent is installed, open a command prompt or terminal window.
    b. Go to the Quest KACE installation directory.

    For example:

    # Windows 32-bit systems: `C:\Program Files\Quest\KACE`
    # Windows 64-bit systems: `C:\Program Files (x86)\Quest\KACE`
    # Mac OS X systems: `/Library/Application Support/Quest/KACE/bin`
    # Linux systems: `/opt/quest/kace/bin`

    c. Enter the following command:

    `KInventory -machine -output` filename

    Where **filename** is the path to the XML file you want to create. If the path contains spaces, enclose the entire path in double quotation marks.

    The Agent collects the inventory data and generates the XML file.
2. On the appliance Administrator Console, go to the *Devices* list:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Inventory**, then click **Device**s.
3. Select **Choose Action** > **New** > **Manual Device** to display the *Device Detail* page.
4. Under *Import Device*, click **Browse**.
5. Select the file, then click **Open** or **Choose**.
6. Click **Save**.

The device's information is added to inventory. If you uploaded an XML file, the appliance ignores all other information on the page and uses the XML file for inventory information.

Forcing inventory updates

You can force managed devices to update their inventory information outside of the regularly scheduled reporting times.

To force inventory updates, one of the following conditions must be met:

- The KACE Agent must be installed on the devices and there must be an active messaging protocol connection between the appliance and the devices.
- Agentless management must be enabled for the devices.

You cannot force an update on devices that are not either Agent-managed or Agentless-managed devices.

Any Managed Installations associated with selected devices are always deployed in order, regardless of whether their specified software packages come from the Software Catalog or the Software list.

Force inventory updates from the appliance

You can use the appliance **Administrator Console** to force devices to report inventory.

1. Go to the *Devices* list:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Inventory**, then click **Device**s.
2. Select the check boxes next to the devices whose inventory you want to update.

    To avoid overwhelming the appliance, do not select more than 50 devices to update at once.
3. Select **Choose Action** > **Force Inventory**.

Inventory information is updated.

Force inventory updates from Windows devices

You can force Windows devices to report inventory by running commands on the devices.

1. Log in to the Windows device and open a command prompt.
2. Go to one of the following directories:
    # On 32-bit systems: `C:\Program Files\Quest\KACE\`
    # On 64-bit systems: `C:\Program Files (x86)\Quest\KACE\`

    NOTE: For Windows Vista and later, use *Run as Administrator* when running the command.
3. Enter the following command:

```
runkbot 4 0
```

Inventory information is updated.

Force inventory updates from Mac OS X devices

You can force Mac OS X devices to report inventory by running commands on the devices.

1. Log in to the Mac OS X device and open a terminal from **Applications** > **Utilities**.
2. Go to the following directory:

```
/Library/Application Support/Quest/KACE/bin/
```

3. Enter the following command:

```
sudo ./runkbot 2 0
```

Inventory information is updated.

Force inventory updates from Linux devices

You can force Linux devices to report inventory by running commands on the devices.

1. Log in to the Linux device and open a terminal from **Applications** > **System Tools**.
2. Go to the following directory:

   ```
   /opt/quest/kace/bin/
   ```

3. Enter the following command:

   ```
   sudo ./runkbot 2 0
   ```

Inventory information is updated.

About Remote Control

The Remote Control feature, provided by Splashtop®, enables you to access the agent-managed Windows and macOS devices remotely. It enhances remote management capabilities, providing a seamless and efficient way for users to control and troubleshoot devices remotely. You can access this feature through the Admin console. This topic details the key functionalities and steps for configuring and using the remote control feature.

NOTE: KACE Remote Control powered by Splashtop® is an optional paid add-on feature. For pricing information, contact your sales representative.

To get started with the remote control access you must follow the steps below:

- Install the Remote Control Agent application on the agent-managed devices (Windows/Mac) and the Splashtop for RMM application on the controlling device.
- Configure the Remote Control Agent settings and permissions.
- Configure Remote Access options as desired.
- Start a remote control session on agent-managed Windows or macOS device.

NOTE: Ensure that your device has active Internet connection and the proxy settings on your device's network settings are configured properly. The Systems Management Appliance must be able to reach the following domain to generate session token: https://st-rmm-kace.api.splashtop.com. For more information, see Make necessary websites accessible to the appliance

Privacy and Data Safety in Remote Connections

When using the Remote Control feature, your information and data remains secure, private, and fully protected. The integration with the Remote Control Agent application ensures that none of your information is stored on their servers, providing an additional layer of security.

For more information on the data protection practices, visit the links:

https://www.splashtop.com/security/compliance

https://www.splashtop.com/security/practices/technical-and-organizational-measures

Install Remote Control Applications

You must install the Remote Control Agent application on the agent-managed devices (Windows/Mac) and the Splashtop for RMM application on the controlling device. This topic describes the different methods of installing the applications.

Install Remote Control Agent

The following are the different ways to install Remote Control Agent on the agent-managed devices (Windows/Mac) :

- Apply Smart Label
- Apply the Remote Control Label to Devices
- Enable Remote Control feature for an Existing label
- Enable Remote Control Feature for an Existing Label Group
- Enable the Deploy Remote Control Agent option

Install Splashtop for RMM

The following are the different ways to install the Splashtop for RMM application on the controlling device:

- Download from the Control Panel page
- Download from the pop-up window after you initiate a remote control session

Apply Smart Label to Devices

You can create a Smart Label with the Remote Control feature enabled. Once a smart label gets applied to a device, the required remote control applications get installed automatically on device.

To apply a smart label to a device,

1. Create a Smart Label with enabled remote control feature. Refer Add Smart Labels

   The Smart Label gets applied automatically to the devices that fulfill the conditions added to the label at inventory interval. The Remote Control Agent application required for remote control gets installed on the devices automatically.

Apply the Remote Control Label to Devices

You can find the Remote Control label in the list of manual labels created for the appliance. You need to apply this label to the desired device or devices. This manual label initiates the installation of remote control application on the devices to which the label is applied.

To apply the Remote Control label,

1. Go to **Inventory** > **Devices** to display the **Devices** page.
2. On the *Devices* page, select the device or devices to which you want to apply the Remote Control label.
3. Click **Choose Actions** > **Apply Labels**. The **Apply Labels** pop-up window displays.
4. Drag and drop the RemoteControl label to the **Apply these label** pane, and then click **Apply Labels**.

   The label gets applied to the device or devices. The remote control icon , after next inventory cycle or force inventory, appears near the device name. You can click this icon to start remote control session.

Enable Remote Control Feature for an Existing Label

You can enable the Remote Control feature manually for an existing label from the Label Details page. This feature gets enabled on devices that have the label assigned.

To enable the Remote Control feature for a label,

1. Go to the *Label Detail* page:
   a. On the *Label Management* panel, click **View and edit master list of labels** under the **Labels** section to display the *Labels* page.
   b. Click the label name to display the *Label Detail* page.
2. Select the **Remote Control** option, in the **Restrict Labels Usage to** section, and save it.

The remote control feature is enabled and gets applied to the devices that have the label assigned.

Enable Remote Control Feature for an Existing Label Group

You can enable the Remote Control feature manually for an existing label group from the Label Details page. This feature gets enabled on the devices that have the sub-label assigned where the sub-label inherits the permission of Remote Control set on its group label.

1. Go to the *Label Detail* page:
    a. On the *Label Management* page, click **View and edit master list of labels** under the **Labels** section to display the *Labels* page.
    b. Click the label group name to display the *Label Detail* page.
2. Select the **Remote Control** option, in the **Restrict Labels Usage to** section, and save it.

The remote control feature is enabled through permission set at group label which is inherited to the sub-label applied to the devices.

Enable the Deploy Remote Control Agent option

You can deploy the Remote Control Agent application when you enable the **Deploy Remote Control Agent to all devices** option. Once enabled, the Remote Control Agent application is installed on all agent-managed Windows and macOS devices.

NOTE: To deploy the Remote Control Agent to all agent-managed Windows and macOS devices, the number of Managed Computers license should be equal to the number of Remote Control computers.

To enable the option,

1. On the left navigation bar, in the *Settings* section, click **Control Panel.**
2. On the *Control Panel* page, in the *Remote Control Settings* section, select **Configure Remote Control Agent Settings**, to open the *Remote Control Settings* page.
3. Go to the *Deploy Remote Control Agent* section, and select the **Deploy Remote Control Agent to all devices** check box, and then save it.

    This installs the Remote Control Agent application to all the agent-managed Windows and Mac devices associated with the SMA.

Download from the Control Panel page

You can install the Splashtop for RMM application on the controlling device by downloading it from the Control Panel page.

When you click the desired OS name, the installer files get downloaded. You must install the application before initiating a remote control session.

To download the Splashtop for RMM application,

1. On the left navigation bar, in the *Settings* section, click **Control Panel.**
2. On the *Control Panel* page, in the *Remote Control Settings* section, select the desired OS name **Windows** or **Mac** to download the installer file.

    The installer file gets downloaded on your device.
3. Install the application to run the remote control session smoothly.

Download from the pop-up window after you initiate a remote control session

You must have the Splashtop for RMM application on the controlling device before you initiate the remote control session. When you initiate the session for the first time, a window pops up that has the installers for the application.

To download the installers,

1. Go to **Inventory** > **Devices** to display the **Devices** page.
2. On the **Devices** page, click the remote control icon near the device name you want to connect with.

    A pop-up window displays that has links to download the installer files.

Or

On the **Devices** page, click the device name to open the *Device Details* page. On the *Device Details* page, click the **Remote Control** button.

A pop-up window displays that has links to download the installer files.

3. If the Splashtop for RMM application is not installed, click the desired OS installer link to download the installer. The installer file gets downloaded on your device.
4. Run the installer to install the application. Once you install the Splashtop for RMM application, you can initiate the remote control session.

Configure Remote Control Settings

You can configure the remote control settings for agent-managed devices. The settings will be updated when the remote control session is initiated.

You can configure the remote control settings in the following ways:

- Configure Settings on the Control Panel page
- Configure Settings Before Starting the Session

Configure Settings on the Control Panel page

The settings applied on this page are the default settings for remote control sessions on all the macOS and Windows devices present in the device inventory.

To configure the remote control settings,

1. On the left navigation bar, in the *Settings* section, click **Control Panel.**
2. On the *Control Panel* page, in the *Remote Control Settings* section, select **Configure Remote Control Agent Settings**, then provide the following information:

Section	Option	Description
Remote Session Settings		
	Security Options	Choose one of the options from the list to set the default security option for a remote control session.
	Audio Routing Options	Choose the option to configure the Remote Control Agent application's audio.
	Permissions Option	Select this option if a device user should allow it before a remote access session starts.
	Resolution Options	Set the default resolution of the Splashtop for RMM application.
	Connection Status Timeout	Specifies the maximum duration to keep a device in connected status. Once the limit is reached, the connection status icon resets back to **ready to connect**. The time must be a whole number between 1 and 72. After this duration, the system will update session status from **active** to **timed out** to display icon. It will not terminate any active remote control session.

Section	Option	Description
Deploy Remote Control Agent	Deploy Remote Control Agent to all devices	Select this option to install the Remote Control Agent to all devices. **NOTE:** To deploy the Remote Control agent to all devices, the number of Managed Computers license should be equal to the number of Remote Control computers. To check the license numbers, click the icon on upper right corner and then icon.
Remote Control Agent Settings		
	Hide tray icon from Taskbar	Select this option to hide the icon from the taskbar.
	Auto Launch	Select this option to launch the Remote Control agent automatically.
	Customize Blank Screen Logo	Upload a custom logo (in PNG format) to be displayed on the blank screen when a remote session is active. Upload a file with size upto 15MB.

3. Click **Save**.

NOTE: You can modify the settings anytime before starting a remote control session. The changes gets applied when a remote control session is initiated.

Configure Settings Before Starting the Remote Control Session

You can customize the remote control settings before starting a Remote control session. The customized settings are applicable to the particular device for that particular session.

To customize the remote control settings,

1. Go to **Inventory** > **Devices** to display the **Devices** page.

   On the *Devices* page, click the remote control icon near the device name you want to connect with.

   Or

   Go to **Inventory** > **Devices** to display the *Devices* page.

   Click the device name to open the device's details page.

   Click the **Remote Control** button on the page.

2. In the *KACE remote control powered by Splashtop®* dialog box that appears, select **Use Custom Settings**, and modify the following details as required.

Section	Option	Description
Remote Session Settings		
	Security Options	Choose one of the options from the list to set the default security option for a remote control session.

Section	Option	Description
	Audio Routing Options	Choose the option to configure the Remote Control Agent application's audio.
	Permissions Option	Select this option if a device user should allow it before a remote access session starts.
	Resolution Options	Set the default resolution of the Splashtop for RMM application.
	Connection Status Timeout	Specifies the maximum duration to keep a device in connected status. Once the limit is reached, the connection status icon resets back to **ready to connect**. The time must be a whole number between 1 and 72. After this duration, the system will update session status from **active** to **timed out** to display icon. It will not terminate any active remote control session.
Deploy Remote Control Agent	Deploy Remote Control Agent to all devices	Select this option to install the Remote Control Agent to all devices. **NOTE:** To deploy the Remote Control agent to all devices, the number of Managed Computers license should be equal to the number of Remote Control computers. To check the license numbers, click the icon on upper right corner and then icon.
Remote Control Agent Settings		
	Hide tray icon from Taskbar	Select this option to hide the icon from the taskbar.
	Auto Launch	Select this option to launch the Remote Control agent automatically.

3. Click **OK**. The changes get applied when a remote control session is initiated.

   If the required applications are already installed on the devices, you are redirected to open the Splashtop for RMM application.

Start a Remote Control Session

NOTE: Before you start a remote control session,

- ensure that your device has an active Internet connection.
- ensure you have Splashtop for RMM installed on your device and Remote Control Agent installed on the remote device.

To start a remote control session,

1. Go to **Inventory** > **Devices** to display the **Devices** page.

   On the *Devices* page, click the remote control icon near the device name you want to connect with.

   Or

   Go to **Inventory** > **Devices** to display the *Devices* page.

Click the device name to open the device's details page.

Click the **Remote Control** button on the page.

2. In the *KACE remote control powered by Splashtop®* dialog box that appears, click **OK**.

   If the required applications are already installed on the devices, you are redirected to open the Splashtop for RMM application.

   NOTE: You can modify the default settings by selecting **Use Custom Settings** and edit the required details. For more details, refer Configure Settings Before Starting the Remote Control Session.

3. Click **Open Splashtop for RMM**. You are connected to the remote device.

   The remote control icon changes to showing the session is active.

   NOTE: The Scoped users can initiate and end remote sessions only for the devices that are associated with their role. The Scoped user can also terminate a remote session initiated by any other user if the device is associated with the Scoped user's role.

Multiple Remote Control Sessions

You can now initiate up to two simultaneous remote control sessions to the same device. Splashtop supports this feature for the Quest RMM account.

When a remote control session is active for a device, you can connect to that device. The Remote Control icon remains enabled even during an active session, allowing a second connection to be initiated. If a third connection is attempted, the Splashtop Viewer displays an error indicating the session limit has been reached.

You can terminate all active sessions by clicking Session Reset. You can track and record history for both the concurrent sessions in Session History.

Statuses of Remote Control Session

The color of the remote control icon changes as the remote control session status changes. The following are the various statuses of a remote control session that a remote control icon shows:

- : The session is active.
- : The device is available to initiate a session.
- : The device is not available for remote control session.

End a Remote Control Session

You can end a remote control session in the following ways:

- End the ongoing session from the Splashtop for RMM application

  Or

- Go to **Inventory** > **Devices** to display the **Devices** page.

  From the **Choose Actions** drop-down list, select **Reset Remote Control Session**. The active session gets terminated.

Track Remote Session History

You get the Remote Control session details in the following ways:

1. **From the Device Details page**
   a. Go to **Inventory** > **Devices**.

b. Click the device name to open the **Device Details** page.

c. Click the **Remote Control Session** tab.

The details related to the last five remote control sessions such as **Username**, **IP address**, **Start time**, **End time**, **Status**, and the **Duration** of the session display.

NOTE: Session tracking will not work in the following conditions:

- SMA is on self-signed certificate and the Splashtop for RMM application is on Mac.
- SMA hostname is not resolvable from the device that is starting Splashtop for RMM application.

2. **From the Reports page**

a. Go to **Reporting** > **Reports**.

b. From the **View By** drop-down list, select the **Remote Control** option. You can see the following three reports:

Overall remote control deployment - Lists the remote control agent deployed.

Remote control sessions for last 7 days - Lists the remote control sessions for last seven days.

Remote control sessions for last 30 days - Lists the remote control sessions for last 30 days.

Upload and View Streamer Logs

You can upload and view Splashtop streamer logs directly from the **Device Details** page. This helps troubleshooting of remote control issues, such as session initiation failures.

The **Upload Agent Files** option on the **Device Details** page allows you to upload diagnostic logs, including Splashtop streamer logs, from the supported Windows and macOS devices. Once uploaded, these logs are available under the **Logs and Diagnostics** section, and helps you to analyze and resolve remote session issues.

Uploading the Streamer Logs

To upload the streamer logs:

1. Go to **Inventory** > **Devices** to display the **Devices** page.
2. On the *Devices* page, select the device to display the device details.
3. Click **Choose Actions** > **Upload Agent Files (Diagnostic)**. This uploads Splashtop-related log files to the server.

NOTE: Based on the operating system of a device, the log files and their locations are as follows:

- Windows Devices: The agent_log and SPLog files are located at `C:\Program Files (x86)\Splashtop\Splashtop Remote\Server\log`.
- macOS Devices: The SPLOG.txt file is located at `/Users/Shared/SplashtopStreamer/`.

Viewing the Streamer Logs

You can access the logs from **Logs and Diagnostics** > **Agent Files (Diagnostic)** on the same **Device Details** page.

You can review these logs to identify and resolve remote control failures efficiently.

Customize the Blank Screen Logo

Administrators can now customize the background image that appears on a device console during a remote control session. This feature is available under Remote Control Agent Settings in the Remote Control Settings page of the KACE System Management Appliance admin console.

Uploading a Custom Blank Screen Logo

To configure a custom background image (in PNG format) that appears during a remote session:

1. Log in to the KACE System Management Appliance Admin UI.
2. Navigate to Settings > Control Panel > Remote Control Settings.
3. Under Remote Control Agent Settings, in the **Customize Blank Screen Logo** section, click **Choose file to upload a .PNG file** and click Save.

NOTE: You can use the blank screen setting in the viewer application to control what appears on the device screen during a remote session.

- If the Blank Screen option in the Viewer application is not selected, and you start a remote session, user can see the device's background contents.
- If the Blank Screen in the Viewer application is selected, and you start a remote session, user will see the uploaded PNG logo instead of the device's background.

File Size Restrictions

You can upload a .PNG file with the size upto 15MB.

If the file size exceeds 15MB, the system displays the following error message: "**The uploaded file exceeds the maximum allowed size of 15MB. Please upload a smaller file**."

Troubleshoot Remote Control

1. **The remote control session is not working**.

   Or

   I am getting a blank or black screen. What should I do?

   To run a remote control session smoothly, ensure the following are fulfilled:

   # **Remote Control Agent Installation** - The Remote Control Agent must be installed on the chosen device and managed by KACE SMA.
   # **Unique ID included in inventory** - The installed Remote Control Agent creates a Unique Id (device identifier). This Unique Id should be reported to KACE SMA by the KACE SMA agent inventory process.
   # **Splashtop RMM Code** - The device should be configured with an RMM code linking it to the correct Splashtop management group.
   # **Force Inventory** - Refresh the updates by forcing an Inventory.

2. **Where can I download the Splashtop for RMM and the Remote Control Agent applications?**

   You must install the **Splashtop for RMM** application on the controlling device. You need to download the **Splashtop for RMM** application through the links provided by SMA. Refer the following topics:

   # Download from the Control Panel page
   # Download from the pop-up window after you initiate a remote control session

   You must install the **Remote Control Agent** application on the agent-managed devices. You can install the application using the different methods described in the **Install Remote Control Agent** section. Refer the link: Install Remote Control Applications
   If you are facing any issue, download the **Remote Control Agent** application from the following links;

   # **For macOS** - https://my.splashtop.com/csrs/mac
   # **For Windows** - https://my.splashtop.com/csrs/win

3. **I am unable to view the screen on my Mac. What should I do?**

   To view the screen on your Mac, you must grant permission for screen control and microphone access to the Remote Control Agent. To grant the permission, follow these steps:

   a. Open **System Settings** on your Mac.
   b. Go to **Privacy and Security**.

c. Grant access to **Accessibility for the Remote Control Agent** (this is mandatory).
d. Grant access to **Screen Recording for the Remote Control Agent** (this is mandatory).
e. Grant access to the **Microphone for the Remote Control Agent** (required for sound).
f. Grant access to **Full Disk Access for the Remote Control Agent** (required to transfer files).

After saving the settings, the remote session should start and you should be able to view the screen.

4. **I am still unable to connect. What should I do?**

If you are still unable to connect,

ensure that your device is connected to the Internet and that the proxy settings on your device's network settings are configured properly.

visit the Splashtop's website that checks if your device can connect: Check Connectivity to Splashtop Servers

check with your network admin if the address is reachable on your network: https://st-rmm-kace.api.splashtop.com

Managing MIA devices

Devices that are under management but that have not communicated with the appliance in the last 1 to 90 days are considered to be MIA (missing in action) or out-of-reach. You can configure MIA device settings and manage MIA devices as needed.

NOTE: Your product license agreement entitles you to manage a specified number of devices that are classified as Managed Computers, Monitored Devices, and Assets. Be aware that devices count toward these limits even if devices are MIA (missing in action) or no longer in use. However, devices that are added to inventory manually, or through the API, do not count toward license limits. See View product licensing information.

NOTE: To increase your license capacity, go to the Quest website: https://quest.com/buy.

Configure MIA settings

You can configure the appliance to automatically delete MIA devices from inventory after devices have not checked in for a specified number of days. Automatically deleting MIA devices can reduce the need to delete MIA devices manually.

Be aware that the process that deletes MIA devices runs daily at 03:45, and it can delete up to 100 devices during a single run. If there are more than 100 MIA devices to be deleted, or if you must delete devices immediately, consider deleting devices manually.

1. Go to the *Devices* list:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Inventory**, then click **Device**s.
2. Select **Choose Action** > **Configure MIA Settings** to display the *MIA Settings* page.
3. Provide the following information:

Option	Description
Automatically Remove MIA Devices	Archive or delete managed devices that are MIA (missing in action) after the specified period of time. Clear the check box to prevent MIA devices from being Archived or deleted automatically.
After n days	The number of days MIA devices remain in inventory if *Automatically Relete MIA Devices* is selected. Managed devices that do not communicate with the appliance for the specified number of days are automatically deleted or archived, as specified.

Option	Description
Archive MIA Asset-Devices	Select this option to archive the MIA devices after the specified number of days.
Delete MIA Devices	Select this option to permanently delete the MIA devices after the specified number of days.

4. Click **Save**.

   Devices are deleted when the deletion process runs daily at 03:45. The process can delete up to 100 devices during a run.

If there are more than 100 MIA devices to be deleted, or if you must delete devices immediately, consider deleting devices manually. See Delete MIA devices manually.

Apply labels to MIA devices

You can use labels to manage groups of MIA devices.

1. Go to the *Devices* list:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Inventory**, then click **Device**s.
2. **Optional**: To view MIA devices: In the *View By* drop-down list, which appears above the table on the right, select **MIA**, then select the number of syncs the device missed, or the number of days the device has been missing.
3. Select the check box next to one or more devices.
4. Select **Choose Action** > **Apply Labels** to display the *Apply Labels* dialog.
5. Search for labels, or drag a listed label into *Apply these labels*, and click **Apply Labels**.

Delete MIA devices manually

You can delete MIA devices manually as needed.

To configure the appliance to automatically delete MIA devices, see Configure MIA settings.

1. Go to the *Devices* list:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Inventory**, then click **Device**s.
2. **Optional**: To view MIA devices: In the *View By* drop-down list, which appears above the table on the right, select **MIA**, then select the number of syncs the device missed, or the number of days the device has been missing.
3. Select the check box next to one or more devices.
4. Select **Choose Action** > **Delete**, then click **Yes** to confirm.

Troubleshoot devices that fail to appear in inventory

If Agent-managed devices do not appear in inventory, verify Agent and appliance configuration.

By default, KACE Agents installed on managed devices communicate with the appliance using HTTP over ports 80 and 443. If network connectivity is in place, but newly installed Agents do not connect to the appliance, there might be problems with the default `kbox` hostname in DNS.

1. Install the Agent with hostname or IP address correctly specified:

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 and SLES)

```
export KACE_SERVER=my_kace_sma
export KACE_SERVER=my_kace_smasudo rpm -ivh ampagent-6.x.xxxxx.xxxx.xx.rpm
```

2. To correct the server name for a device that is already installed, use the AMPTools utility:

   Windows

   32-bit systems: `"C:\Program Files\Quest\KACE\AMPTools" host=my_kace_sma`

   64-bit systems: `"C:\Program Files (x86)\Quest\KACE\AMPTools" host=my_kace_sma`

   Mac OS X

   ```
   /Library/Application\ Support/Quest/KACE/bin/AMPTools host=my_kace_sma
   ```

   Linux

   ```
   /opt/quest/kace/bin/AMPTools host=my_kace_sma
   ```

3. Verify that you are able to ping the appliance, and reach it through a web browser at `http://`**appliance_hostname**.
4. Verify that Internet Options are not set to use proxy. Verify that proxy is excluded for the local network or **appliance_hostname**.
5. Verify that no firewall or anti-spyware applications are blocking communication between the appliance and any of the Agent components, including:

Table 23. KACE Agent components for each operating system

Operating system	Agent components
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 and Linux	AMPAgent AMPAgentBootup

Operating system	Agent components
	AMPctl AMPTools AMPWatchDog Inventory KBoxClient KCopy KDeploy KInventory konea kpatch KSWMeterSvc KUpdater KUserAlert runkbot

6. Verify that the following processes are running:
   - **Windows: AMPAgent.exe, AMPWatchDog.exe, konea.exe.**
   - **Mac and Linux: AMPAgent, konea.**

If, after verifying these items, the Agent still fails to connect to the appliance, contact **Quest Support** at https://support.quest.com/contact-support.

Obtaining Dell warranty information

The appliance periodically runs a background service that gathers and updates Dell warranty information on the Dell devices that are in your appliance inventory.

This service runs every four hours. If you have multiple organizations, the service selects a different organization in a round-robin fashion and collects warranty information on approximately 100 devices per organization. Over time, warranty information is gathered and updated for all Dell devices.

You can update Dell warranty information any time, and you can run reports to track warranty information.

NOTE: The Dell warranty information is available only for Dell computers that are in inventory. In addition, the appliance must be able to reach the following domain to gather warranty information: **api.dell.com**. See Make necessary websites accessible to the appliance.

Obtain Dell warranty information on a single Dell device instantly

You can obtain warranty information for any managed Dell device in your inventory from the **Administrator Console**.

If you have many Dell devices, it might take a while to update the warranty information through the appliance's background service.

1. Go to the *Devices* list:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.

b. On the left navigation bar, click **Inventory**, then click **Device**s.

2. In the list of devices, click the name of a Dell device to display the *Device Detail* page.
3. In the *Inventory Information* section, expand **Hardware**.

   Dell warranty information appears under the *Dell Service Information* section.
4. Click **Refresh**.

The warranty information is updated immediately.

Renew a Dell warranty

You can access the Dell Support website to renew warranties on Dell devices in inventory.

1. Go to the *Devices* list:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Inventory**, then click **Device**s.
2. In the list of devices, click the name of a Dell device to display the *Device Detail* page.
3. In the *Inventory Information* section, expand **Hardware**.
4. Select the **support.dell.com** link in the *Dell Service Information* section.

   You are directed to the Dell Support website where you can renew your warranty if it is out of date or view additional information.

Run Dell warranty reports

You can run reports that show the warranty status of the Dell devices in the inventory. If the Organization component is enabled on your appliance, you can run these reports at the organization level and at the System level.

1. Go to the *Reports* list:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Reporting**, then click **Reports**.
2. In the *View By* drop-down list, which appears above the table on the right, select **Dell Warranty** to display the Dell Warranty reports.
3. In the *Generate Report* column, click a report type to run the report.

See About reports.

Managing applications on the Software page

Applications that are found on managed devices are listed on the *Software* page.

About the Software page

The *Software* page shows all the applications installed on managed devices and any applications that have been added to inventory manually or uploaded using the inventory API.

If the Organization component is enabled on your appliance, you manage applications for each organization separately.

The information and features accessible from the *Software* page differ from information and features available from the *Software Catalog* page. See Differences between the Software page and the Software Catalog page.

View items in Software page inventory

You can view items that have been added to inventory on the *Software* page. If the Organization component is enabled on your appliance, you view *Software* page inventory for each organization separately.

1. Go to the *Software* list:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Inventory**, then click **Software**.

Tracking changes to inventory settings

If History subscriptions are configured to retain information, you can view the details of the changes made to settings, assets, and objects.

This information includes the date the change was made and the user who made the change, which can be useful during troubleshooting. See About history settings.

Adding and deleting applications in Software page inventory

Applications are added to the *Software* page inventory automatically when managed devices upload inventory information to the appliance. In addition, you can add applications to the *Software* page manually as needed.

Add applications to Software page inventory manually

You can manually add applications to the *Software* page inventory list as needed.

Usually, it is best to have applications added to the appliance inventory automatically, than to add applications to the appliance manually. However, adding applications manually is useful if you want to add an application that is not currently installed on managed devices. You can manually add the application, then create a Managed Installation for it, and deploy it to managed devices.

If you add applications manually, you might want to include a Custom Inventory rule so that information about the applications is current and packages are not reinstalled each time Agents check in. See Writing custom inventory rules.

TIP: Applications that are added manually are displayed on the *Software* page, but they are not displayed on the *Software Catalog* page. You cannot add applications manually to the *Software Catalog* page.

1. Go to the *Software Detail* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Inventory**, then click **Software**.
    c. Select **Choose Action** > **New**.
2. Provide general information: *Name*, *Version*, *Publisher*.

For proper downstream reporting, enter this information consistently across software inventory.

3. Provide the following information:

Option	Description
Assign To Label	(Optional) The label associated with the item.
Notes	Any additional information you want to provide.
Supported Operating Systems	The operating systems on which the application runs. Applications are deployed only to devices with the selected operating systems. 1. Click **Manage Operating Systems**. 2. In the **Operating Systems** dialog box that appears, select the OS versions in the navigation tree, as applicable. You have an option to select OS versions by their family, product, architecture, release ID, or build version. You can choose a specific build version, or a parent node, as needed. Selecting a parent node in the tree automatically selects the associated child nodes. This behavior allows you to select any future OS versions, as devices are added or upgraded in your managed environment. For example, to select all build current and future versions associated with the Windows 10 x64 architecture, under **All** > **Windows** > **Windows 10**, select **x64**.
Custom Inventory Rule	(Optional) The custom inventory rules to apply to the application. Custom inventory rules enable you to detect applications and other items on a device and capture details for reporting. For example, the appliance first verifies whether an application is present on a device before deploying that application. In some instances, however, installed programs do not register in *Add/Remove Programs* or in standard areas of the registry. In such cases, the appliance might not be able to detect the presence of the application without additional information from the administrator. Therefore, the appliance might repeat the installation each time the device connects. Custom Inventory rules can prevent this. The following rule verifies that the version of the Network Associates VirusScan installed on a device is newer than a given version before deploying it: `RegistryValueGreaterThan(HKEY_LOCAL_MACHINE\Software \Network Associates\TVD\Shared Components\VirusScan Engine \4.0.xx,szDatVersion,4.0.44)` See Getting values from a device (Custom Inventory Field).

4. Next to *Upload and Associate File*, click **Browse** or **Choose File** to locate a file, then click **Open** or **Choose**.

   To distribute applications using Managed Installations or File Synchronizations, you need to associate the actual application files with the application.

5. To prevent the file from being copied to Replication Shares, select **Don't Replicate Associated File**.

   This is useful for large files that you do not want users to install from Replication Shares, such as software suites.

6. **Optional**: Select a *Category* and *Threat Level* for the software.
7. Click **Save**.

Related topics

Using software threat levels and categories

Delete applications

Deleting applications from the *Software* page removes them from the *Software* page inventory, and also removes Managed Installations or File Synchronizations that are associated with applications.

However, if the deleted applications are installed on managed devices, the records for those applications are recreated, with new IDs, when the devices update inventory information. Managed Installations and File Synchronizations that were associated with the deleted applications, however, are not recreated.

1. Go to the *Software* list:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Inventory**, then click **Software**.
2. Select the check box next to one or more applications.
3. Select **Choose Action** > **Delete**, then click **Yes** to confirm.

Creating Software assets

To set up License Compliance for applications that appear on the *Software* page, you first need to add Software assets for those applications. After you create Software assets, you can associate them with License assets.

You can create assets for applications that have been added to the appliance automatically or manually.

NOTE: Software assets are not required to set up License Compliance for applications on the *Software Catalog* page.

If the Organization component is enabled on your appliance, you create Software assets for each organization separately.

Add Software assets in the Inventory section

You can add Software assets for one or more applications by selecting the applications in the *Inventory* section on the *Software* list.

Software assets can also be added from the *Assets* section. See Add Software assets in the Assets section.

1. Go to the *Software* list:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Inventory**, then click **Software**.
2. Select the check box next to one or more applications.
3. Select **Choose Action** > **Create Asset**.

    The assets are created, and they appear on the *Assets* page.

Add Software assets in the Assets section

You can add Software assets one-at-a-time in the *Assets* section.

Software assets can also be added from the *Inventory* section. See Add Software assets in the Inventory section.

1. Go to the *Assets* list:

a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
b. On the left navigation bar, click **Asset Management**, then click **Assets**.

2. Select **Choose Action** > **New** > **Software** to display the *Software Asset Detail* page.
3. Complete the asset fields as follows:
   a. In the *Name* field, enter a name for the asset.

      For example, Office Pro SW Asset.

   b. **Optional**: In the *Software* field, select the name of the application to associate with the asset. To search for items, begin typing in the field.
   c. **Optional**: In the *Software Label* field, select a label in the *Select label* drop-down list. The list is empty unless you have created a Smart Label. To filter the labels list, enter a few characters of the label name in the *Filter* field.
4. Click **Save**.

The new asset appears on the *Assets* page.

Attach digital assets to applications and select supported operating systems

To distribute applications to managed devices using Managed Installations or **User Console** downloads, you need to attach the appropriate digital assets to applications. Digital assets are the files required for deployment, such as installers. In addition, you need to select the supported operating systems for the application. You perform these tasks on the *Software* detail page.

To associate multiple files with an application, create a ZIP file that contains the files, then associate the resulting archive file with the application.

TIP: Digital assets can be attached to applications displayed on the *Software* page, but they cannot be attached to items in the *Software Catalog* page.

1. Go to the *Software Detail* page:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Inventory**, then click **Software**.
   c. Click the name of a software application.
2. Do one of the following:
   - **Next to *Upload and Associate File*, click Browse or Choose File.**
   - **Next to *Upload and Associate Client Drop File*, click Browse or Choose File. This option is available only if you have copied files to the appliance or organization Client Drop location, and those files are larger than the size specified in the appliance's *Client Drop File Size Filter* or the organization's in the Client Drop Size. If the Organization component is enabled on your appliance, files are available to the selected organization only. To make files available to multiple organizations, copy the files to the Client Drop location for each organization. Copy files to the appliance Client Drop location.**
3. Locate the file to upload, then click **Open** or **Choose**.
4. In the *Supported Operating Systems* section, select the operating systems on which the application can be installed.
   a. Click **Manage Operating Systems**.
   b. In the **Operating Systems** dialog box that appears, select the OS versions in the navigation tree, as applicable.

      In the Operating Systems dialog box that appears, select the OS versions in the navigation tree, as applicable.

You have an option to select OS versions by their family, product, architecture, release ID, or build version. You can choose a specific build version, or a parent node, as needed. Selecting a parent node in the tree automatically selects the associated child nodes. This behavior allows you to select any future OS versions, as devices are added or upgraded in your managed environment. For example, to select all build current and future versions associated with the Windows 10 x64 architecture, under **All** > **Windows** > **Windows 10**, select **x64**.

NOTE: If no operating systems are selected, the application cannot be distributed to managed devices. Deployments such as Managed Installations can be created, but they can be deployed only if the correct supported operating system information is provided.

5. Modify other details as necessary, then click **Save**.

NOTE: The table at the bottom of the *Software Detail* page shows which devices have the software installed.

Copy files to the appliance Client Drop location

You can upload large files, such as application files and backup files, to the appliance by copying them to the Client Drop location on the appliance. Copying files to the Client Drop location is an alternative to uploading files through the **Administrator Console** using the default HTTP mechanism, which can result in browser timeouts for large files.

- Enable file sharing (Samba). See Configure security settings for the appliance.
- If the Organization component is enabled on your appliance, enable file sharing for each organization. See Configure Admin-level or organization-specific General Settings.
- If the Organization component is not enabled on your appliance, configure the Client Drop File Size Filter setting for the appliance. See Configure appliance General Settings without the Organization component.
- If the Organization component is enabled on your appliance, configure the Client Drop Size setting for each organization. See Configure Admin-level or organization-specific General Settings.

1. In a file system navigator, go to the Client Drop location on the appliance:
   - **In Windows Explorer, enter a UNC path with the appliance host name or IP address. For example: `\\kbox\clientdrop`. Use two backslashes to indicate that the location is a Samba path.**
   - **On Mac OS X, Go > Connect to Server, then enter the SMB address in the *Server Address* field.**
   - **On Linux, select Search, then enter the SMB address.**

   The `client Share` and `clientdrop Share` folders are displayed.

   NOTE: If the Organization component is enabled, each organization has a separate Client Drop location. For example:
   - ORG1: clientdrop
   - ORG2: clientdrop_2
   - ORG3: clientdrop_3
2. If prompted, provide your login credentials for the Client Drop location. These credentials are specified in the appliance security settings. See Configure security settings for the appliance.

   TIP: If you are connecting from a Windows device, type \admin in the *Username* field. This prevents the system from using workgroup\admin or domain\admin during authentication.
3. Copy your files to the Client Drop location. If the Organization component is enabled on your appliance, copy the files to the Client Drop location for the organization where you want to select the files.

The files are available as follows:

Application files: Files are available for selection on the *Software Detail* page provided that they are larger than the size configured for the appliance in the *Client Drop File Size Filter* or for the organization in the Client Drop Size. If the Organization component is enabled on your appliance, files are available to the selected

organization only. To make files available to multiple organizations, copy the files to the Client Drop location for each organization.

Appliance backup files: Appliance backup files that are placed in any Client Drop location are automatically identified as appliance backup files, and they become available for selection on the *Backup Settings* page within five minutes.

If you are uploading application files to be selected on the *Software Detail* page, verify the *Client Drop* location filter setting. The filter setting determines whether files are displayed on the *Software Detail* page, based on their size. See Configure appliance General Settings without the Organization component or Add or edit organizations.

Using software threat levels and categories

Threat levels and categories can be used to indicate the relative safety of applications and to classify applications.

This information is made available for tracking purposes only. The appliance does not enforce policies based on threat levels or categories.

Software categories classify software as belonging to a specified group, such as software drivers or security applications. For applications listed on the *Software* page, categories are assigned manually. For applications listed on the *Software Catalog* page, software categories are assigned to applications automatically.

Assign threat levels to applications

You can assign threat levels to applications that are listed on the *Software* page. Threat levels cannot be assigned to items listed on the *Software Catalog* page.

1. Go to the *Software* list:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Inventory**, then click **Software**.
2. Select the check box next to one or more applications.
3. Select **Choose Action** > **Set Threat Level**, then select a threat level.

Assign categories to applications

You can assign categories to applications that are listed on the *Software* page. Categories are assigned automatically to applications listed on the *Software Catalog* page.

1. Go to the *Software* list:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Inventory**, then click **Software**.
2. Select the check box next to one or more applications.
3. Select **Choose Action** > **Set Category**, then select a category.

Finding and labeling applications

You can use Advanced Search and labels to manage your software inventory.

About finding applications using Filter

The Filter option enables you to specify values for each field present in software inventory and search the entire inventory for that particular value or combination of values.

For example, you could use Filter to find devices with a specific operating system that have a specific application installed. See Searching at the page level with advanced options.

Add manual software labels

You can add manual labels in the *Inventory* section as needed. This is useful when you want to group software applications by manually applying labels to them.

1. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
2. Do one of the following:
   - **Select Inventory > Software to display the *Software* page.**
   - **Select Inventory > Software Catalog to display the *Software Catalog* page.**
3. Select **Choose Action > Add Label**.
4. In the *Add Label* window, enter a name for the label.

   TIP: Avoid using backslashes (\) in label names. If you need to use a backslash in a label name, add a second backslash (\\) to escape it.

5. Click **Save**.

Apply manual labels to or remove labels from software

You can apply manual labels to, or remove manual labels from, software in the appliance inventory as needed.

Add a manual label. See Add manual software labels.

1. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
2. Do one of the following:
   - **Select Inventory > Software to display the *Software* page.**
   - **Select Inventory > Software Catalog to display the *Software Catalog* page.**
3. Select the check box next to one or more applications.
4. Do one of the following:
   - **Select Choose Action > Apply Label, then select the label to apply.**
   - **Select Choose Action > Remove Label, then select the label to remove.**

For more information about labels, see Managing manual labels.

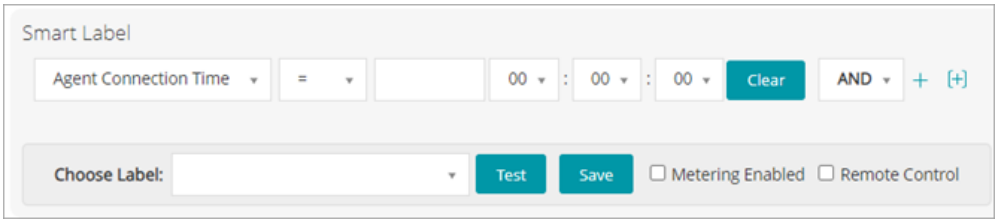
Add software Smart Labels

You can add software Smart Labels on the *Software* page as needed. This is useful when you want to automatically group applications based on whether they meet the criteria of the Smart Label.

For example, you could use a Smart Label to group all copies of an application purchased from a particular vendor. The label would be applied automatically to applications you have already purchased from the vendor, as well as any you might purchase in the future. See Managing Smart Labels.

NOTE: Smart Labels cannot be applied to applications on the *Software Catalog* page.

1. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
2. Select **Inventory** > **Software** to display the *Software* page.
3. Click the **Smart Label** tab above the application list on the right to display the *Smart Label* panel.



4. Specify the criteria required to find applications from a particular vendor:

```
Vendor Contact | contains | Smith
```

5. Click **Test**.

   Items that match the specified criteria are displayed.
6. Adjust the criteria as needed until the results are what you expect.
7. In the *Choose label* drop-down list, do one of the following:
   - **Select an existing label to associate with the Smart Label. Type in the *Choose label* field to search for existing labels.**

     NOTE: If you select a label group instead of a label, you will not be able to apply the Smart Label to a patching schedule. Patching schedules can only use Smart Labels based on a single item.
   - **Enter a new name for the Smart Label in the *Choose label* field, then press Enter or Return.**

   NOTE: Press **Enter** or **Return** after you enter a new Smart Label name to move the text from the search field to the label field.
8. Click **Create**.

Smart Labels are automatically applied to or removed from applications when the applications are updated on the *Inventory* > *Software* page, based on whether the applications meet the specified criteria.

Managing Software Catalog inventory

Applications that have been identified as present on managed devices, and that match application definitions in the Software Catalog, are referred to as Software Catalog inventory.

About the Software Catalog

The Software Catalog is a database that contains standardized information about more than 60,000 Windows and Mac applications and software suites. Information in the catalog includes the name, version, publisher, and category of each application or suite, as well as the operating system on which the application or suite runs.

The Software Catalog is available to all KACE SMAs running version 5.5 or higher. The catalog is continually updated and maintained by Quest to ensure that it is comprehensive, accurate, and up-to-date.

When managed devices that are running Agent version 5.5 or higher report application inventory, that inventory information is compared to items in the Software Catalog. Standardized application inventory information is then displayed under the *Software Catalog* tab.

The Software Catalog enables you to:

- Identify the software installed on devices and view standardized information about that software. See Viewing Software Catalog information.
- Enable metering to gather detailed information about software usage. See Using software metering.
- Associate license information with software in the Software Catalog. This enables you to monitor software license compliance and usage for devices. See Add License assets for Software Catalog inventory.
- Identify and mark software as Not Allowed. This enables you to prevent the use of software marked as Not Allowed. See Using Application Control.

The catalog contains information about software designed to run on Windows and Mac operating systems only. Software designed to run on Linux and other unsupported operating systems are not available in the catalog.

Application classifications

Applications that appear on the Software Catalog page are classified as Discovered, Not Discovered (Cataloged), and Uncataloged. The classification determines the kinds of actions you can perform and the type of information that is available for the applications.

Discovered applications

Discovered applications are executables in the appliance inventory that match the definitions of applications in the Software Catalog. You can enable metering for Discovered applications and suites, mark them as Not Allowed, and add license information for them. In addition, the Discovered application list can be exported in CSV format. You can export the Discovered application list, the Uncataloged list, and the Locally Cataloged list; you cannot export the entire Software Catalog.

Not Discovered applications

Applications that do not exist in the appliance inventory, but that do exist in the Quest KACE Software Catalog, are referred to as Not Discovered applications. You can enable metering for Not Discovered applications, mark them as Not Allowed, and add license information for them. However, because the applications have not been found in the local appliance inventory, the Not Discovered application list cannot be exported in CSV format.

Uncataloged applications

Uncataloged applications are executables that are in the appliance inventory but that do not appear in the Software Catalog. You can view applications that are listed as Uncataloged on the *Software Catalog* page. However, you cannot enable metering for Uncataloged applications, mark them as Not Allowed, or add license information for them.

Uncataloged applications must be added to the local or public Software Catalog before they can be metered, marked as Not Allowed, or associated with license information. See Adding applications to the Software Catalog.

NOTE: If data retention is disabled for Uncataloged applications, the Uncataloged applications list is empty. See Configure Admin-level or organization-specific General Settings.

About cataloged applications

Cataloged applications are executables that are in the official Software Catalog database. This includes both applications that appear in the appliance inventory (Discovered applications) and applications that do not appear in the inventory (Not Discovered applications).

About Locally Cataloged applications

Applications that are not in the official version of the Software Catalog, but that have been added to the local version on the appliance, are referred to as Locally Cataloged applications.

About Not Allowed applications

Not Allowed applications are applications that have been marked as Not Allowed on the *Software Catalog* page.

Windows and Mac applications can be marked as Not Allowed only if they are classified as Discovered, Not Discovered, or Locally Cataloged applications. Applications that are Uncataloged cannot be marked as Not Allowed until they are added to the Software Catalog. Applications that are marked as Not Allowed can be blocked or denying access on managed devices if those devices have an Application Control-enabled label applied to them.

See Using Application Control.

Application categories

Applications in the Software Catalog are grouped into categories, such as Productivity Applications and Antivirus Utilities.

These categories are useful for Reporting and License Compliance. In addition, applications in the *Operating System* category cannot be metered.

How Software Catalog information is collected

At a specified interval, the appliance collects information about every executable installed on managed devices. This information includes the executable's publisher, published date, file size, and registry information.

The information is compared to information in the Software Catalog to determine whether Discovered applications are Cataloged or Uncataloged. See Schedule metering and inventory collection intervals.

How the Software Catalog is used with the Organization component

Each appliance has a single Software Catalog. If the Organization component is enabled on your appliance, all organizations use the same Software Catalog that is installed on the appliance. In addition, Locally Cataloged applications are available to all organizations.

Uncataloged applications, and settings such as metering and license configuration, however, are organization-specific. For example, if you enable metering for an application in one organization, it is enabled only for that organization. You enable metering and other settings separately for each organization.

Similarly, Discovered applications are also organization-specific. Applications are marked as Discovered only if they are found in the inventory of the organization.

How Software Catalog information is localized

The application categories in the Software Catalog are localized to match the appliance locale setting. However, application names, such as Microsoft Excel, are not localized.

How you can help improve the Software Catalog

The Software Catalog is continually updated as new information or new applications become available and as cataloging requests are received. You can help improve the catalog by sharing your appliance inventory information with Quest KACE.

The Quest KACE catalog team uses this information to identify new applications and standardize application names and versions. See Configure data sharing preferences.

Differences between the Software page and the Software Catalog page

Both the Software page and the Software Catalog page use the application information reported by managed devices. However, the two pages represent separate inventory systems, and the way you perform software management tasks differs for each system.

For more information about managing information on the *Software* page, see Managing applications on the Software page. The following table compares the *Software* page and the *Software Catalog* page:

Task	Software page	Software Catalog page
Inventory collection process	Uses the classic inventory collection process available in version 5.4 of the appliance. Managed devices that are running Agent version 5.4 and lower report inventory only to the *Software* page; they do not report inventory to the *Software Catalog* page. Managed devices that are running Agent version 5.5 and higher report inventory to both the *Software* page and the *Software Catalog* page.	Uses an inventory collection process introduced in version 5.5 of the appliance. This process gathers information about every executable installed on managed devices. Managed devices must be running Agent version 5.5 or higher to report inventory to the *Software Catalog* page.
Viewing software inventory information	The *Software* page displays information about all of the applications found on managed devices or added to appliance inventory manually or through WSAPI.	Software inventory information is presented on the *Software Catalog* page as: • **Discovered**: Applications installed on managed devices that match application information in the Software Catalog. • **Not Discovered**: Applications in the Software Catalog that are not installed on managed devices. • **Uncataloged**: Applications that are installed on managed devices but that are not in the Software Catalog. Inventory information added to the appliance manually or through

Task	Software page	Software Catalog page
		WSAPI is not available under the *Software Catalog* page.
Metering applications	Not available.	Enabled for each application separately on the *Software Catalog* page or on the *Software Catalog Detail* page.
Tracking license information for applications	Enabled by creating a Software asset and a License asset for the application. License information appears on the License Compliance Dashboard widget. It does not appear on the *Licence Compliance* page.	Enabled by creating a License asset and associating it with an application in the Software Catalog. License information appears on both the *License Compliance* page and the License Compliance Dashboard widget. See About License Compliance for Software Catalog applications.
Marking applications as Not Allowed	Not available.	Available as a flag that is set on the *Software Catalog Detail* page. See Mark applications and suites as Not Allowed.
Adding digital assets to applications	Available on *Software Detail* pages; used for deploying software to managed devices. See Attach digital assets to applications and select supported operating systems.	Not available.
Distributing software in Managed Installations or File Synchronizations	Available for applications that have digital assets associated with them. See Distributing software and using Wake-on-LAN.	Not available.
Viewing summary license information	Available on the *License Compliance* and *Software License Configuration* chart on the *Dashboard* page. See About Dashboard widgets.	Available on the *License Compliance* and *Software License Configuration* chart on the *Dashboard* page. See About Dashboard widgets.
Setting threat levels for software	Available on the *Software* list. See Using software threat levels and categories.	Not available.
Setting software categories	Available on *Software Detail* pages. See Assign categories to applications.	Predefined by the Quest KACE Software Catalog team.

Viewing Software Catalog information

You can view application information on the Software Catalog page.

View lists of Discovered and Not Discovered applications

On the *Software Catalog* list, you can view Discovered and Not Discovered applications.

Discovered applications are executables in the inventory that match the definitions of applications in the Software Catalog. You can enable metering for Discovered applications and suites, mark them as Not Allowed, and add license information for them. In addition, the Discovered application list can be exported in CSV format. You can export the Discovered application list, the Uncataloged list, and the Locally Cataloged list; you cannot export the entire Software Catalog.

Applications that do not exist in the inventory, but that do exist in the Quest KACE Software Catalog, are referred to as Not Discovered applications. You can enable metering for Not Discovered applications, mark them as Not Allowed, and add license information for them. However, because the applications have not been found in the local inventory, the Not Discovered application list cannot be exported in CSV format.

1. Go to the *Software Catalog* list:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Inventory**, then click **Software Catalog**.
2. Click the **Discovered** tab.

    The list is filtered to show only those applications that are classified as Discovered. Information for Discovered applications includes:

Item	Description
Name	The name and version of the application. If the application is a suite, the name appears in bold. For example, **Microsoft Office 2010 Professional**.
Publisher	The application's publisher. This information is normalized to ensure accurate reporting. For example, Microsoft Corp. and Microsoft Inc. are reported as Microsoft Corporation.
Category	The category of the application as established by the Software Catalog team.
Installed	The number of managed devices that have the application installed. Click a number to view device information.
Licenses	The number of licenses available for the application. This information is available only if a License asset has been associated with the application. See Add License assets for Software Catalog inventory.
Variance	The number of unused licenses remaining. This information is available only if a License asset has been associated with the application.
Recently Added	The number of devices on which the application has been added in the past seven days.
Recently Removed	The number of devices from which the application has been removed in the past seven days.

3. Click the **Not Discovered** tab.

    The list is filtered to show only those applications that are classified as Not Discovered. Information for Not Discovered applications includes:

Item	Description
Name	The name and version of the application. If the application is a suite, the name appears in bold. For example, **Microsoft Office 2010 Professional**.
Publisher	The application's publisher. This information is normalized to ensure accurate reporting. For example, Microsoft Corp. and Microsoft Inc. are reported as Microsoft Corporation.
Category	The category of the application as established by the Software Catalog team.
Platform	The operating system on which the application is designed to run. For example, Windows.

4. To include or exclude a software catalog item from the *License Compliance* page, or from selected reports, select it in the list, click **Choose Action**, and select one of the following options, as required:
   - **Exclude from License Compliance**
   - **Include in License Compliance**
   - **Exclude from Reports**
   - **Include in Reports**
5. To view additional details, click the application name.

See View details of Software Catalog applications.

TIP: On the *Software Catalog* page, you can search for applications using Advanced Search and Custom Views based on Advanced Search criteria. See Searching at the page level with advanced options.

View the list of Uncataloged applications

On the *Software Catalog* list, you can view applications that are Uncataloged.

Uncataloged applications are executables that are in the appliance inventory but that do not appear in the Software Catalog. You can view applications that are listed as Uncataloged on the *Software Catalog* list. However, you cannot enable metering for Uncataloged applications, mark them as Not Allowed, or add license information for them. Uncataloged applications must be added to the local or public Software Catalog before they can be metered, marked as Not Allowed, or associated with license information.

Information that is available for Uncataloged applications differs from information that is available for applications whose titles are listed in the public version of the Software Catalog. For example, some information that is available for Cataloged applications might not be available for Uncataloged applications. The information available for Uncataloged applications is limited to the information collected from managed devices.

1. Go to the *Software Catalog* list:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Inventory**, then click **Software Catalog**.
2. Click the **Uncataloged** tab.

The list is filtered to show only those applications that are classified as Uncataloged. Information available for Uncataloged applications includes:

Item	Description
Name	The name and version of the application.

Item	Description
Installed	The number of managed devices that have the application installed.
File Name	The name of the application executable file.
File Version	The version number of the application.
Publisher	The application's publisher.

3. To include or exclude a software catalog item from the *License Compliance* page, or from selected reports, select it in the list, click **Choose Action**, and select one of the following options, as required:
   - **Exclude from License Compliance**
   - **Include in License Compliance**
   - **Exclude from Reports**
   - **Include in Reports**
4. To view additional details, click the application name.

See View details of Software Catalog applications.

View the list of Locally Cataloged applications

You can use Advanced Search to sort the *Software Catalog* page to show applications that have been added to the local version of the Software Catalog.

Applications that are not in the official version of the Software Catalog, but that have been added to the local version on the appliance, are referred to as Locally Cataloged applications. Locally cataloged applications can be metered, marked as Not Allowed, and associated with License assets.

1. Go to the *Software Catalog* list:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Inventory**, then click **Software Catalog**.
2. Click the **Advanced Search** tab above the list on the right, then specify the criteria required to view Locally Cataloged applications:

```
Software Catalog: Local Catalog Only | is | True
```

3. Click **Search**.

The list is filtered to show only those applications that are Locally Cataloged. Information available for Locally Cataloged applications includes:

Item	Description
Name	The name and version of the application. If the application is a suite, the name appears in bold. For example, **Microsoft Office 2010 Professional**.
Type	The classification of the application in the Software Catalog. Locally Cataloged applications are classified as Discovered.
Installed	The number of managed devices that have the application installed.

Item	Description
Publisher	The application's publisher. This information is normalized to ensure accurate reporting. For example, Microsoft Corp. and Microsoft Inc. are reported as Microsoft Corporation.
Category	The category of the application as established by the Software Catalog team.
Platform	The operating system on which the application is designed to run. For example, Windows.

4. To view additional details, click the application name.

See View details of Software Catalog applications.

View details of Software Catalog applications

You can view details of Discovered, Not Discovered, Uncataloged, and Locally Cataloged suites and applications.

To view details of Uncataloged applications, data retention for Uncataloged applications must be enabled. You cannot view details of Uncataloged applications if data retention is disabled. See Configure Admin-level or organization-specific General Settings.

TIP: For information about license compliance, go to the *License Compliance* page. See View License Compliance information for Software Catalog applications.

1. Go to the *Software Catalog* list:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Inventory**, then click **Software Catalog**.
2. Click the name of a suite or application to display the *Software Catalog Detail* page.

Information on this page includes:

Item	Description
Summary	
Not allowed	Indicates if the suite or application is marked as Not Allowed. Marking applications as Not Allowed prevents them from running on Agent-managed devices.
Metered	Indicates if metering is enabled for the suite or application. If metering is enabled for the application, usage data is collected for Agent-managed devices that also have metering enabled. See Enabling and configuring metering for devices and applications.
Installed	The number of Agent-managed devices on which the suite or application is installed.
Licenses	The number of License assets associated with the suite or application.
Expired Licenses	The number of expired License assets associated with the suite or application.
Exclude from License Compliance	Indicates if the suite or application appears on the *License Compliance* page.

Item	Description
Exclude from Reports	Indicates if the suite or application appears on selected reports.
Properties	
Publisher	The publisher of the suite or application. This information is normalized to ensure accurate reporting. For example, Microsoft Corp. and Microsoft Inc. are reported as Microsoft Corporation.
Platform	The operating system on which the suite or application is designed to run. For example, Windows.
Software Type	Indicates if the suite or application is an individual application, such as Microsoft Word, or a suite of applications, such as Microsoft Office.
Publisher License Type	The suggested license type for the suite or application.
Category	The category of the suite or application as established by the Software Catalog team. For applications that are Locally Cataloged, this is specified when the cataloging request is submitted.
Application ID or Suite ID	A code that identifies the suite or application.
General Availability	The date the suite or application was first released to customers.
End of Life	The date that support for the suite or application was discontinued.
MSRP ($)	The Manufacturer's Suggested Retail Price of the suite or application.
Metering Enabled	The date and time when metering was enabled for the suite or application.
Versions or Applications Installed	
File Name	For applications, the name of the executable file.
Product Name	For suites, the suite name.
Version	The version number associated with the suite or application.
Category	The category of the suite or application as established by the Software Catalog team. For applications that are Locally Cataloged, this is specified when the cataloging request is submitted.
Language	The language for which the suite or application is designed. For example, English. Applications that are not designed for a specific language are designated as Language Neutral.

Item	Description
Installed	The number of managed devices that have the suite or application installed. Click a number to view device information.
App-V	Refers to Microsoft Application Virtualization (App-V) which manages applications without installing them on devices.
Associated Files	One or more files that are associated with the selected version and attached to the software catalog. To attach a file, click +, and select the file location. You can edit or delete attached files, as needed. • To associate a file with a software version, navigate to the file using a file browser. • Alternatively, for larger files, use a Samba share. • Provide a note about the file. For example, Script Host 5.8 - x86 or Script Host 5.8 - x64 • To copy the file to the Replication Share, ensure the **Replicate Associated File** check box is selected.
Replicated	Indicates if the files are copied to the Replication Share.
Notes	A note about the attached file, if one is provided.
Licenses	Available only if a License asset has been added for the suite or application.
Name	The name of the license, such as **Office Professional PO #1234**. This is the name that you use to find the asset. If you plan to have multiple licenses associated with an application consider including a purchase order number or purchase date.
Count	The number of installations or seats the license allows. For example, 50.
Mode	The mode of the License asset. The mode is used in the License Compliance chart that is displayed on the *Dashboard* of the **Administrator Console**. Values that are marked as ignored on the *Asset Detail* page are shown with a usage level of 100 percent.
Key, Unit Cost, and Expiration	Additional information about the license. You can modify and edit the default information, which can be captured for a License Asset Type.
Vendor	The name of the Vendor asset you want to associate with the suite or application. the *Vendor* drop-down list is empty unless you have added a Vendor asset. To search for a vendor, begin typing in the list.
Order Number	The purchase order number associated with the license.
Purchased	The date the license was obtained. Click in the field, then select a date on the calendar.
Metering	
Last Used (days ago)	The number of managed devices that have launched the suite or application in the past 24 hours.

Item	Description
1-7	The number of managed devices that have launched the suite or application in the past 7 days.
8-30	The number of managed devices that have launched the suite or application in the past 8-30 days.
31-90	The number of managed devices that have launched the suite or application in the past 31-90 days.
Not Used	The number of managed devices that have not launched the suite or application in the last 90 days.

Adding applications to the Software Catalog

Quest reviews its extensive data warehouse and automatically adds new applications to the Software Catalog as needed. If an application does not yet appear in the catalog, however, you can send a cataloging request to the Quest catalog team for consideration.

A cataloging request is a form you can submit to request that an application that is not included in the Software Catalog (Uncataloged) be added to the public Software Catalog. When Quest receives a cataloging request, that request is evaluated to determine whether or not the application should become part of the public Software Catalog. In addition, applications are automatically added to the local version of the Software Catalog on the appliance when cataloging requests are submitted.

As an alternative, if you have applications that are internal to your organization, and you do not want those applications to be added to the public Software Catalog, you can add them to your local version of the Software Catalog. See Submit cataloging requests.

Submitting cataloging requests automatically adds applications to the local Software Catalog

When you submit a cataloging request for an application, the application is automatically and immediately added to the local version of the Software Catalog on your appliance.

The application then becomes Locally Cataloged, and it can be metered, marked as Not Allowed, and associated with License assets.

If the Organization component is enabled on your appliance, you can submit cataloging requests from any organization, and the title is added to your local appliance Software Catalog immediately. It is available to all of your organizations.

IMPORTANT: Cataloging requests can be submitted only if data retention for Uncataloged applications is enabled for the organization. See Configure Admin-level or organization-specific General Settings.

How Locally Cataloged applications change to Cataloged applications

Applications that are Locally Cataloged change to Cataloged applications when they are added to the public version of the Software Catalog.

Locally Cataloged applications are added to the public version of the Software Catalog when:

- You submit a cataloging request to the Quest KACE catalog team and the application is accepted into the Software Catalog.
- Another customer submits a cataloging request to the Quest KACE catalog team and the application is accepted into the Software Catalog.
- The Software Catalog team pro-actively adds the application to the Software Catalog.

When the Software Catalog that contains the application is updated on your appliance the name of the application might change. For example, if the characteristics, such as the name of the executable, file size, version, and other information of the Cataloged application match the characteristics of your Locally Cataloged application, the local information is replaced by catalog information. If the name of the application matches, but the file size or other information differs significantly, the new application is added but it does not replace the local catalog information.

In other words, the information in the public Software Catalog always takes precedence over local catalog information. Local Catalog applications that match applications in the public Software Catalog are replaced by public Software Catalog entries. However, this does not affect any information you have added for the application, such as licensing information, and it does not change settings such as metering or Not Allowed.

How custom names are resolved when Locally Cataloged applications are added to the Software Catalog

Application names might be standardized when custom applications are added to the public Software Catalog.

If you use custom names for local applications, the custom names are replaced with standard names when the application is added to the public Software Catalog. For example, if an application named **Updater** was not in the public catalog, you could create a local entry for that application. You could name that application, **MyUpdater**, and it would appear as **MyUpdater** in the local catalog. However, if the application was subsequently added to the public catalog, and the official name was determined to be **RealTime Updater**, the name **MyUpdater** would be replaced with **RealTime Updater** when the public catalog was updated. This name change does not affect metering, license, or history settings. However, if you have custom views or searches based on the old application name, you need to update those views and searches if you want to continue to use them.

Submit cataloging requests

You can submit cataloging requests for Uncataloged applications as needed. Requests are processed continuously and approved or denied at the discretion of the Quest KACE Software Catalog team.

Data retention for Uncataloged applications is enabled. You cannot submit cataloging requests if data retention is disabled. See Configure Admin-level or organization-specific General Settings.

Some applications, such as supporting executables for applications that are already cataloged, cannot be cataloged. In addition, if you have an Uncataloged application that has several versions, you need to submit cataloging requests for each version separately. You cannot associate multiple executables with a single cataloging request.

TIP: You can help improve the cataloging request process by sharing your inventory data with Quest. The Software Catalog team uses this data to identify new applications and standardize application names and versions. See Configure data sharing preferences.

1. Go to the *Software Catalog* list:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.

b. On the left navigation bar, click **Inventory**, then click **Software Catalog**.

2. Click the **Uncataloged** tab above the list on the left.
3. Click an application name to display the *Software Detail* page.
4. Click **Add to catalog** to display the *Add to Catalog* form.
5. Provide the following information:

Option	Description
Software Title	The name you want to use to identify the application. See How custom names are resolved when Locally Cataloged applications are added to the Software Catalog.
Category	The category of the application. Categories can be useful for organizing and managing applications.

6. Select sharing options and provide contact information:

Option	Description
Sharing	The cataloging option: • **Add software title to this appliance and share with the Quest KACE catalog**: Submit the request to Quest and add the title to the local version of the Software Catalog. • **Add software title to this appliance only**: Add the title to the local version of the Software Catalog, but do not submit the title to the Quest KACE Software Catalog.
Contact Details	Provide your contact information. The Software Catalog team uses this information to contact you if they have questions about the request.

7. Click **Save**.

The cataloging request is sent to Quest. The button, **Remove from local Software Catalog**, appears on the *Software Catalog Detail* page. When cataloging requests are added to the public Software Catalog, and that catalog is updated on your appliance, the **Remove from local software catalog** button no longer appears on the *Software Catalog Detail* page. Tracking for cataloging requests is not currently available.

NOTE: Information for titles that are added to the public catalog might differ from the information originally submitted. This is because titles are standardized when they are added to the public catalog.

Cancel cataloging requests and remove local cataloging

You can cancel cataloging requests and remove applications from the local Software Catalog if certain conditions are met.

- No License assets are associated with the applications. You must remove applications from License assets before you can remove applications from the catalog.
- Applications have not been accepted by the Software Catalog team or added to the public catalog. For example, if you submit a request, then cancel it the same day, the likelihood that the Software Catalog team would have accepted it is low, so the request might be canceled. However, if you submit a request, and then cancel that request after a few days or weeks, the Software Catalog team might already have approved the request and made the title part of the public Software Catalog. In that case, the add to catalog request cannot be canceled.

You can remove Locally Cataloged applications only. Cataloged applications cannot be removed from the catalog.

1. Go to the *Software Catalog* list:

a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
b. On the left navigation bar, click **Inventory**, then click **Software Catalog**.

2. Click an application name to display the *Software Catalog Detail* page.
3. If the application is associated with a License asset:
   a. On the *Software Catalog Detail* page, in the *Licenses* section, click the name of the License asset to display the *License Asset Detail* page.
   b. In the *Applies to Cataloged Software* field, select the name of the application, then click **Remove**.
   c. Click **Save**.
4. Return to the *Software Catalog Detail* page.
5. Click **Remove from local software catalog**.

The title is removed from the local version of the Software Catalog and **Add to catalog** button appears on the *Software Catalog Detail* page.

Managing License assets for Software Catalog applications

License assets can be associated either with items in the Software Catalog or with items listed on the *Software* page. However, they cannot be associated with both Software Catalog and *Software* page items at once.

If you have existing License assets, you can migrate them from items on the *Software* page to items on the *Software Catalog* page. This enables you to take advantage of features available through the Software Catalog, including License Compliance. See Migrate License assets to applications in the Software Catalog.

Add License assets for Software Catalog inventory

You can add License assets for applications in the Software Catalog inventory. Adding License assets enables you to view license compliance information on the *License Compliance* list and on the License Compliance *Dashboard* widget.

Software Catalog applications must be classified as *Discovered*, *Not Discovered*, or *Locally Cataloged*. You cannot add License assets for applications classified as *Uncataloged*.

When you associate License assets with applications, you can also view license information on the *Software Catalog Detail* page. If the Organization component is enabled on your appliance, you manage license information for each organization separately.

TIP: To add License assets for multiple applications at once, you can import the information from spreadsheets or CSV files. See Example: Import license data from prepared spreadsheets.

1. Go to the *Software Catalog* list:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Inventory**, then click **Software Catalog**.
2. Click the name of an application to display the *Software Catalog Detail* page.
3. Near the bottom of the page, in the *License* section, click **Add New License** to display the *License Asset Detail* page.
4. On the *License Detail* page, on the *General* tab, provide the following information:

Option	Description
Name	The name of the license, such as **Office Professional PO #1234**. This is the name that you use to find the asset. If you plan to have multiple licenses associated with an application, provide the purchase order number or purchase date in the fields below to differentiate the licenses.
License Subtype	The Asset Subtype to associate with the license. See About Asset Subtypes, custom fields, and device detail preferences.
Asset Status	The license status, if applicable. You can select a default asset status, or a custom one (if they exist). A default installation of the appliance includes the following asset statuses: • **Active**: Any asset that is deployed, active, or in use. • **Disposed**: An asset that is no longer available for use. • **Expired**: A software license or contract asset that has expired. • **In Stock**: A recently received asset. • **Missing**: Any asset that cannot be located. • **Repair**: An asset that is being repaired. • **Reserved**: An asset that is set aside for a specific person or use. • **Retired**: Any asset that reached its end-of-life state, or is no longer in use. • **Stolen**: An asset that has been reported as stolen. For more information, see View and configure asset lifecycle settings.
Location	The name of the location where the asset is located. See Managing locations.
License Count	The number of installations or seats the license allows. For example, 50.
Applies to Cataloged Software	Applications in the Software Catalog inventory to which the license applies. You can associate License assets with multiple applications in the Software Catalog if necessary. However, it is not necessary to associate a License asset with multiple versions of the same application because the appliance does this automatically to support upgrades and downgrades. You can simply associate the current version with the License asset when you add the license information. In addition, if you assign applications from different publishers, such as Microsoft Office and Adobe Acrobat, to the same License asset, the total number of seats specified in the License asset is assigned to each application. For example, if the License asset has 100 seats, both Microsoft Office and Adobe Acrobat are assigned 100 seats.
Applies to Software	Leave this field blank. A software license cannot be associated with applications from the *Software Catalog* inventory and the *Software* page inventory at the same time. For more information on how to create license assets for cataloged software, see Add License assets for Software page inventory.
License Mode	The mode of the License asset. For applications that require licenses, and to display license usage information on the *License Compliance* page, select either *Enterprise* or *Unit License*. **NOTE:** Most modes, including *Not Specified*, *Client License*, *Subscription*, *Shareware*, *Freeware*, *OpenSource*, *No Licensing*, and *Site License*, are not used for License Compliance.

Option	Description
	The license mode is used in these sections of the **Administrator Console**: • The *License Compliance* list. See View License Compliance information for Software Catalog applications. • The License Compliance chart that is displayed on the *Dashboard*. Values that are marked as ignored on the *Asset Detail* page are shown with a usage level of 100 percent. See About Dashboard widgets.

5. On the *License Detail* page, on the *Purchase* tab, provide the following information:

Option	Description
Contract	The contract asset associated with the license.
Product Key	The product key associated with the license. You can modify and edit the default information, which can be captured for a License Asset Type.
Unit Cost	The unit cost associated with the license. You can modify and edit the default information, which can be captured for a License Asset Type.
Vendor	The name of the Vendor asset you want to associate with the application. the *Vendor* drop-down list is empty unless you have added a Vendor asset. To search for a vendor, begin typing in the list. **NOTE:** Assigning multiple vendors to a single software License asset is not recommended because it can result in inaccurate License Compliance information.
Purchase Order Number	The purchase order number associated with the license.
Purchase Date	The date the purchase was made. Click in the field, then select a date on the calendar.
Purchase	Select one or more purchase records associated with this license. See Managing purchase records.

6. On the *License Detail* page, on the *Maintenance* tab, provide the following information:

Option	Description
Includes Upgrade Rights	Indicates if the license includes upgrade rights. Upgrade rights refer to the ability to upgrade to a newer version of the licensed software, when such versions become available. For more information, see About license upgrades. Select one of the following options: • **Yes**: Upgrade rights are calculated by comparing the number of existing licenses for the selected software with the counts of available licenses for newer versions of the same software. • **Yes - Select from list**: Choose one or more software versions for which you want to grant upgrade rights. Under *Upgrade Software list*, click **Select cataloged software to add**. The list that appears is populated with higher versions of the selected software to which the license can be upgraded. When you click an entry in the list, your selection appears in the *Upgrade Software list* box. You can add one or more versions, as

Option	Description
	needed. To delete an item from the list, select it in the *Upgrade Software list* box, and click **Remove**. • **No**: If you do not want to grant upgrade rights to the selected software, select this option.
Includes Maintenance	Whether the license entitles users to upgrade the installed version of the application. See About License Compliance for Software Catalog applications.
Expiration Date	If the license includes maintenance, the expiration date of the maintenance period. The appliance License Compliance feature leverages Software Catalog information, such as application release dates. If new application versions are released during the maintenance period, they are automatically covered by this License asset.
Includes Downgrade Rights	Indicates if the license includes downgrade rights. Downgrade rights refer to the ability to apply licenses for newer software versions to older versions of the same software. For more information, see About license downgrades. Select one of the following options: • **Yes**: Downgrade rights are calculated by comparing the number of existing licenses for the selected software with the counts of available licenses for older versions of the same software. • **Yes - Select from list**: Choose one or more software versions for which you want to grant downgrade rights. Under *Downgrade Software list*, click **Select cataloged software to add**. The list that appears is populated with lower versions of the selected software to which the license can be downgraded. When you click an entry in the list, your selection appears in the *Downgrade Software list* box. You can add one or more versions, as needed. To delete an item from the list, select it in the *Downgrade Software list* box, and click **Remove**. • **No**: If you do not want to grant downgrade rights to the selected software, select this option.

7. Click **Next**.
8. On the *License Detail* page, on the *Related* tab, provide the following information:

Option	Description
Department	The business group or department that owns the application.
Cost Center	The cost center associated with the department that owns the application.
Approved for Device	The devices that are approved to use the license. This information is used in License Compliance reporting. For example, if devices have the application installed, but are not on the list of approved devices, the devices are listed in the report titled, *Unapproved Software Installation*. However, the appliance does not enforce license compliance. For example, the appliance does not prevent applications from being installed on managed devices if a license is expired or otherwise out of compliance.

Option	Description
Barcodes	Add or edit barcodes associated with this license, as required. For more information, see Add barcodes to assets.

9. Click **Next**.
10. On the *License Detail* page, on the *Custom* tab, provide additional custom data. You can modify the License Asset Type to include as many additional fields as necessary to meet your business objectives. For more information, see Add or customize Asset Types.
11. Click **Next**.
12. On the *License Detail* page, on the *Notes* tab, provide the following information:

Option	Description
Notes	Any additional information you want to provide.
License Text	Any supplemental information about the license, such as a license number.

13. Click **Save**.

    The new License asset appears on the *Licenses* page. The *License Count* number does not change until you update the asset. However, the number in the *Installed* column changes when managed devices that have the software installed check in to the appliance. This enables you to track the number of licenses that have been purchased and installed.

Perform the following optional tasks:

- Enable metering for Software Catalog inventory. When metering is enabled, the *License Compliance* page shows whether applications have or have not been used in the past 90 days. See About software metering.
- Set license usage warning thresholds. These thresholds are used by the License Compliance Dashboard widget to identify license compliance issues.

Migrate License assets to applications in the Software Catalog

If you have existing License assets, you can migrate or transfer them from applications on the *Software* page to applications on the *Software Catalog* page. This enables you to take advantage of enhanced features available through the Software Catalog.

To migrate licenses, change the assignment from an application on the *Software* list to an application on the *Software Catalog* list.

License assets can be associated either with applications on the *Software Catalog* list or with applications on the *Software* list. However, they cannot be associated with both types of applications at once.

1. Go to the *Assets* list:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Asset Management**, then click **Assets**.
2. Click the name of a license associated with a *Software* list application to display the *License Asset Detail* page.

   A note appears in the top section stating that the license needs to be transferred to apply to a Software Catalog item.
3. In the top section, click **Transfer Now**.
4. In the *Applies to Cataloged Software* section, select the application you want to associate with the license.
5. Click **Save** at the bottom of the page.

Associate Managed Installations with Cataloged Software

You can add one or more Managed Installations to Software Catalog items to manage the deployment of these applications to end-user devices.

1. Go to the *Software Catalog* list:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Inventory**, then click **Software Catalog**.
2. Click the name of an application to display the *Software Catalog Detail* page.
3. Near the bottom of the page, click one of the following buttons:
    # **Add New Managed Install**, to install the selected Software Catalog using a Managed Installation.
    # **Add New Managed Uninstall**, to uninstall the selected Software Catalog using a Managed Installation.
4. On the *Managed Installation Detail* page that appears, specify the applicable details. For more information, see the following sections:
    # Create Managed Installations for Windows devices
    # Create Managed Installations for macOS X devices
    # Create Managed Installations for RPM files

Using software metering

You can manage software metering information using the KACE appliance.

About software metering

Software metering enables you to collect information about how applications are installed and used on the Windows and Mac devices that you manage.

Information collection includes Windows Store applications, such as Bing Travel. Metering is not available for applications installed other operating systems, such as Linux. In the Software Catalog, metering can be enabled for applications that are listed as Discovered and Not Discovered and for applications that are Locally Cataloged. Metering cannot be enabled for operating system software, applications installed on unsupported operating systems, such as Linux, or for applications that are listed as Uncataloged in the Software Catalog.

About Classic Metering

Classic Metering is the metering system that was available on the appliance prior to version 5.5. If you upgraded to version 5.5 from version 5.4 or lower, and you enabled metering prior to the upgrade, you can continue to access Classic Metering in the 5.5 release.

However, the Software Catalog metering system, which provides more detailed information than Classic Metering, replaced Classic Metering in the 6.0 release. Classic Metering is no longer available in version 6.0 and higher.

About metering information

When you enable metering for applications, information is collected for devices on which the applications are installed provided that metering is also enabled for the devices.

The following information is collected:

- Version information
- Information about suites
- Number of installations
- Usage and launch information

See Viewing Software Catalog metering information.

In addition, you can configure the frequency at which metering information is gathered and the length of time metering information is retained. See Configure options for metering Software Catalog applications.

About the scripts that collect metering information

The software metering service is bundled with the KACE Agent and installed on managed devices. When metering is enabled, scripts run to collect metering info.

These collection scripts vary, depending on the operating system:

- **Windows**: On Windows devices, metering is an event-driven process that monitors Windows assets using WMI (Windows Management Instrumentation) events.
- **Mac**: On Mac devices, the metering script identifies process events asynchronously using NSWorkspace notification center.

Information, including the application filename, version, and file size are compared to the information in the Software Catalog to identify the application.

How suites are metered

If metering is enabled for a suite, such as Microsoft Office, the system checks to determine whether any of the applications in the suite are running on managed devices that have metering enabled. Usage information is reported for the suite as a whole, as well as for each individual application.

Managed devices that have any application in the suite installed, as determined by an *Add/Remove programs* entry, are counted as having the suite installed. Devices do not need to have every application in the suite installed to count as having the suite installed.

When metering is enabled for a suite, it is also enabled for the individual applications that are part of the suite. You cannot enable or disable metering for individual applications in suites.

Enabling and configuring metering for devices and applications

To obtain metering information for Software Catalog applications, you need to enable metering for applications and for the devices on which those applications are installed.

Choosing the devices and applications to meter

Enabling metering on devices simply makes it possible to collect metering information, and it does not significantly increase server or network activity.

Therefore, Quest recommends that you enable metering for all of the Windows and Mac devices you manage. However, be selective when choosing the applications that you want to meter. Storing the metering information for a large number of applications could significantly increase disk space requirements and impact system performance.

Enabling metering on devices

To enable software metering on a managed devices, you need to apply a metering-enabled label to the devices.

To apply a metering-enabled label to devices, do one of the following:

- Apply the built-in label, *MeteredDevices*, to your devices. This label has the metering option enabled. See Setting up and using labels to manage groups of items.
- Create a manual label for metering and apply it to devices. See Enable metering on devices using manual labels.
- Create a Smart Label for metering (applied to devices automatically). See Disable metering for devices using Smart Labels.

TIP: To enable metering on managed devices, you can use manual labels or Smart Labels, but you must use labels. Metering can be enabled at the label level only; metering cannot be enabled in the settings of individual devices.

Enable metering on devices using manual labels

To enable metering on devices, you can enable metering for a manual label, and then apply that label to devices.

1. Go to the *Smart Labels* list:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, in the **Home** section, click **Label Management**.
   c. On the Label Management panel, click **Labels**.
2. Select **Choose Action** > **New Manual Label** to display the *Label Detail* page.

   TIP: Avoid using backslashes (\) in label names. If you need to use a backslash in a label name, add a second backslash (\\) to escape it.

3. Provide the following information:

Option	Description
Name	The name of the label.
Description	Any additional information you want to provide.
Alternate Location	(Optional) The alternate download location for Managed Installations, File Synchronizations, and other deployments that are performed on items assigned to this label. The location you specify replaces the string KACE_ALT_LOCATION. **CAUTION: You should not have a device in two labels that both specify a value in this field.**
Path	If you specify an alternate download location, specify the path to the location.
Login **Password**	If you specify an alternate download location, specify the username and password for the location.
Restrict Label Usage To	The type of label. To create a label that enables metering, select the *Device Inventory* check box. You can select additional label types as needed, but Metering can be enabled only if the *Devices* label type is selected.
Meter Software Usage	Enable metering on devices that have the label assigned. This enables metering on the devices only. To meter software, you need to also enable metering for individual applications.

Option	Description
Allow Application Control	Enable Application Control on devices. Software marked as Not Allowed is prevented from running on devices to which the label is applied. See Using Application Control.
Label Group	(Optional) The label group to which the label is assigned. To assign the label to a label group, click **Edit** next to the *Label Group* field, then select a label group. This is useful if you have a large number of labels and you want to organize them into sub-labels. For example, you could include the labels of your licensed applications in a group label named *Licenses*. In addition, labels inherit any restrictions of the groups to which they belong.

4. Click **Save**.

   The *Labels* page appears, and the new label appears on the list. The metering icon appears in the metering column next to the label: .

5. Manually apply the label to managed devices:
   a. Click **Inventory > Devices**.

      The *Devices* page appears.

   b. Select the check box next to one or more devices.
   c. Select **Choose Action** > **Apply Labels**.

      One of the following metering icons appears next to the device name on the *Devices* list:

Icon	Description
	Metering is enabled on the device, and the KACE Agent is scheduled to report metering information for Software Catalog applications that also have metering enabled. See Enabling and configuring metering for devices and applications. It might take as long as 24 hours for the appliance to display metering information in the **Administrator Console**, depending on the metering interval. To change the metering interval, see Enable metering for Software Catalog applications.
	Metering is scheduled to begin. This icon appears when the metering label is applied to a device, but that device has not yet reported metering information to the appliance. If the metering label has been applied to devices running Linux or other operating systems that are not supported, metering icons are not displayed.

Enable metering on devices using Smart Labels

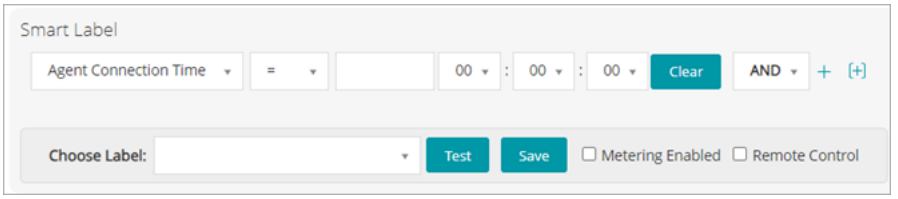
You can enable metering using Smart Labels provided that the Smart Label is a device label.

Smart Labels are applied to and removed from managed devices when the appliance processes device inventory. So if you create a Smart Label that enables metering on devices, it might take time for the Smart Label to be applied to devices and for devices to report metering information. Metering is enabled for devices that match the Smart Label criteria only after devices are inventoried and the Smart Label is applied.

1. Go to the *Smart Labels* list:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, in the **Home** section, click **Label Management**.

c. On the Label Management panel, click **Smart Labels**.

2. Select **Choose Action** > **New** > **Device Smart Label** to display the device Smart Label panel.
3. Specify the search criteria using the available fields.
   - **To add a row, click Add line.**
   - **To add a subset of rules, select AND or OR from the operator drop-down list at the right of the Smart Label criteria, then click Add Group.**



4. Click **Test** to display items that match the specified criteria.
5. Adjust the criteria as needed until the results are what you expect.
6. Select the *Metering Enabled* check box near the Smart Label criteria.
7. In the *Choose label* drop-down list, do one of the following:
   - **Select an existing label to associate with the Smart Label. Type in the *Choose label* field to search for existing labels.**

     NOTE: If you select a label group instead of a label, you will not be able to apply the Smart Label to a patching schedule. Patching schedules can only use Smart Labels based on a single item.
   - **Enter a new name for the Smart Label in the *Choose label* field, then press Enter or Return.**

   NOTE: Press **Enter** or **Return** after you enter a new Smart Label name to move the text from the search field to the label field.
8. Click **Save**.

When managed devices are inventoried, the Smart Label is applied if the devices match the specified criteria. When the label is applied to a device, one of the following metering icons appears next to the device name on the *Devices* list:

Icon	Description
	Metering is enabled on the device, and the KACE Agent is scheduled to report metering information for Software Catalog applications that also have metering enabled. See Enabling and configuring metering for devices and applications. It might take as long as 24 hours for the appliance to display metering information in the **Administrator Console**, depending on the metering interval. To change the metering interval, see Enable metering for Software Catalog applications.
	Metering is scheduled to begin. This icon appears when the metering label is applied to a device, but metering information is not yet available to the appliance. If the metering label has been applied to devices running Linux or other operating systems that are not supported, metering icons are not displayed.

Enable metering for Software Catalog applications

You can enable metering for applications that are listed as Discovered or Not Discovered in the Software Catalog, as well as for applications that are Locally Cataloged. When you enable metering for applications, those applications are identified as metered.

However, you also need to enable metering for the devices on which the applications are installed. In other words, you have to enable metering both on the device and on the application to obtain metering information.

When metering is enabled for an application, and for devices on which the application is installed, metering information is displayed on the *Software Catalog Detail* page for the application. Metering information is also displayed on the detail page of managed devices that have the application installed. See Viewing Software Catalog metering information.

CAUTION: Metering is not available for operating system software, applications installed on unsupported operating systems, such as Linux, or for applications that are listed as Uncataloged in the Software Catalog. However, you can enable metering for Uncataloged applications after you add the applications to the local version of the Software Catalog.

1. Go to the *Software Catalog* list:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Inventory**, then click **Software Catalog**.
2. Select the check box next to an application that is Discovered, or Not Discovered.
3. Select **Choose Action** > **Enable Metering**.

A metering icon appears in the metering column next to the selected applications: . Provided that metering is enabled for devices with the application installed, metering information is reported according to the metering schedule. See:

- Enabling metering on devices
- Configure options for metering Software Catalog applications

Configure options for metering Software Catalog applications

You can configure metering options, such as the frequency at which metering information is gathered, and the length of time metering information is retained in the appliance database.

If the Organization component is enabled on your appliance, you configure settings for each organization separately.

1. Do one of the following:
    - **If the Organization component is enabled on your appliance, log in to the appliance System Administration Console, `https://appliance_hostname/system`, or select System in the drop-down list in the top-right corner of the page next to the login information. Then click Organizations. To display the organization's information, click the organization's name.**

      On the *Organization Detail* page that appears, locate the *Communication and Agent Settings* section.
    - **If the Organization component is not enabled on your appliance, log in to the appliance Administrator Console, `https://appliance_hostname/admin`. Then select Settings > Provisioning., and click Communication Settings on the *Provisioning* panel.**

      The *Communication Settings* page appears.
2. In the *Agent and Communication Settings* section, specify the following settings:

Option
Agent Logging
Agent Inventory
Agentless Inventory
Catalog Inventory
Metering

Option
Scripting Update

3. Click **Save**.
4. To configure data retention settings for metering, go to the Admin-level *General Settings* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Settings**, then click **General Settings**.
5. In the *Data Retention* section, select the options for retaining data on the appliance.

Option	Description
Retain Metering Data	The number of months that metering data is retained in the appliance database. Metering data that is older than the selected number of months is deleted from the database on the first day of every month. See About metering information.

6. At the bottom of the page, click **Save** or **Save and Restart Services**, depending on whether the Organization component is enabled on your appliance.
7. If you have multiple organizations, repeat the preceding steps for each organization.

Viewing Software Catalog metering information

You can view metering information on the *Software Catalog Detail* page and on the *device detail* page.

NOTE: Metering information is available only if metering is enabled for devices and applications. For information, see Enabling and configuring metering for devices and applications.

View metering information on the Software Catalog Detail page

You can view metering information for Software Catalog applications on the *Software Catalog Detail* page.

The amount of metering information available on the *Software Catalog Detail* page is determined by the metering data retention settings. See About metering information.

1. Go to the *Software Catalog* list:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Inventory**, then click **Software Catalog**.
2. **Optional**: Click the metering column header to sort the list by applications that are metered:
3. Click the name of a metered application to display the *Software Catalog Detail* page.

Information on this page includes:

Column name	Description
Versions or Applications Installed	
File Name	For applications, the name of the executable file.
Product Name	For suites, the suite name.

Column name	Description
Version	The version number associated with the application.
Language	The language for which the application is designed. For example, English. Applications that are not designed for a specific language are designated as Language Neutral.
Installed	The number of managed devices that have the application installed. Click a number to view device information.
Metering	
Last Day	The number of managed devices that have launched the application in the past 24 hours.
1-7 Days Ago	The number of managed devices that have launched the application in the past 7 days.
8-30 Days Ago	The number of managed devices that have launched the application in the past 8-30 days.
31-40 Days Ago	The number of managed devices that have launched the application in the past 31-40 days.

View metering information on the Device Detail page

You can view metering information for Software Catalog applications on the *Device Detail* page.

1. Go to the *Devices* list:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Inventory**, then click **Device**s.
2. Click the name of a managed device that has metering enabled to display the *Device Detail* page.
3. In the *Software* tab, click **Metered Software** to expand the panel.

Information in this section includes:

Column name	Description
Application	The name of the metered application. Click the application name to go to the detail page for the application.
Version	The version of the application installed. Major versions are listed separately in the Software Catalog, and they are metered separately. For example, version **4.1** and version **4.2** of an application appear as separate entries. This enables you to manage them and meter their usage separately. Minor versions, such as **4.123**, **4.134**, and **4.145** appear under the same entry, such as **4.x**. Each version grouped under the **4.x** entry is listed on the detail page for the application.
Hours Used	The length of time the application has been running on the device in the past seven days, expressed as a decimal. For example, 0.75 indicates that the application has been running for 45 minutes.

Column name	Description
Launches	The number of times the application has been launched on the device in the past seven days.
Last Launch	The date and time of the most recent launch in the past seven days.

NOTE: If new applications are installed between the time the inventory is collected from a device and the time the metering report is generated, those applications are not reported until the next time inventory is collected.

Disabling metering for Software Catalog applications and managed devices

Disabling metering for applications and devices stops the system from saving metering data for those applications and devices. Metering data that has already been saved, however, is retained.

Disable metering for Software Catalog applications

If metering is enabled for Software Catalog applications, you can disable it as needed.

1. Go to the *Software Catalog* list:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Inventory**, then click **Software Catalog**.
2. Select the check box next to an application.
3. Select **Choose Action** > **Metering** > **Disable**.

Metering is disabled and the metering icon is removed from the metering column next to the selected applications. Metering data, however, is retained.

Disabling metering for devices

If metering is enabled for devices, you can disable it as needed.

Disable metering for devices using manual labels

If metering is enabled for devices using manual labels, you can disable it by disabling metering in the label details.

1. Go to the *Labels* list:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, in the **Home** section, click **Label Management**.
    c. On the Label Management panel, click **Labels**.
2. Select the check box next to a metering label.
3. Select **Choose Action** > **Disable Metering**.

Metering is disabled on all the devices to which the label is applied. Metering data, however, is retained.

Disable metering for devices using Smart Labels

If metering is enabled for devices using Smart Labels, you can disable it by disabling metering in the Smart Label details.

1. Go to the *Smart Label Detail* page:

a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
b. On the left navigation bar, in the **Home** section, click **Label Management**.
c. On the Label Management panel, click **Smart Labels**.
d. Click the name of a Smart Label.

2. Clear the *Enable Metering* check box.

Metering is disabled on all the devices to which the label is applied. Metering data, however, is retained.

Managing metering and scheduling inventory collection

Metering is available for Software Catalog applications only. Metering is not available for applications that appear on the *Software* page.

For information about enabling metering, see About metering information.

Schedule metering and inventory collection intervals

Metering and inventory collection intervals determine the frequency with which metering and inventory information is collected from managed devices. If the Organization component is enabled on your appliance, you can schedule the metering and inventory collection intervals separately for each organization.

1. Do one of the following:

   - **If the Organization component is enabled on your appliance, log in to the appliance System Administration Console, `https://appliance_hostname/system`, or select System in the drop-down list in the top-right corner of the page next to the login information. Then click Organizations. To display the organization's information, click the organization's name.**

     On the *Organization Detail* page that appears, locate the *Communication and Agent Settings* section.

   - **If the Organization component is not enabled on your appliance, log in to the appliance Administrator Console, `https://appliance_hostname/admin`. Then select Settings > Provisioning., and click Communication Settings on the *Provisioning* panel.**

     The *Communication Settings* page appears.

2. In the *Agent and Communication Settings* section, specify the following settings:

Option	Suggested Setting	Notes
Agent Logging	Enabled	Whether the appliance stores scripting results provided by Agents installed on managed devices. Agent logs can consume as much as 1GB of disk space in the database. If disk space is not an issue, enable *Agent Logging* to keep all log information for Agent-managed devices. These logs can be useful during troubleshooting. To save disk space, and enable faster Agent communication, disable *Agent Logging*.
Agent Inventory	12 hours	The frequency at which Agents on managed devices report inventory. This information is displayed in the *Inventory* section.
Agentless Inventory	1 Day	The frequency at which Agentless devices report inventory. This information is displayed in the *Inventory* section.
Catalog Inventory	24 hours	The frequency at which managed devices report inventory to the *Software Catalog* page.

Option	Suggested Setting	Notes
Metering	4 hours	The frequency at which managed devices report metering information to the appliance. Requires metering to be enabled on devices and applications.
Scripting Update	4 hours	The frequency at which Agents on managed devices request updated copies of scripts that are enabled on managed devices. This interval does not affect how often scripts run.

3. Click **Save**.

Using Application Control

Application Control enables you to mark applications as Not Allowed and block them or prevent them from running on Agent-managed Windows and Mac devices. This is useful if you want to restrict specific applications from running in your environment.

Application Control enables you to:

- Prevent specific applications from running on Agent-managed Windows or Mac devices. This feature is not available for Linux or Agentless devices. See Requirements for blocking applications.
- Create reports on applications that are marked as Not Allowed. See Create reports showing applications marked as Not Allowed.
- Search for applications that are marked as Not Allowed using *Advanced Search*. See Searching for information and filtering lists.

Applications marked as Not Allowed are organization-specific. If the Organization component is enabled on your appliance, you mark applications as Not Allowed for each organization separately.

Requirements for blocking applications

Application Control requirements must be met for applications to be blocked.

To block applications and prevent them from being launched on managed devices, you must:

- **Install the KACE Agent version 6.0 or higher on devices**. Application Control is not available for Agent versions lower than 6.0, and it is not available for Linux or Agentless devices. See Updating the KACE Agent on managed devices.
- **Apply a label that has Application Control enabled, to devices**. This enables the Agent to monitor application launches, including applications that are marked as Not Allowed. See Apply the Application Control label to devices.
- **Mark applications as Not Allowed**. Windows and Mac applications can be marked as Not Allowed only if they are in the Software Catalog as Discovered, Not Discovered, or Locally Cataloged applications. Applications that are Uncataloged cannot be marked as Not Allowed until they are added to the Software Catalog. See Adding applications to the Software Catalog. Linux applications cannot be marked as not allowed.
- **Specify the version of the application to be blocked**. For example, if you want to block all versions of Adobe Acrobat®, you must mark all versions of the application as Not Allowed. For example, Acrobat 8.x, Acrobat 9.x, and so on. However, when you mark a suite as Not Allowed, all of the applications in the suite are also marked as Not Allowed. If an application that runs on both Windows and Mac devices is marked as Not Allowed, that application is blocked on both Windows and Mac devices.

How applications are blocked

When an application that is marked as Not Allowed is launched on a managed device that has an Application Control-enabled label applied, the Agent terminates the application and displays a message on the device.

The message shows the application name and indicates that the application has been terminated because it is on the Not Allowed list. Applications that are terminated are identified in the local database that records software usage.

About denying access to application editions that share executable files

Some applications have different editions, such as Pro and Standard, that share the same executable file. If such applications are blocked, they are blocked for all editions that share the executable file.

Applications that cannot be blocked

Some applications, such as plug-ins to other applications, cannot be blocked.

The following applications can be marked as Not Allowed but they cannot be blocked or prevented from running on managed devices:

- Browser plug-ins or external DLLs
- Microsoft Visual Studio® plug-ins such as Infragistics
- Java® applications

Apply the Application Control label to devices

To enable Application Control on devices, you need to apply the *ApplicationControlDevices* label, or any label that has Application Control enabled, to devices.

After the label is applied to devices, applications that have been marked as Not Allowed are blocked or prevented from running on the devices.

1. Go to the *Devices* list:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Inventory**, then click **Device**s.
2. Select the check boxes next to one or more devices.
3. Select **Choose Action** > **Apply Labels**.
4. Drag and drop to the **Apply these Label** space, and click the **Apply Label** button.

The label appears next to device names on the *Devices* page.

Mark applications and suites as Not Allowed

You can mark individual applications, and application suites, as Not Allowed to prevent them from running on Agent-managed devices.

When you mark a suite as Not Allowed, the applications in that suite are also marked as Not Allowed. If you want to mark only some of the applications in a suite as Not Allowed, remove the Not Allowed designation from the suite, then mark the individual applications as Not Allowed.

1. Go to the *Software Catalog* list:

a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.

b. On the left navigation bar, click **Inventory**, then click **Software Catalog**.

2. Select the check box next to one or more applications.
3. Select **Choose Action** > **Mark Not Allowed**.

The applications are marked as Not Allowed, and the Not Allowed icon appears next to the application names: .

View applications and suites that are marked as Not Allowed

You can view applications and suites that are marked as Not Allowed on the *Software Catalog* page.

1. Go to the *Software Catalog* list:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.

   b. On the left navigation bar, click **Inventory**, then click **Software Catalog**.
2. Do one of the following:
   - **Click the Discovered or Not Discovered tab above the list on the left, then click the Not Allowed button on the *Software Catalog* page to sort the results by applications that are marked as Not Allowed:** .
   - **Click the Advanced Search tab above the list on the right, then specify the criteria required for to view applications marked as Not Allowed:**

     ```
     Software Catalog: Not Allowed | is | True
     ```
3. Click **Search**.

Create reports showing applications marked as Not Allowed

You can create reports that show the applications that are marked as Not Allowed, and the devices on which those applications are installed.

1. Go to the *Reports* list by doing one of the following:
   - **If your appliance has the Organization component enabled, and you want to access a System-level report:**

     Log in to the appliance System Administration Console, `https://`**appliance_hostname**`/system`, or select **System** from the drop-down list in the top-right corner of the page. Then click **Reporting**.
     System-level reports include consolidated reports that aggregate information from all organizations, as well as standard reports for various appliance components.
   - **If your appliance does not have the Organization component enabled, or if you want to access an organization-level report, log in to the appliance Administrator Console, `https://`appliance_hostname`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information. Then click Reporting.**

     Organization-level reports include standard reports for various appliance components. If the Organization component is enabled on your appliance, these reports provide information specific to the selected organization.

The *Reports* list appears.

2. Select **Choose Action** > **New (Wizard)** to display the *Report Title* page.
3. Specify the following settings:

Option	Description
Title	Not Allowed Software.
Category	Software.
Description	Software marked as Not Allowed.
Show Line Numbers	(Optional) Select the check box to add a column with line numbers to the report.
Topic	Software Catalog - Discovered Software.
Subtopic	Device

4. Click **Next** to display the *Fields to Display* page.
5. Select report fields, such as:
   - **Name: The name of the application.**
   - **Installed On: The number of devices on which the application is installed.**
   - **Category: The category of the application.**
   - **Device: Information about the devices on which the application is installed.**
6. Click **Next** to display the *Column Order* page.
7. Drag the columns to set the order in which you want columns to appear in the report, then click **Next** to display the *Sort and Breaks* page.
8. Select Sort and Break options, then click **Next** to display the *Filters* page.
9. Click **Specify rules to filter the records**, then specify the criteria required to find applications marked as Not Allowed:

```
Discovered Software Info: Not Allowed | = | 1
```

10. Click **Save** in the row, then click **Save** at the bottom of the page.

    The *Reports* list appears with the new report listed. the *View By* list, which appears above the table on the right, is automatically set to the category of the new report.
11. To run the report, click a format in the *Generate Report* column.

The report is generated. In HTML reports, the first data column is automatically linked to the detail page for the item in the **Administrator Console**. For more information about reports, see Creating reports.

Remove the Not Allowed designation from applications

If you have marked applications as Not Allowed, you can remove that designation as needed.

The Not Allowed designation is organization-specific. If the Organization component is enabled on your appliance, you apply and remove the Not Allowed designation from applications in each organization separately.

TIP: By default, applications are allowed unless you mark them as Not Allowed.

1. Go to the *Software Catalog* list:

a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.

b. On the left navigation bar, click **Inventory**, then click **Software Catalog**.

2. Select the check box next to one or more applications.
3. Select **Choose Action** > **Mark Allowed**.

   The applications are marked as Allowed and the Not Allowed symbol is removed.

Update or reinstall the Software Catalog

The Software Catalog is continually updated as new applications become available and as cataloging requests are received. These updates are automatically downloaded and installed to KACE SMAs periodically. You can manually check for updates to the Software Catalog, or reinstall the catalog.

If you have an offline appliance that does not connect to the Internet, you can obtain Software Catalog updates by contacting **Quest Support** at https://support.quest.com/contact-support.

NOTE: When catalog updates are downloaded, the appliance determines whether any Locally Cataloged applications have been added to the public Software Catalog. If applications have been added, Local Cataloging is removed. Otherwise, Local Cataloging is preserved.

1. Go to the appliance *Control Panel*:
   - **If the Organization component is not enabled on the appliance, log in to the appliance Administrator Console, `https://appliance_hostname/admin`, then select Settings > Control Panel.**
   - **If the Organization component is enabled on the appliance, log in to the appliance System Administration Console, `https://appliance_hostname/system`, or select System in the drop-down list in the top-right corner of the page, then select Settings > Control Panel.**
2. Click **Appliance Updates** to display the *Appliance Updates* page.
3. Do one of the following:
   - **In the *Software Catalog* section, click Check for Update.**

     If the Software Catalog is up to date, the *Logs* page appears showing the version information. If an update is available, installation information is displayed. The full catalog might be installed if any of the following are true: If there is no baseline catalog present on the appliance, if there is no pathway to updating the full catalog, or if there are more than five updates available
   - **In the *Software Catalog* section, click Reinstall.**

     The version of the Software Catalog that is stored on the appliance is replaced with the latest Software Catalog available from Quest KACE. The full Software Catalog includes the latest full version of the catalog as well as any updates, or differentials, that have been added since the latest full version was released.
   - **If your appliance is offline and does not have Internet access, contact Quest Support at https://support.quest.com/contact-support.**

Managing process, startup program, and service inventory

You can manage processes, startup programs, and services in appliance inventory.

Managing process inventory

When processes are detected on managed devices, they are reported and available to be managed in the *Inventory* section.

To manage process inventory, you can:

- View process usage information for the last 1, 2, 3, 6, or 12 months
- Apply labels to, and remove labels from, processes
- Assign categories and threat levels to processes
- Delete processes

Process inventory cannot be metered, and you cannot block processes. However, you can block applications. See Mark applications and suites as Not Allowed.

View and edit process details

You can view and edit the details of processes in inventory.

1. Go to the *Process Detail* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Inventory**, then click **Processes**.
    c. Click the name of a process.
2. Provide the following information:

Option	Description
Restrict To Label	(Optional) the label associated with the item.
Notes	Any additional information you want to provide.
Category	The category of the item, such as Business, Driver, or Security.
Threat Level	The threat level of the item. Threat levels include: 1. Safe 2. Fairly Safe 3. Unknown 4. Could be harmful 5. Harmful

3. Click **Save**.

Add labels for processes

Add manual labels to manage processes in inventory as a group.

1. Go to the *Processes* list:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.

b. On the left navigation bar, click **Inventory**, then click **Processes**.

2. Select **Choose Action** > **Add Label**.
3. In the *Add Label* window, enter a name for the label.

   TIP: Avoid using backslashes (\) in label names. If you need to use a backslash in a label name, add a second backslash (\\) to escape it.

4. Click **Add Label**.

Apply labels to or remove labels from processes

Labels can be applied to or removed from processes in inventory as needed.

1. Go to the *Processes* list:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Inventory**, then click **Processes**.
2. Select the check box next to one or more processes.
3. Do one of the following:
   - **Select Choose Action > Apply Label, then select the label to apply.**
   - **Select Choose Action > Remove Label, then select the label to remove.**

Categorize processes

To organize and manage processes in inventory, you can manually assign them to categories.

1. Go to the *Processes* list:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Inventory**, then click **Processes**.
2. Select the check box next to one or more processes.
3. Select **Choose Action** > **Set Category**, and then select a category.

Assign threat levels to processes

To manage processes that might pose threats to devices and systems, you can manually assign threat levels to those processes.

Threat levels can be used to indicate the relative safety of items and the number of devices on which those items are located. This information is for tracking purposes only. The appliance does not enforce policies based on threat levels.

1. Go to the *Processes* list:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Inventory**, then click **Processes**.
2. Select the check box next to one or more processes.
3. Select **Choose Action** > **Set Level**, and then select a threat level.

Delete processes

You can manually delete processes from inventory as needed.

However, if the deleted processes are found on managed devices, the records for those processes are recreated, with new IDs, when the devices update inventory information.

1. Go to the *Processes* list:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Inventory**, then click **Processes**.
2. Do one of the following:
    - **Select the check box next to one or more processes, then select Choose Action > Delete.**
    - **Click a process name, then on the *Process Detail* page, click Delete.**
3. Click **Yes** to confirm.

Managing startup program inventory

When startup programs are detected on managed devices, they are reported and available to be managed in the *Inventory* section.

The startup inventory page enables you to view and edit information about startup programs that have been detected on managed devices.

Startup inventory details include the name of the device running the startup programs, the system description, and the last user.

Startup programs cannot be metered.

View and edit startup program details

You can view and edit the details of startup programs in inventory.

1. Go to the *Startup Program Detail* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Inventory**, then click **Startup Programs**.
    c. Click the name of a startup program.

    Devices that are running the program are listed at the bottom of the page.
2. Provide the following information:

Option	Description
Restrict To Label	(Optional) the label associated with the item.
Notes	Any additional information you want to provide.
Category	The category of the item, such as Business, Driver, or Security.
Threat Level	The threat level of the item.

Option	Description
	Threat levels include: 1. Safe 2. Fairly Safe 3. Unknown 4. Could be harmful 5. Harmful

3. Click **Save**.

Add labels for startup programs

Add manual labels to manage startup programs in inventory as a group.

1. Go to the *Startup Programs* list:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Inventory**, then click **Startup Programs**.
2. Select **Choose Action** > **Add Label**.
3. In the *Add Label* window, enter a name for the label.

    TIP: Avoid using backslashes (\) in label names. If you need to use a backslash in a label name, add a second backslash (\\) to escape it.

4. Click **Save**.

Apply labels to or remove labels from startup programs

Labels can be applied to or removed from startup programs in inventory as needed.

1. Go to the *Startup Programs* list:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Inventory**, then click **Startup Programs**.
2. Select the check box next to one or more programs.
3. Do one of the following:
    - **Select Choose Action > Apply Label, then select the label to apply.**
    - **Select Choose Action > Remove Label, then select the label to remove.**

Categorize startup programs

To organize and manage startup programs in inventory, you can manually assign them to categories.

1. Go to the *Startup Programs* list:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Inventory**, then click **Startup Programs**.
2. Select the check box next to one or more programs.
3. Select **Choose Action** > **Set Category**, then select a category.

Assign threat levels to startup programs

To manage startup programs that might pose threats to devices and systems, you can manually assign threat levels to those programs.

Threat levels can be used to indicate the relative safety of items and the number of devices on which those items are located. This information is for tracking purposes only. The appliance does not enforce policies based on threat levels.

1. Go to the *Startup Programs* list:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Inventory**, then click **Startup Programs**.
2. Select the check box next to one or more programs.
3. Select **Choose Action** > **Set Threat Level**, then select a threat level.

Delete startup programs

You can manually delete startup programs from inventory as needed.

However, if the deleted startup programs are found on managed devices, the records for those programs are recreated, with new IDs, when the devices update inventory information.

1. Go to the *Startup Programs* list:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Inventory**, then click **Startup Programs**.
2. Do one of the following:
    - **Select the check box next to one or more programs, then select Choose Action > Delete.**
    - **Click a program name, then on the *Startup Program Detail* page, click Delete.**
3. Click **Yes** to confirm.

Managing service inventory

When services are detected on managed devices, they are reported and available to be managed in the *Inventory* section.

The service inventory page enables you to track the services running on managed devices.

Service detail pages provide information on services, including the name of the device running the services, system description, and the last user.

Service inventory cannot be metered.

View and edit service details

You can view and edit the details of services in inventory.

1. Go to the *Service Detail* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Inventory**, then click **Services**.

c. Click the name of a service.

Devices that are running the service are listed at the bottom of the page.

2. Provide the following information:

Option	Description
Restrict To Label	(Optional) the label associated with the item.
Notes	Any additional information you want to provide.
Category	The category of the item, such as Business, Driver, or Security.
Threat Level	The threat level of the item. Threat levels include: 1. Safe 2. Fairly Safe 3. Unknown 4. Could be harmful 5. Harmful

3. Click **Save**.

Add labels for services

Add manual labels to manage services in inventory as a group.

1. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
2. Select **Inventory** > **Services** to display the *Services* page.
3. Select **Choose Action** > **Add Label**.
4. In the *Add Label* window, enter a name for the label.

   TIP: Avoid using backslashes (\) in label names. If you need to use a backslash in a label name, add a second backslash (\\) to escape it.

5. Click **Save**.

Apply labels to and remove labels from services

Labels can be applied to or removed from services in inventory as needed.

1. Go to the *Services* list:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Inventory**, then click **Services**.
2. Select the check box next to one or more services.
3. Do one of the following:
   - **Select Choose Action > Apply Label, then select the labels to apply.**
   - **Select Choose Action > Remove Label, then select the labels to remove.**

Categorize services

To organize and manage services in inventory, you can manually assign them to categories.

1. Go to the *Services* list:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Inventory**, then click **Services**.
2. Select the check box next to one or more services.
3. Select **Choose Action** > **Set Category**, and then select a category.

Assign threat levels to services

To manage services that might pose threats to devices and systems, you can manually assign threat levels to those services.

Threat levels can be used to indicate the relative safety of items and the number of devices on which those items are located. This information is for tracking purposes only. The appliance does not enforce policies based on threat levels.

1. Go to the *Services* list:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Inventory**, then click **Services**.
2. Select the check box next to one or more services.
3. Select **Choose Action** > **Set Threat Level**, and then select a threat level.

Delete services

You can manually delete services from inventory as needed.

However, if the deleted services are found on managed devices, the records for those services are recreated, with new IDs, when the devices update inventory information.

1. Go to the *Services* list:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Inventory**, then click **Services**.
2. Select the check box next to one or more services.
3. Do one of the following:
    - **Select the check box next to one or more programs, then select Choose Action > Delete.**
    - **Click a program name, then on the *Startup Program Detail* page, click Delete.**
4. Select **Yes** to confirm.

Writing custom inventory rules

You can write Custom Inventory rules to collect detailed information about items in inventory.

For information on using the Inventory component, see Managing applications on the Software page.

About Custom Inventory rules

Custom Inventory rules enable you to capture customized information during the inventory collection process.

Custom Inventory rules are useful for:

- Managing software that is not listed in the Windows *Add/Remove Programs* section.
- Managing versions of software with the same entry in the Windows *Add/Remove Programs* section, especially with incorrect or incomplete *Display Version* information.
- Capturing customized details for use in reports.
- Writing deployment rules, scripts, and reports based on the presence of an application or a value that is not reported by the KACE Agent.

For more information, see:

- Create Custom Inventory rules
- Types of Custom Inventory rules
- How Custom Inventory rules are implemented
- Test Custom Inventory rules

Types of Custom Inventory rules

Custom Inventory rules test, or obtain the values of, registry keys and entries, program, files, scripts, environment variables, system properties, and the output of commands.

There are two types of Custom Inventory rules:

- **Conditional rules**: These rules test whether conditions exist on devices. When a rule returns true, the KACE Agent reports the item as an Installed Program. When the rule returns false, the item does not appear as an Installed Program.
- **Value Return rules**: These rules obtain data from devices. If the value exists, the KACE Agent reports the item as an Installed Program and sets a corresponding *Custom Inventory Field*.

Create Custom Inventory rules

You can create custom applications, and Custom Inventory rules for those applications, so that information about the applications is gathered from managed devices.

1. Go to the *Software Detail* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click *Inventory*, then click *Custom Inventory*.
    c. Select **Choose Action** > **New**.
2. Provide general information: *Name*, *Version*, *Publisher*.

    For proper downstream reporting, enter this information consistently across software inventory.
3. Provide the following information:

Option	Description
Restrict To Label	(Optional) The label associated with the item.

Option	Description
Notes	Any additional information you want to provide.
Supported Operating Systems	The operating systems on which the application runs. Applications are deployed only to devices with the selected operating systems.

Custom Inventory Rule	(Optional) The custom inventory rules to apply to the application. Custom inventory rules enable you to detect applications and other items on a device and capture details for reporting.
	For example, the appliance first verifies whether an application is present on a device before deploying that application. In some instances, however, installed programs do not register in *Add/Remove Programs* or in standard areas of the registry. In such cases, the appliance might not be able to detect the presence of the application without additional information from the administrator. Therefore, the appliance might repeat the installation each time the device connects. Custom Inventory rules can prevent this repetition.
	The following rule verifies that the version of the Network Associates VirusScan installed on a device is newer than a given version before deploying it:
	`RegistryValueGreaterThan(HKEY_LOCAL_MACHINE\ Software\Network Associates\TVD\`
	`Network Associates\TVD\Shared Components\ VirusScanEngine\4.0.xx,szDatVersion,4.0.44)`

4. Next to *Upload and Associate File*, click **Choose File** to locate a file, then click **Open** or **Choose**.

   To distribute applications using Managed Installations or File Synchronizations, you need to associate the actual application files with the application.

5. To prevent the file from being copied to Replication Shares, select **Don't Replicate Associated File**. This setting is useful for large files that you do not want users to install from Replication Shares, such as software suites.
6. **Optional**: Select a *Category* and *Threat Level* for the software.
7. Click **Save**.

Related topics

About labels

Getting values from a device (Custom Inventory Field)

Using software threat levels and categories

How Custom Inventory rules are implemented

The KACE Agent receives new Custom Inventory rules during the first device inventory after the rules are created. During that first inventory, the Agent runs the new rules and reports the findings to the appliance.

The Agent runs all rules as well as any other processes scheduled for that session. Therefore, after a device is inventoried, it could take several minutes to run all the rules and other processes before the Agent reports the results.

After the Agent reports the results, the device's detail page shows the results under *Software* in *Installed Programs* and *Custom Inventory Fields*.

NOTE: The applications with Value Return rules that set a *Custom Inventory Field* also appear as Installed Programs.

If results are not what you expect, verify that the device has been inventoried recently. The inventory time is shown in the *Last Inventory* field of the device detail page.

Syntax for Custom Inventory rules

Use the correct syntax for function names and arguments in Custom Inventory rules.

Conditional and Value Return rules use the following syntax:

```
functionName(argument,argument,...)
```

For specific information on functions and their arguments see:

- Checking for conditions (conditional rules)
- Getting values from a device (Custom Inventory Field)
- Matching filenames to regular expressions

Function syntax

Enter the **functionName** followed by an opening parenthesis, enclose the arguments with a closing parenthesis. No spaces are allowed between the name of the function and the opening parenthesis.

Argument syntax

Enter **argument** syntax for all rules except `command` and `regex` (regular expression) as follows:

- Separate arguments by commas.
- Commas are not allowed anywhere else in the string, except as described in Commas and parentheses as values in a rule.
- Do not include single or double quotation marks.
- White space is trimmed from the front and back of each argument.

For example, the following syntaxes are the same:

```
RegistryValueEquals(HKEY_LOCAL_MACHINE\SOFTWARE\Mozilla\Mozilla Firefox, CurrentVersion, 78.0.2)
RegistryValueEquals(HKEY_LOCAL_MACHINE\SOFTWARE\Mozilla\Mozilla Firefox,CurrentVersion,78.0.2)
```

Commas and parentheses as values in a rule

If comma, open parenthesis, or close parenthesis are to be used as values in a rule, they must be escaped as {{comma}}. {{op}}, and {{cp}}, respectively.

- In arguments where commas are needed as part of the parameter value, the comma needs to be escaped as {{comma}}, except for the last argument in the function.

  For example, if the user want to test against the registry value in which the value name is "**test,value**", the user would need to escape the comma in this case because registry value name is not the last argument in the Custom Inventory (CI) function.

  `RegistryValueEquals(HKEY_LOCAL_MACHINE\SOFTWARE\TestSoft,` **`test{{comma}}value`**`, HelloWorld)`

  If the user wants to test against the registry value where the value itself contains a comma, then there is no need to escape, because value is the last argument in the Custom Inventory function. The following Custom Inventory tests registy value HKLM\SOFTWARE\TestSoft\test1 and looks to see if the value is equal to **2,4**.

  `RegistryValueEquals(HKEY_LOCAL_MACHINE\SOFTWARE\TestSoft,test1,`**`2,4`**`)`

  If the Custom Inventory function contains only one parameter, it takes everything between the parentheses as the value for the argument. Commas in this case do not need to be escaped and will be part of the argument to the Custom Inventory function.

  `ShellCommandTextReturn(`**`wmic MEMORYCHIP get BankLabel,Capacity,description,manufacturer`**`)`

- An unmatched literal open parenthesis needs to be escaped as **{{op}}**. When the parser is tokenizing the arguments for the function, it counts the number of open and close parentheses to determine the end of the function and argument. Therefore, an unmatched literal open parenthesis would throw off the count, and cause the argument value to be parsed incorrectly. If a literal open parenthesis is needed as part of the argument value, it should be represented with **{{op}}**.

For example, if the user wants to echo the string "**Hello (World**", then the CI should look like the following:
`ShellCommandTextReturn(echo` **Hello {{op}} World**`)`

- Unmatched literal close parentheses needs to be escaped as **{{cp}}**.

  While the parser is tokenizing the arguments for the function, it counts the number of open and close parentheses in order to determine the end of the function when it encounter the last matched close parentheses. However, if the argument value itself contains a close parenthesis that is not matched, the parenthesis tricks the parser to believe that is the end of the function and the argument value will be truncated prematurely.
  If a literal close parentheses is needed as part of the argument value, it must be represented with **{{cp}}**.
  For example, if the user wants to echo the string "**Hello) World**", then the CI should look like the following:
  `ShellCommandTextReturn(echo` **Hello {{cp}} World**`)`

Checking for conditions (conditional rules)

You can write Custom Inventory rules that identify whether (true/false) an application is installed.

When using a conditional rule, if the rule returns true, the Display name (Title) of the custom application appears in the *Software: Installed Programs* section of the *Device Detail* page in the *Inventory* section.

The following sections describe the rules that test for conditions:

- Conditional rule reference
- Verifying whether a condition exists (Exists rules)
- Evaluating device settings (Equals rules)
- Comparing device values (Greater Than and Less Than rules)
- Testing for multiple conditions

When the rule returns false, the application does not appear in the *Installed Programs* section in the device's inventory details.

TIP: You can view a list of devices that have the item installed on the *Inventory* > *Custom Inventory* > *Custom_item: Detail* page.

Conditional rule reference

The following table describes which data types can be used for comparison.

Table 24. Data types supported for comparison functions

Conditional rule	Data types supported for comparison functions `Equals`, `GreaterThan`, `LessThan`
`EnvironmentVariable`	DATE, NUMBER, TEXT
`FileInfo`	DATE, NUMBER, TEXT
`FilenamesMatchingRegex`	NUMBER
`FileVersion`	TEXT
`PlistValue`	NUMBER, TEXT
`ProductVersion`	TEXT

Conditional rule	Data types supported for comparison functions `Equals`, `GreaterThan`, `LessThan`
`RegistryValue`	TEXT

The following table describes how comparisons are made.

Table 25. How comparisons are made

Data type	Considerations
DATE	• Before evaluation, target values are parsed as a date using the same rules as in the PHP DateTime class and then normalized to use the following format: `MM/DD/YYYY HH:MM:SS` • The timestamp listed in the appliance database uses the 24-hour clock (0 – 24 hours). • The timestamp listed in the appliance database reflects UTC (Coordinated Universal Time) time, so that it is normalized for all devices, regardless of their respective timezones. • If the target value contains only a date, a timestamp will be added that is based upon midnight for UTC.
NUMBER	• Only whole numbers are evaluated. • If a target value contains any other characters (letters, punctuation marks and so on), only the numbers up to the first non-number are evaluated. For example, if the target value is 52a1, only 52 is evaluated. • Only numbers up to the 32-bit integer maximum positive value (2,147,483,647) are supported.
TEXT	• Values are evaluated verbatim, without any potential formatting changes (as can occur with DATE and NUMBER data types). • Text strings are evaluated in lexicographical order. • Commas can be present in the strings being evaluated — no escaping is required.

The following table lists available conditional rules with links to specific details on how to specify the arguments.

Table 26. Conditional rule reference

Syntax	Win	RHEL	OS X	Description
`DirectoryExists (path)`	X	X	X	Checks for a directory at the specified path on the device.
`FileExists (path)`	X	X	X	Checks for a file at the specified path on the device. Include the name of the file and extension in the path.
`FileVersionEquals (path, version)`	X			Verifies that the **Version** > **File Version** property of the file specified in the path matches the TEXT value you entered.

Syntax	Win	RHEL	OS X	Description
`FileVersionLessThan (path, version)`	X			Verifies that the **Version** > **File Version** property of the file you specified as the path is lower than the TEXT value you entered.
`FileVersionGreaterThan (path, version)`	X			Verifies that the **Version** > **File Version** property of the file you specified is higher than the TEXT value you entered.
`ProductVersionEquals (path, version)`	X			Verifies that the **Version** > **Product Version** property of the executable or installation file you specified matches the TEXT value you entered.
`ProductVersionLessThan (path, version)`	X			Verifies that the **Version** > **Product Version** property of the executable or installation file you specified is lower than the TEXT value you entered.
`ProductVersionGreaterThan (path, version)`	X			Verifies that the **Version** > **Product Version** property of the executable or installation file you specified is higher than the TEXT value you entered.
`FileInfoGreaterThan (fullpath, attribute, type, value)`	X	X	X	Verifies that the **File Info** property of the executable or installation file you specified is higher than the value you entered.
`FileInfoLessThan (fullpath, attribute, type, value)`	X	X	X	Verifies that the **File Info** property of the executable or installation file you specified is lower than the value you entered.
`FileInfoEquals (fullpath, attribute, type, value)`	X	X	X	Verifies that the attribute of the executable or installation file you specified matches the value you entered.
`RegistryKeyExists (registryPath)`	X			Verifies that a registry key exists.
`RegistryValueEquals (registryPath, valueName, value)`	X			Verifies that a registry entry exactly matches the value you specify. Value is compared as TEXT.
`RegistryValueLessThan (registryPath, valueName, value)`	X			Verifies that the registry entry is lower than the value you specify. Value is a TEXT.

Syntax	Win	RHEL	OS X	Description
`RegistryValueGreaterThan (registryPath, valueName, value)`	X			Verifies that the registry entry is higher than the value you specify. Value is a TEXT.
`EnvironmentalVariableExists (var)`	X	X	X	Verifies that an environment variable with the name you specify exists.
`EnvironmentalVariableGreaterThan (var, type, value)`	X	X	X	Verifies that the environment variable definition is higher than the value you specify. All three types are valid, TEXT, DATE (in the full format `mm/dd/yyyy hh:mm:ss`), and NUMBER.
`EnvironmentalVariableLessThan (var, type, value)`	X	X	X	Verifies that the environment variable definition is lower than the value you specify. All three types are valid, TEXT, DATE (in the full format `mm/dd/yyyy hh:mm:ss`), and NUMBER.
`EnvironmentalVariableEquals (var, type, value)`	X	X	X	Verifies that the environment variable definition exactly matches the value you specify. All three types are valid, TEXT, DATE (in the full format `mm/dd/yyyy hh:mm:ss`), and NUMBER.
`PlistValueExists (fullpath, entry)`			X	Verifies that a named value exists in a PLIST file.
`PlistValueGreaterThan (fullpath, entry, type, value)`			X	Verifies that the named value is a NUMBER or TEXT higher than the value you specified.
`PlistValueLessThan (fullpath, entry, type, value)`			X	Verifies that the named value is a NUMBER or TEXT lower than the value you specified.
`PlistValueEquals (fullpath, entry, type, value)`			X	Verifies that the named value is a NUMBER or TEXT that exactly matches the value you specified.

For information on `Equals`, `GreaterThan`, and `LessThan` for `FilenamesMatchingRegex`, see Regular Expression Rule Reference.

Verifying whether a condition exists (Exists rules)

Rules whose name ends with **Exists** check for the presence of a file, directory, registry key, or other item. If the KACE Agent locates the item on the device, the rule returns true, and the item appears in the device's Inventory Details as an Installed Program.

Use any of the following Exists rules:

- `DirectoryExists (path)`
- `FileExists (path)`
- `RegistryKeyExists (registryPath)`
- `EnvironmentalVariableExists (var)`
- `PlistValueExists (fullpath, entry)`
- `FilenameMatchingRegexExist (fullpath, regex)`

Example: Check for a directory (folder)

The following example tests whether the Windows directory exists on the device:

```
DirectoryExists(C:\WINDOWS\)
```

Example: Check for a file

NOTE: The following example verifies that the pad executable file exists on the device:

```
FileExists(C:\WINDOWS\notepad.exe)
```

Evaluating device settings (Equals rules)

Rules whose name ends with **Equals** compare the value set on the device to the value you specify in the rule. The rules return true if the values exactly match.

Rules that use arguments with set data types can only compare values of the same type.

Use any of the following Equals rules:

- `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)`

Example: Testing JAVA_HOME setting

To verify that the JAVA_HOME setting is C:\Program Files\Java\jdk1.6.0_02:

```
EnvironmentVariableEquals(JAVA_HOME, TEXT, C:\Program Files\Java\jdk1.6.0_02)
```

Example: Testing McAfee® Registry Entry setting

To check the setting use the same format as the date in the entry:

```
RegistryValueEquals(HKEY_LOCAL_MACHINE\Software\McAfee\AVEngine, AVDatDate, 2014/03/01)
```

Example: Detecting Windows 7 Service Pack 1

Windows 7 Service Pack 1 appears in *Add/Remove programs* for devices that were originally on Windows 7 then upgraded to SP1 only. The default application inventory for this item does not reflect devices that are already on SP1 because they were originally imaged at the SP1 level.

When using the appliance to deploy Windows 7 Service Pack 1, create the following Custom Inventory rule for a custom application:

```
RegistryValueEquals(HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\
CurrentVersion,CSDVersion,Service Pack 2)
```

You can then exclude devices with this item installed to prevent the appliance from trying to deploy the SP2 to devices that are already at that level (that is, Windows 7 devices that have been upgraded, as well as devices originally imaged with SP1).

Comparing device values (Greater Than and Less Than rules)

Functions whose names end with **GreaterThan** and **LessThan** compare values as listed in Table 24.

Use any of the following Greater Than and Less Than rules:

- `FileVersionGreaterThan (path, version)` and `FileVersionLessThan (path, version)`
- `ProductVersionGreaterThan (path, version)` and `ProductVersionLessThan (path, version)`
- `FileInfoGreaterThan (fullpath, attribute, type, value)` and `FileInfoLessThan (fullpath, attribute, type, value)`
- `RegistryValueGreaterThan (registryPath, valueName, value)` and `RegistryValueLessThan (registryPath, valueName, value)`
- `EnvironmentalVariableGreaterThan (var, type, value)` and `EnvironmentalVariableLessThan (var, type, value)`
- `PlistValueGreaterThan (fullpath, entry, type, value)` and `PlistValueLessThan (fullpath, entry, type, value)`
- `FilenameMatchingRegexGreaterThan (fullpath, regex, value)` and `FilenameMatchingRegexLessThan (fullpath, regex, value)`

Example: Testing whether the product version is higher

To verify that the product version is higher than a given number:

```
ProductVersionGreaterThan(C:\Program Files\Mozilla Firefox\firefox.exe, 78)
```

To verify that the production version is a given number or higher, enter the following:

```
ProductVersionEquals(C:\Program Files\Mozilla Firefox\firefox.exe, 78)
OR ProductVersionGreaterThan(C:\Program Files\Mozilla Firefox\firefox.exe,
 78)
```

Example: Testing for a product version range

To test whether the product version is within a range, combine less than and greater than rules:

```
ProductVersionGreaterThan(C:\Program Files\Mozilla Firefox\firefox.exe, 77)
 AND ProductVersionLessThan(C:\Program Files\Mozilla Firefox\firefox.exe, 79)
```

IMPORTANT: Do not enter rules on separate lines. Separate the rules by space only. Having rules on separate lines invalidates the compound rule.

Testing for multiple conditions

You can join rules using AND operators or OR operators to test for multiple conditions.

NOTE: Using both AND and OR operators in the same Custom Inventory rule is not supported. Set up separate applications.

Joining conditional rules produces the following results:

- AND operator: All the rules must return true in order for the results to return true and report the application as an Installed Program.
- OR operator: Only one rule must return true for the application to be reported as an Installed Program.

IMPORTANT: Do not enter rules on separate lines. Separate the rules by space only. Having rules on separate lines invalidates the compound rule.

Checking for multiple true conditions (AND)

Use the AND operator to join conditional rules in the Custom Inventory Field when you want the item to be reported as an Installed Program only if all the rules are true.

In the *Custom Inventory Field*, join rules using the following syntax:

```
Function
(arguments...
) AND Function
(arguments
) AND ...
```

Separate the conditional statements from the operator with spaces.

Example: Checking for a registry key and comparing values

To check for a registry key and a registry entry value on a Windows device use AND to combine the rules as follows:

```
RegistryKeyExists(registryPath
) AND RegistryValueEquals(registryPath, valueName, value)
```

Checking for one true condition (OR)

When you join rules using the `OR` operator, if any of the rules in the *Custom Inventory Field* are true, the application appears in the *Installed Program* list of the device.

In the *Custom Inventory Field*, join the rules using the following syntax:

```
Function
(arguments
) OR Function
(arguments
) OR ...
```

Separate the function statements and operator using a space.

Example: Checking for either registry value

To check that a registry entry is one value or another:

```
RegistryValueEquals(registryPath, valueName, value) OR
RegistryValueEquals(registryPath, valueName, value)
```

TIP: To specify a range use `RegistryValueGreaterThan` and `RegistryValueLessThan` rules joined by the `AND` operator.

Getting values from a device (Custom Inventory Field)

The rules that end with **ValueReturn** enable you to gather information from the device. You can use these rules to collect information that the KACE Agent normally does not collect.

The returned values are set with the custom application display name (Title). This appears on the *Device Detail* page under *Software* in *Installed Programs* and *Custom Inventory Fields*.

Use the *Custom Inventory Field* values to manage installations and to distribute software as well as reports, *View By* filtering, Smart Label search criteria, or any other process that can be performed with an automatically detected setting.

This section covers the following topics:

- Value Return rule reference
- Getting registry key values
- Getting command output
- Getting PLIST values
- Getting multiple values

Value Return rule reference

The following table shows all available value return rules that you can use to set a *Custom Inventory Field* :

Syntax	Win	RHEL	OS X	Description
`RegistryValueReturn (registryPath, valueName, type)`	X			Returns the value of a registry entry, and sets the datatype to the one you specified.
`EnvironmentalVariableReturn (var, type)` Specifying environment or user variables	X	X	X	Returns the value of an environment variable, and sets the datatype to the one you specified.
`FileInfoReturn (path, attribute, type)`	X	X	X	Returns the value of a file attribute, see valid types in Defining rule arguments.
`ShellCommandTextReturn (command)`	X	X	X	Returns the output of the command, and sets the datatype to TEXT.
`ShellCommandDateReturn (command)`	X	X	X	Returns the output of the command, and sets the datatype to DATE.
`ShellCommandNumberReturn (command)`	X	X	X	Returns the output of the command, and sets the datatype to NUMBER.
`PlistValueReturn (fullpath, entry, type)`			X	Returns the value of the PLIST key, and sets the datatype to TEXT, NUMBER, or DATE.

Getting File Information values

You can set the *Custom Inventory Field* to any of the Windows File Information attributes using the `FileInfoReturn` rule.

Example: Getting Mozilla Firefox version

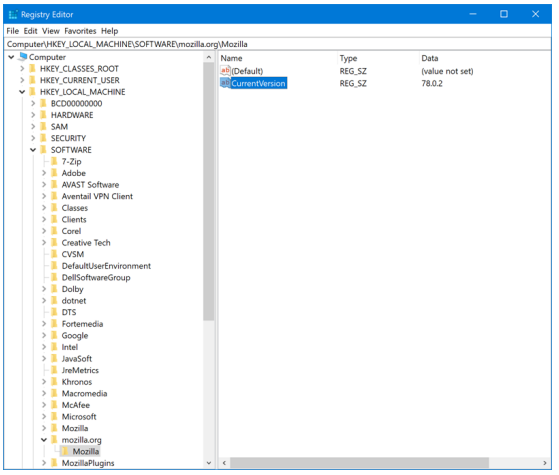
The following example sets the *Custom Inventory Field* for the Mozilla Firefox Product Version as a NUMBER:

In the *Custom Inventory Field*, enter the following:

```
FileInfoReturn(C:\Program Files\Mozilla Firefox\firefox.exe,CurrentVersion,TEXT)
```

Getting registry key values

You can set the *Custom Inventory Field* to a registry key using the `RegistryValueReturn` rule. Where the `registryPath` (on left) is the path to the entry, the `valueName` (on right) is the key you want to return.



Example: Getting the Mozilla FireFox CurrentVersion key

To set the CurrentVersion registry key as a *Custom Inventory Field*:

```
RegistryValueReturn (HKEY_LOCAL_MACHINE\SOFTWARE\Mozilla\Mozilla Firefox\CurrentVersion, TEXT
```

Getting command output

Command rules enable you to set the output of a command to a *Custom Inventory Field*. The command depends on the command interpreter and executable path on the device.

For example, on Windows devices you can write MS-DOS commands, but not Cygwin-style UNIX commands unless Cygwin is installed and available in the default path for all users.

Use any of the following rules to set the output of the command to a *Custom Inventory Field*:

- `ShellCommandTextReturn (command)`
- `ShellCommandDateReturn (command)`
- `ShellCommandNumberReturn (command)`

Example: Getting uptime on a Mac OS X

To set the uptime as a *Custom Inventory Field*:

```
ShellCommandTextReturn(/usr/bin/uptime | sed -e 's/.*load averages://' | awk '{print $1}')
```

Getting PLIST values

`PlistValueReturn` rules enable you to set a Property List (PList) key as a *Custom Inventory Field*.

Example: Getting the system locale

To distribute applications using Managed Installations based on the System-provided language, enter the following rule to get the device locale and then create a corresponding Smart Label that is applied to the device based on the language code reported by the KACE Agent in the *Custom Inventory Field*:

```
PlistValueReturn(~/Library/Preferences/GlobalPreferences.plist, AppleLocale, TEXT)
```

Getting multiple values

Join `ValueReturn` rules using either the AND or OR operator. The rule shows the application as an Installed Program, if any of the values are not empty.

The joined values are all set in the same *Custom Inventory Field* separated by the operator and therefore are technically considered for the purposes of Search Criteria, filters, reports, and other appliance processes as TEXT.

`ValueReturn` rules joined by the:

- AND operator: All the values are reported in the *Custom Inventory Field*.
- OR operator: All values are reported in the *Custom Inventory Field*.

In the Custom Inventory field, join rules using the following syntax:

`Function``(`**`arguments...`**`) AND` **`Function`**`(`**`arguments`**`) AND ...`

Separate the conditional statements from the operator with spaces. Do not join AND and OR operators in the same rule.

Matching filenames to regular expressions

Regular expressions match a character or the specified string to the filenames in the specified directory.

This section describes the regular expressions that match filenames in Conditional and Value Return rules using a regular expression.

NOTE: The KACE Agent only provides functions that compare filenames using regular expressions.

Understanding regular expressions

You can use regular expression syntax to match filenames.

TIP: For more information on writing regular expressions go to http://msdn.microsoft.com/en-us/library/az24scfc.aspx.

The following table provides an overview of the regular expression syntax used to match filenames:

Character	Description	Example Expression	Target Files	Files Matched
(any string)	Non-special characters match any filename that contains the string.	`abc`	abcFile.xls Example.jpg File.doc Myabc.txt MyFile.abc	abcFile.xls Myabc.txt MyFile.abc
.	Dot matches any single character. When entered alone it matches all files.	.	abcFile.xls Example.jpg File.doc Myabc.txt MyFile.abc	abcFile.xls Example.jpg File.doc Myabc.txt MyFile.abc
\	Backslash is used to escape a special character and for creating a back-reference. For more information, go to http://rexegg.com/regex-capture.html.	`.*\.txt$`	abcFile.xls Example.jpg File.doc Myabc.txt MyFile.abc	Myabc.txt

Character	Description	Example Expression	Target Files	Files Matched
^	Caret matches the characters you specify to the start of the filename.	`^k`	install.exe kinstaller.exe runkbot.bat	kinstaller.exe
|	Pipe separates a list of options to match.	`run|install`	install.exe kinstaller.exe runkbot.bat	install.exe kinstaller.exe runkbot.bat
$	Dollar matches the characters you specify to the end of the filename.	`bat$`	install.exe kinstaller.exe runkbot.bat	runkbot.bat
?	Question mark makes the preceding character optional in matches.	`\.log10?$`	a.log1 afile.txt3 app.log appconf.log11 mylog.log10	a.log1 mylog.log10
*	Asterisk matches the preceding character zero or more times.	`\.log1*$`	a.log1 afile.txt3 app.log appconf.log11 mylog.log10	a.log1 app.log appconf.log11
+	Plus matches the preceding character one or more times.	`ap+.*\.log`	a.log1 afile.txt3 app.log appconf.log11 mylog.log10	app.log appconf.log11
[ ]	Brackets enclose a character class and match any character within the brackets. Character class special character rules differ from normal regular expressions.	`[123]`	a.log1 afile.txt3 app.log appconf.log11 mylog.log10	a.log1 afile.txt3 appconf.log11 mylog.log10
()	Parentheses enclosing characters create a back reference and match the preceding	`(p)\1`	a.log1 afile.txt3 app.log appconf.log11	app.log appconf.log11

Character	Description	Example Expression	Target Files	Files Matched
	characters and/ or the enclosed characters. For more information, go to http://rexegg.com/regex-capture.html.		mylog.log10	
{n}	Curly brackets repeat the preceding character the number of specified times, where **n** is greater than or equal to 1.	`{p}\.log$`	a.log1 afile.txt3 app.log appconf.log11 mylog.log10	app.log

Regular Expression Rule Reference

The syntax of a regular expression rule varies slightly from the other File rules. The `fullpath` argument is a string that matches the absolute path to the file location, but does not include name of the file. The filename is specified as a separate argument using a regular expression.

The following table provides a list of rules that allow you to use regular expressions.

Syntax	Win	RHEL	OS X	Description
`FilenamesMatchingRegexExist (fullpath,regex)`	X	X	X	Returns true if any files in the specified directory match the filename you entered using a regular expression.
`FilenamesMatchingRegexGreaterThan (fullpath,regex,value)`	X	X	X	True if the number of files that match is more than the value.
`FilenamesMatchingRegexLessThan (fullpath,regex,value)`	X	X	X	True if the number of files that match is less than the value.
`FilenamesMatchingRegexEqual (fullpath,regex,value)`	X	X	X	True if the number of files that match is the same as the value.
`FilenamesMatchingRegexReturn (fullpath,regex,type)`	X	X	X	Sets the Custom Inventory Field to the matching filenames (includes path).

Defining rule arguments

You can define arguments in Custom Inventory rules to find paths, files, registry keys, registry entries, version information, environment variables, and other attributes.

For rule syntax and usage, see the tables in Checking for conditions (conditional rules), Getting values from a device (Custom Inventory Field), and Matching filenames to regular expressions.

Finding a path or file

`path` and `fullpath` are strings that specify the absolute path to a directory or file on the device. For example:

```
C:\Program Files\Mozilla Firefox\firefox.exe
```

The KACE Agent locates the directory or file and performs the specific test.

Finding a registry key and entry

`registryPath` is a string that specifies the absolute path in the registry to a registry key. For example:

```
HKEY_LOCAL_MACHINE/application/kace
```

Specifying a version

`version` is an integer (type is TEXT) that the KACE Agent compares to the version of the item being tested on the device.

For example, the `FileVersionGreaterThan` test returns 'true' if the value you specify is higher than the version number of the file or folder and otherwise returns 'false'.

To test a range, join a Less Than and Greater Than rule as follows:

```
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)
```

Specifying environment or user variables

`var` is a string that matches the actual name of the environment variable on the device.

For example, to test that the Program Files directory variable is correctly set:

```
EnvironmentVariableEquals(ProgramFiles, TEXT,
C:\Program Files)
```

Specifying a file attribute

`attribute` is a system property, a file or folder property, or a KACE Agent-assigned property on the device. The appliance provides operating system-dependent argument types.

Using Windows file attributes

You can use the `FileInfoGreaterThan`, `FileInfoLessThan`, and `FileInfoEquals` functions to test a file property on Windows in the following syntax:

```
FunctionName (fullpath, attribute, type, value)
```

The following table shows the attributes supported by Windows:

Attribute	Type	Description
AccessedDate	DATE	Last date and time the file was accessed.
Comments	TEXT	Additional information provided for diagnostic purposes.
CompanyName	TEXT	Name of the company that produced the file.
CreatedDate	DATE	When the file was created.
FileBuildPart	NUMBER	Third position of the File Version. For example: In version 1.2.3, 3=Build.

Attribute	Type	Description
FileDescription	TEXT	File Description of the Windows File Properties Detail page.
FileMajorPart	NUMBER	First position of the File Version. For example: In version 1.2.3, 1=Major.
FileMinorPart	NUMBER	Second position of the File Version. For example: In version 1.2.3, 2=Minor.
FileName	TEXT	Current name of the file. Also see FileExists.
FilePrivatePart	NUMBER	Fourth position of the File Version: For example: In version 1.2.3.4, 4=Private.
FileVersion	TEXT	Complete File Version shown on the file properties Detail page. Also see FileVersionEquals, FileVersionGreaterThan, and FileVersionLessThan.
InternalName	TEXT	Internal name of the file, if one exists, such as the component name. If the file has no internal name, it is equal to the original filename, without an extension.
Language	TEXT	Language code, displays corresponding name on the File Properties Detail page.
LegalCopyright	TEXT	Copyright notices that apply to the file.
LegalTrademarks	TEXT	Trademarks and registered trademarks that apply to the file.
ModifiedDate	DATE	Last day and time the file was modified.
OriginalFilename	TEXT	Provides the full name of the file when it was put or installed on the device.
PrivateBuild	TEXT	Information about the version of the file.
ProductBuildPart	NUMBER	Third position of the Product Version. For example: In version 1.2.3, 3=Build.
ProductMajorPart	NUMBER	First position of the Product Version. For example: In version 1.2.3, 1=Major.
ProductMinorPart	NUMBER	Second position of the Product Version. For example: In version 1.2.3, 2=Minor.
ProductName	TEXT	String that matches the Product Name of the Windows property.

Attribute	Type	Description
ProductPrivatePart	NUMBER	Fourth position of the Product Version. For example: In version 1.2.3.4, 4=Private.
ProductVersion	TEXT	The full production version. Also see ProductVersionEquals, ProductVersionGreaterThan, and ProductVersionLessThan.
SpecialBuild	TEXT	Additional information about the build.

Testing for Linux and Mac file attributes

On Linux and Mac devices you can use the following arguments to test file attributes:

Attribute	Type	Description
access_time	DATE	The last time the user or system accessed the file
block_size	NUMBER	The block size of the file
blocks	NUMBER	The number of blocks used by the file
creation_time	DATE	The time the file was created
device_number	NUMBER	The identification number of the device (disk) containing the file
group	TEXT	The group name of the file owner
inode	NUMBER	The inode number of the file
modification_time	DATE	The last time a change was made and saved
number_links	NUMBER	The number of hard links to the file
owner	TEXT	The username of the person who owns the file
size	NUMBER	The size of the file

Specifying the datatype

`type` identifies the type of data you are testing or returning.

The KACE Agent supports the following types:

- `TEXT` is a string. Only valid for exactly matching in conditional rules such as Equals. In ValueReturn rules, this sets the *Custom Inventory Field* type to string and therefore limits search criteria and filtering to matching operators.
- `NUMBER` is an integer. Valid in all conditional rules, this allows you to specify a whole number for comparison.
- `DATE` must be in the format of `MM/dd/yyyy HH:mm:ss`. For example:`09/28/2006 05:03:51`. Time is required. For example, in a comparison such as greater than, you must at least specify the time as 00:00:00.

Specifying values to test

`value` typically follows `type` except in a rule where the datatype is known, such as in a version rule. The value you specify must match the type. See Specifying the datatype.

Specifying the name of a registry entry (Windows only)

`valueName` is a string that matches the name of the registry entry you want to test. Used only in registry tests for Windows devices.

Specifying a PLIST key (Mac only)

`entry` is either NUMBER, TEXT, or DATE and matches a key in a PLIST file on a Mac OS X device. If the wanted key is contained in an array/dictionary within the PLIST file, it can be referenced by specifying the name/integer for the array/dictionary, using a delineating colon, and then the name/integer of the key (**dictionary**:**key**) in the entry argument.

Argument examples:

- A key, **Item 0**, within an array, **PackageGroups**, is referenced by using `PackageGroups:0` for the argument
- A key, **contentType**, within the dictionary, **Item 102**, is referenced by using `102:contentType` for the argument.

Using a regular expression

`regex` is a regular expressions that matches a filename in a Conditional or Value Return rule. See Matching filenames to regular expressions for more details.

Defining commands

The shell command functions allow you to specify the `command` you want to run on the device. The guidelines for writing rule arguments do not apply to commands. However, white space after the opening parenthesis, and immediately before the closing parenthesis, is stripped from the command.

Test Custom Inventory rules

To test Custom Inventory rules you can run a custom inventory command on a KACE Agent-managed device. This ability enables you to debug Custom Inventory rules without running the entire inventory process.

1. Open a command prompt on a device that has the KACE Agent installed.
2. Enter the following command: `kdeploy -custominventory`

   The Agent contacts the appliance and runs the Custom Inventory. Queries and return values are displayed.

Deploying packages to managed devices

You can deploy packages to managed devices to install software remotely using the appliance.

Distributing software and using Wake-on-LAN

You can distribute applications, updates, and files from the appliance to managed devices. In addition, you can use Wake-on-LAN to power on devices remotely.

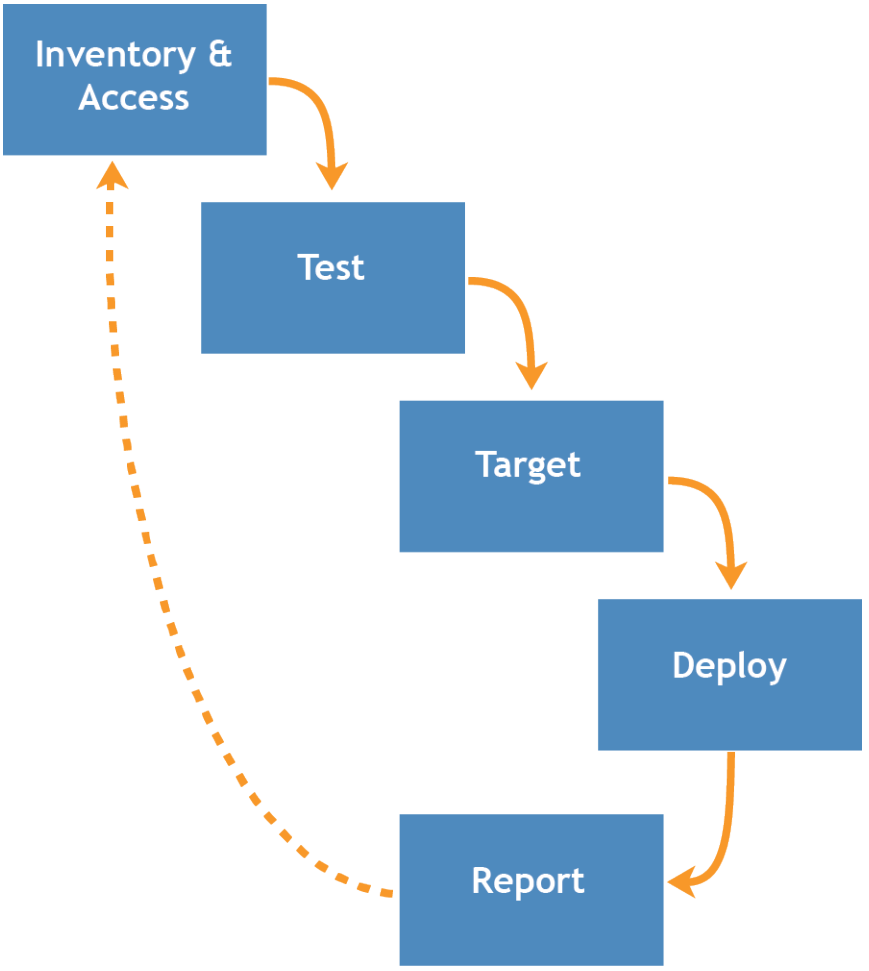
About software distribution

Software can be distributed from the appliance to Agent-managed Windows, Mac, and Linux devices.

TIP: Software distribution is available for items on the *Software* page and for Agent-managed devices only. It is not available for items on the *Software Catalog* page, Microsoft Application Virtualization (App-V) software, or Agentless devices.

The figure shows a high-level example of a software distribution process. You can modify this process as needed.

Figure 10. Software distribution procedure



About testing software distribution

Before distributing software to a large number of managed devices, test the deployment on a small but representative group of devices to verify that the package is compatible with target operating systems and other applications.

When the appliance distributes software to managed devices, it verifies that a package is designated for a particular device or operating system. However, the appliance cannot assess the software's compatibility with other software on the device. As a result, you should develop a process for testing all deployments.

For example, you could create a test group by applying a label to devices used for testing. Then deploy the required application to the test group using the label before you go deploy to the larger group of devices. This practice helps you to verify the compatibility of the application with the operating system and other applications in your test group. For more information about labeling devices, see Add or edit manual labels.

This section focuses primarily on the test, target, and deploy portions of the process. For more information about managing inventory, see Managing applications on the Software page.

Tracking changes to distribution settings

If History subscriptions are configured to retain information, you can view the details of the changes made to settings, assets, and objects.

This information includes the date the change was made and the user who made the change, which can be useful during troubleshooting. See About history settings.

Types of distribution packages

Packages can be distributed to managed devices as Managed Installations, File Synchronizations, User Console packages, and MSI installers.

- **Managed Installations**: Installation packages that are configured to run silently or with user interaction. Managed Installations include installation, uninstallation, and command-line parameters. See Using Managed Installations.
- **File Synchronizations**: A method of distributing files to managed devices. Unlike Managed Installations, however, File Synchronizations do not install files; they simply distribute files. See Create and use File Synchronization.
- **User Console packages**: Installation packages that contain printer drivers and other applications distributed through the User Console. See About Service Desk.
- **MSI Installer template**: A utility for creating policies and setting basic command line arguments for running Windows MSI-based installers. See .

Attaching digital assets to applications and selecting supported operating systems

To distribute applications to managed devices using Managed Installations or **User Console** downloads, you need to attach the appropriate digital assets to applications. Digital assets are the files required for deployment, such as installers. In addition, you need to select the supported operating systems for the application. You perform these tasks on the *Software* detail page.

This rule applies even if:

- You want to send a command, rather than an installation or a digital file, to devices.
- You are redirecting the KACE Agents installed on managed devices to retrieve the digital asset, such as EXE or MSI files, from an alternate download location.

See Attach digital assets to applications and select supported operating systems.

Distributing packages from the appliance

Packages distributed from the appliance are deployed to managed devices only if the inventory item is designated to run on the device's operating system.

For example, if the inventory item is designated for Windows 7 only, the inventory item is not deployed to devices running Windows 8.

Also, packages are deployed only to devices that meet label requirements. For example, if the package is set to deploy to a label named *Office A*, the package does not deploy to devices that are not labeled *Office A*. When the appliance creates an application inventory item, it only records the operating systems on which the item was installed in the inventory detail record.

To deploy Managed Installations, you must select an execution option and a deployment window. See Using Managed Installations.

Distributing packages from alternate download locations and Replication Shares

You can distribute packages from alternate download locations and Replication Shares.

This distribution is useful when:

- You have remote sites with restricted bandwidth that might have trouble accessing the appliance.
- You want to avoid storing large distribution packages on the appliance.

About alternate download locations

Alternate download locations are managed devices that can host the files required to distribute software from the appliance to other managed devices.

An alternate download location can be any network location that has all the files required to install a particular application. You can distribute packages from alternate download locations including a UNC address or DFS source. The CIFS and SMB protocols, Samba servers, and file server appliances are supported. You specify the location when you create a Managed Installation.

See Attach digital assets to applications and select supported operating systems.

About Replication Shares

Replication Shares are devices that keep copies of files for distribution. Replication shares are especially useful if your managed devices are deployed across multiple geographic locations.

For example, using a Replication Share, a device in New York could download files from another device at the same office, rather than downloading those files from an appliance in Los Angeles. A Replication Share is a full replication of all digital assets and is managed automatically by the appliance. Whenever a Replication Share is specified for a label, devices in that label go to the Replication Share to get files.

The KACE Agent always looks to the appliance for distribution files if no Replication Shares are specified for any label applied to a device. If the appliance uses multiple Replication Shares, the agent makes a random selection.

See Using Replication Shares.

Distributing applications to Mac OS X devices

The appliance provides various methods for distributing applications, updates, and files to Mac OS X devices.

About installers and plain packages

On Mac OS X, there is a universal installer with the usual PKG file extension. You cannot upload a PKG file directly, as these files consist of low-level directories, and web browsers cannot handle uploading entire directories.

Plain (APP) packages, which can be installed by dragging them to the *Applications* folder on the Mac, do not require installers. However, APP packages must be archived because they consist of low-level directories, similar to the installer packages.

You can archive installers along with plain applications. The appliance runs installers first and then copies applications into the *Applications* folder.

Supported package deployments on Mac OS X

The supported package deployments are PKG, APP, DMG, ZIP, TGZ, and TAR.GZ.

If you package the file as a disk image, the appliance mounts and unmounts it quietly. This section provides examples for each type of deployment. For each of these examples, you must have already uploaded the file to the appliance prior to creating the Managed Installation package. Quest recommends that you install the application on a test device. When the KACE Agent connects to the appliance, the appliance creates an inventory item and a Managed Installation package for the application.

Using Managed Installations

Managed Installations (MI) are the primary mechanism for deploying applications to, or removing applications from managed devices. Each Managed Installation describes a specific application title and version to be installed or removed, including installation commands, installation files, and target devices (identified by label).

Managed Installations always take place at the same time that managed devices upload inventory data to the appliance. In this way, the appliance confirms that the installation is actually needed before it performs the installation. Installation packages can be configured to run silently or with user interaction. Managed Installations can include installation, uninstallation, and command-line parameters.

Managed Installations requires an active network connections to the appliance. If the connection becomes disrupted during an installation, the process continues when the agent reconnects.

On Windows the most common Managed Installation package deployments are MSI, EXE, and ZIP files.

Supported package deployments for Linux devices include RPM, ZIP, BIN, TGZ, and TAR.GZ files.

Adding applications to inventory

Before you create a Managed Installation, the files you want to deploy must be associated with an application on the *Software* page. If the application is not yet on the *Software* page, you can add it as needed.

To add an application that is not on the *Software* page, you can:

- Install the application on a managed device, then request an inventory update from the device. See Forcing inventory updates.
- Manually add the application to inventory. See Add applications to Software page inventory manually.

> **CAUTION: If the display name of the application inventory item does not exactly match the name that the application registers in *Add/Remove* programs, the appliance might attempt to deploy a package repeatedly even though it is already there. To solve this problem, add the application to the *Software* inventory list, then use the registered application name in the Managed Installation.**

About creating Managed Installations

You can create Managed Installations for items that appear on the *Software* page.

See:

- Create Managed Installations for Windows devices
- Create Managed Installations for macOS X devices
- Create Managed Installations for RPM files
- Create Managed Installations for TAR.GZ files
- Create Managed Installations for ZIP files

To create packages with special settings, such as parameters, labels, or deployment definitions, you can create multiple distribution packages for a single inventory item. However, the Managed Installation cannot be verified against more than one inventory item because it checks for the existence of only one inventory item.

For each of these examples, you must have already uploaded the file to the appliance before creating the Managed Installation package. Quest recommends installing the application on a test device, waiting for the KACE Agent to connect to the appliance and create an inventory item for the application, and then creating the Managed Installation package from the application.

NOTE: Agent deployment is discussed in Provisioning the KACE Agent. For information about updating an existing version of the Agent, see Upload Agent updates manually.

About installation parameters

You can add installation parameters to the package definitions used to distribute and install applications on managed devices.

Packaged definitions can contain MSI, EXE, ZIP, and other file types for application deployment. If an administrator installs the file on a local device, either by running a single file, BAT file, or VBScript, the package can be installed remotely by the appliance.

To simplify the distribution and installation process, the package definition can also contain parameters that are passed to the installer at run time on the local device. For example, you could use parameters as custom installation settings to bypass an automatic restart.

Identify parameters that are supported by installer files

You can display the parameters that are supported by installer files from the Windows command line.

1. Open an command prompt.
2. Go to the directory that contains the target installer.

   For example: `c:\...\adobe.exe`
3. Type **filename** `/?`

   For example: `adobe.exe /?`

   If that package supports parameters, they are displayed. For example: `/quiet, /norestart`.
4. Use the parameter definitions identified to update your package definition.

For more information, see the application vendor's documentation.

Create Managed Installations for Windows devices

You can create Managed Installations to deploy software to Agent-managed Windows devices.

When you create Managed Installations for the Windows platform, you can specify whether you want to display messages to users before and after the installation. You can also indicate whether to deploy the package when the user is logged in or not and limit deployment to a specific label.

For specific details on creating a Managed Installation for an MSI, EXE, or a ZIP file, see Examples of common deployments on Windows.

To distribute applications to managed devices, you must attach the digital assets, which are the files required for installation, to applications. In addition, you must select the supported operating systems for applications. See Attach digital assets to applications and select supported operating systems.

1. Go to the *Managed Installation Detail* page:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Distribution**, then click **Managed Installations**.
   c. Select **Choose Action** > **New**.
2. In the *Configure* tab, provide the following information:

Option	Description
Name	A name that identifies the Managed Installation. This name appears on the *Managed Installations* page.
Execution	The package deployment setting. Options include: • **Disabled**: Do not deploy the package. • **Anytime**: Deploy the package at the next opportunity, such as the next time the KACE Agent reports inventory information to the appliance. • **At bootup**: Deploy the package the next time the device starts up. **NOTE:** If a device has an Active Directory or Group Policy Object setting that displays a message that the user must acknowledge before logging on, packages are not deployed and scripts do not run until the message is acknowledged. • **After login**: Deploy the package after the user logs in but before the desktop loads. • **With user logged in**: Deploy the package while the user is logged on. • **With user logged off**: Deploy the package only when the device is running and the user is logged off.
Inventory	Indicate if you want to deploy the software title from **Cataloged Software** or all **Software** by selecting one of these options. • To search for a specific title, begin typing in the *Software* or *Cataloged Software* field. **NOTE: Reclaiming unused software licenses only.** The name of the software that you want to uninstall appears in this field by default. For more information, see Reclaim unused software licenses. • If you want to display only the software that has one or more associated files, select **Only Display Software With an Associated File**.
Associated File	A Software and Cataloged Software title can have one or more files attached to them, as needed. Indicate if you want to select a specific file associated with the selected software title. • **Choose associated file**: Select this option if you want to associate a file. You can select a file in the list. If you know the file name, start typing it in the box, and select it from the available entries in the list. • **Do not associate file**: Select this option if you do not want to associate a file.
Alternate Location	Specify a location from which files can be downloaded for a specific Managed Installation. **Path**: Enter the location where the KACE Agent can retrieve digital installation files. **Checksum**: Enter an alternate checksum (MD5) that matches the MD5 checksum on the remote file share. If no checksum is entered, the digital asset on the file share must match the digital asset associated with the deployment package on the appliance. Also, the target path must include the complete filename (for example, `\\fileserver_one\software\adobe.exe`). You can create the checksum using any tool, including KDeploy.exe, which is installed with the KACE Agent. **To create the checksum using KDeploy.exe:**

Option	Description
	1. On a device with the KACE Agent installed, open a command prompt or terminal window. 2. Go to the Quest KACE installation directory. For example: Windows 32-bit devices: `C:\Program Files\Quest\KACE` Windows 64-bit devices: `C:\Program Files (x86)\Quest\KACE` Mac OS X devices: `/Library/Application Support/Quest/KACE/bin` 3. Enter the following command: KDeploy -hash=**filename** Where **filename** is the UNC path to the file. If the path contains spaces, enclose the entire path in double quotation marks. 4. Press **Ctrl C** or **Command C** to copy the MD5 checksum. You can then paste it into other files, such as Notepad. **Credential**: The details of the service account required to connect to the device and run commands. Select existing credentials from the drop-down list, or select **Add credential** to add credentials not already listed. See Add and edit User/Password credentials. **NOTE:** If the target device is part of a replication label, the appliance does not fetch applications from the alternate download location. You can edit an existing label or create a label to specify the alternate location globally. Because that label cannot be specific to any Managed Installation, you cannot specify an alternate checksum that matches the checksum on the remote file share. See Distributing packages from alternate download locations and Replication Shares and Add or edit manual labels.
Default Installation	Use the default commands during installation. **Additional Parameters**: Specify the installation behavior as follows: • The maximum field length is 256 characters. If a path exceeds this limit, use the command line to point to a BAT file that contains the path and the command. • If a file path includes spaces, enclose the complete path in double quotation marks. For example: `"\\kace_share\demo files\share these files\setup.bat"`
Override Default Installation	Specify the full command-line parameters. See the MSI Command Line documentation for available runtime options. • **Uninstall**: Uninstall the application from the command line. • **Run Command Only (do not download file)**: Run the command line only. • **Don't Prepend msiexec.exe**: Prevent the appliance from adding `msiexec.exe` to the beginning of the file.
Delete Downloaded Files	Delete the files when the deployment is complete.

3. Specify deployment settings in the *Deploy* tab :

Option	Description
All Devices	Deploy to all devices. Clear the check box to limit the deployment to specific labels or devices.

Option	Description
Restrict to Labels	Limit deployment to devices that belong to specified labels. To select labels, click **Edit**, drag labels to the *Limit Deployment to* window, then click **Save**. If you select a label that has a Replication Share or an alternate download location, the appliance copies digital assets from that Replication Share or alternate download location instead of downloading them directly from the appliance. **NOTE:** The appliance uses a Replication Share before it uses the KACE Alt Location.
Devices	Limit deployment to specific devices. In the drop-down list, select the devices to which you want to deploy the application. To filter the list, type a few characters in the *Devices* field. The number next to the field indicates the number of devices available. **NOTE: Reclaiming unused software licenses only.** Any devices from which you want to remove the applicable software are listed. You can edit the list of devices, as needed. To remove the software from all devices, simply select , as described above. For more information, see Reclaim unused software licenses.

4. Specify user notification settings in the Notify tab

Option	Description
Alert user before run	Display a message on managed devices before installation. When you select this option, the following fields appear: • **Message**: The message that appears on managed devices before installation begins. It starts with snooze options that allow the user to run the managed install at a later time. • **Timeout**: The length of time, in minutes, during which the message appears. • **Action**: The action that takes place at the end of the **Initial Message Timeout** period. Options include **Install later** or **Install now**. Select **Install now** to install the application immediately, or select **Install later** to postpone the installation until a user responds. Install later is useful when you want to notify users of an installation or reboot before it occurs.
Initial Message	Display a message on managed devices before installation. When you select this option, the following fields appear: • **Message**: The message that appears on managed devices before installation begins. • **Timeout**: The length of time, in minutes, during which the message appears. • **Action**: The action that takes place at the end of the **Initial Message Timeout** period. Options include **Install later** or **Install now**. Select **Install now** to install the application immediately, or select **Install later** to postpone the installation until a user responds. Install later is useful when you want to notify users of an installation or reboot before it occurs.
Completion Message	Display a message on managed devices after the installation is complete. When you select this option, the following fields appear: • **Message**: The message that appears on managed devices when the installation is complete. • **Timeout**: The length of time, in minutes, during which the message appears.

5. Select the options in the Schedule tab:

Option	Description
Deployment Window Start End	The time, in 24-hour clock format, for package deployment to start and end. The *Deployment Window* time affects all *Action* options. Also, the run intervals defined in the appliance *Settings* interact with or override the deployment window of specific packages.
Order	The order in which to install or uninstall applications. The lowest value is deployed first. If an install action and an uninstall action both have the same order value, the uninstall action is performed first. **NOTE:** Managed Installations are always deployed in order, regardless of whether their specified software packages come from the Software Catalog or the Software list. Managed Installations with a lower deploy order always prevent other Managed Installations from running until they are successfully installed or exceed the specified retry times.
Maximum Attempts	The maximum number of attempts, between 0 and 99, to indicate the number of times the appliance tries to install the package. If you specify 0, the appliance attempts to install the package indefinitely.

6. Click **Save**.

Examples of common deployments on Windows

The most common Managed Installation package deployments are MSI, EXE, and ZIP files.

Standard MSI example

Using MSI files is an easy, self-contained way to deploy software to Windows devices. If your MSI file requires no special transformation or customization, the deployment is straightforward.

MSI files require a `/i` switch when using other switches with an install.

The appliance parameter line does not require the filename or `msiexec` syntax. Only the `/*` input is required:

`/qn /I` (Correct)

`msiexec /I /qn` (Incorrect)

NOTE: To use parameters with MSI files, all your target devices must have the same version of Windows Installer (available from Microsoft). Some switches might not be active on older versions. The most up-to-date version of Windows Installer can be distributed to devices from the appliance.

TIP: If you are using Windows Installer 3.0 or higher, you can identify the supported parameters by selecting the **Run** program available from the *Start* menu. Enter msiexec in the pop-up window. A window that shows the supported parameters list appears.

Standard EXE example

EXE files are similar to MSI files with one exception.

EXE files differ from MSI files as follows: /I is not required in the *Run Parameters* line when using an EXE file.

When using an executable file, it is often helpful to identify switch parameters for a quiet or silent installation. To switch parameters, specify /? in the *Run Parameters* field.

Create Managed Installations for ZIP files

Deploying software using a ZIP file is a convenient way to package software when multiple files are required to deploy a title.

For example, a software title might require a `setup.exe` file, configuration files, and data files. If you have a CD-ROM that contains a group of files required to install a particular application, you can package them together in a ZIP file and upload them to the appliance for deployment.

NOTE: The KACE Agent automatically runs deployment packages with MSI and EXE extensions.

NOTE: In addition, you can create a ZIP archive that contains many files and direct the appliance to unpack the archive and run a specific file. Place the name of the file that you want to run in the command (executable) field within the deployment package (for example, `runthis.exe`).

To distribute applications to managed devices, you must attach the digital assets, which are the files required for installation, to applications. In addition, you must select the supported operating systems for applications. See Attach digital assets to applications and select supported operating systems.

1. Browse to the location that contains the necessary installation files, select all the files and create a ZIP file using a utility such as WinZIP®.
2. Log in to the appliance Administrator Console.
3. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
4. Create an inventory item for the target deployment.

   You can do this manually from the *Inventory* > *Software* page or by installing the package on a device that regularly connects to the appliance. See About the Software page.
5. Associate the ZIP file with the inventory item and upload it to the appliance:
   a. On the left navigation bar, click **Distribution**, then click **Managed Installations**.
   b. Select **Choose Action** > **New**.
   c. Select the application title that the ZIP file is associated with from the *Software* drop-down list. To see all application titles, clear the check box **Only display records with an associated file**.
6. In the *Additional Parameters* field, specify the complete command with arguments.

   For example: `setup.exe /qn`
7. Specify additional settings as needed.

   See Create Managed Installations for Windows devices.
8. Click **Save**.

Create Managed Installations for RPM files

You can create Managed Installations to deploy software on Linux-based devices using RPM files.

To distribute applications to managed devices, you must attach the digital assets, which are the files required for installation, to applications. In addition, you must select the supported operating systems for applications. See Attach digital assets to applications and select supported operating systems.

1. Go to the *Managed Installation Detail* page:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Distribution**, then click **Managed Installations**.

c. Select **Choose Action** > **New**.

2. In the *Software* drop-down list, select a software title. To search for a title, begin typing in the *Software* field.

   By default, the KACE Agent attempts to install the RPM file using the following command. In general, this command is sufficient to install a new package or update an existing one to a new version:

   `rpm -U` **packagename.rpm**

   If you select a ZIP, TGZ, or TAR.GZ file, the content is unpacked, and the root directory is searched for all RPM files. The installation command runs against each of these files. The appliance finds all RPM files at the top level of an archive automatically, so you can install more than one package at a time. You can also create an archive containing a shell script and then specify that script name as the full command. The appliance runs that command if it is found; otherwise, the appliance logs an error.

   Default parameters are used unless you specify parameters in the *Run Parameters* field.

   You can specify wildcards in the filenames you use. If the filename contains spaces, enclose it in single or double quotation marks. The files are extracted into a directory in `/tmp` and it becomes the current working directory of the command.

   NOTE: On Red Hat Linux, if you only want to run your script, you do not need to include any other files in your archive.

   If the path environment variable of your root account does not include the current working directory, and you want to run a shell script or other executable that you have included inside an archive, specify the relative path to the executable in the *Full Command Line* field. The command runs inside a directory alongside the files that have been extracted.

   For example, to run a shell script called `installThis.sh`, package it alongside an RPM file, and then enter the command: ./installThis.sh in the *Installation Command* field. If you archive it inside another directory, the *Installation Command* field is:

   `./dir/filename.sh`

   Both these examples, as well as some other appliance functions, assume that `sh` is in the root's path. If you are using another scripting language, you might need to specify the full path to the command processor you want to run in the installation command, such as:

   `/bin/sh ./`**filename**`.sh`

   Include appropriate arguments for an unattended, batch script.

   If you select the uninstall check box in the MI detail, the KACE Agent runs the following command on either your standalone RPM file or each RPM file it finds in the archive, removing the packages automatically:

   `//usr/sbin/rpm -e` **packagename**`.rpm`

   The package is removed only if the archive or package has been downloaded to the device. If you select the *Uninstall Using Full Command Line* check box, specify a full command line in the *Installation Command* field to ensure the correct removal command runs on the correct package. Because no package is downloaded in this case, specify the path in the installation database where the package receipt is stored.

3. If your package requires additional options, provide the following information:

Option	Description
Name	A name that identifies the Managed Installation. This name appears on the *Managed Installations* page.
Execution	Select the most appropriate time for this package to be deployed. For the Linux platform, the options are **Anytime (next available)** and **Disabled**.

Option	Description
Inventory	Indicate if you want to deploy the software title from **Cataloged Software** or all **Software** by selecting one of these options. • To search for a specific title, begin typing in the *Software* or *Cataloged Software* field. **NOTE: Reclaiming unused software licenses only.** The name of the software that you want to uninstall appears in this field by default. For more information, see Reclaim unused software licenses. • If you want to display only the software that has one or more associated files, select **Only Display Software With an Associated File**.
Associated File	A Software and Cataloged Software title can have one or more files attached to them, as needed. Indicate if you want to select a specific file associated with the selected software title. • **Choose associated file**: Select this option if you want to associate a file. You can select a file in the list. If you know the file name, start typing it in the box, and select it from the available entries in the list. • **Do not associate file**: Select this option if you do not want to associate a file.
Alternate Location	Specify a location from which files can be downloaded for a specific Managed Installation. **Path**: Enter the location where the KACE Agent can retrieve digital installation files. **Checksum**: Enter an alternate checksum (MD5) that matches the MD5 checksum on the remote file share. If no checksum is entered, the digital asset on the file share must match the digital asset associated with the deployment package on the appliance. Also, the target path must include the complete filename (for example, `\\fileserver_one\software\adobe.exe`). You can create the checksum using any tool, including KDeploy.exe, which is installed with the KACE Agent. **To create the checksum using KDeploy.exe:** 1. On a device with the KACE Agent installed, open a command prompt or terminal window. 2. Go to the Quest KACE installation directory. For example: Windows 32-bit devices: `C:\Program Files\Quest\KACE` Windows 64-bit devices: `C:\Program Files (x86)\Quest\KACE` Mac OS X devices: `/Library/Application Support/Quest/KACE/bin` 3. Enter the following command: KDeploy -hash=**filename** Where **filename** is the UNC path to the file. If the path contains spaces, enclose the entire path in double quotation marks. 4. Press **Ctrl C** or **Command C** to copy the MD5 checksum. You can then paste it into other files, such as Notepad. **Credential**: The details of the service account required to connect to the device and run commands. Select existing credentials from the drop-down list, or select **Add credential** to add credentials not already listed. See Add and edit User/Password credentials. **NOTE:** If the target device is part of a replication label, the appliance does not fetch applications from the alternate download location. You can edit an existing label or create a label to specify the alternate location globally. Because that label cannot be specific to any Managed Installation, you cannot specify an alternate checksum that matches the checksum on the remote file share.

Option	Description
	See Distributing packages from alternate download locations and Replication Shares and Add or edit manual labels.
Installation Command	Installation command options.
Default Installation	Select this option if you have an RPM file and you want the appliance to run the default installation command. Linux devices use: rpm [-U | Run Parameters] "**packagename**.tgz" **Additional Parameters**: (Optional) If you select **Use Default**, specify the parameters to use. Additional parameters are not required if you have an RPM file. Enter a value to override (Default `-U` default). For example, if you set **Run Parameters** to: -ivh --replacepkgs, then the command that runs on the device is: `rpm -ivh -replacepkgs package.rpm`
Override Default Installation	Select this option to specify the complete command line here. If you are using an archive file, this command runs against all of the RPM files it finds.
Uninstall	Remove the package from the device using the command line. If you specified a command in the *Full Command Line* field, the command runs. Otherwise, the KACE Agent attempts to run the command, which is generally expected to remove the package.
Run Command Only (do not download file)	Run the command only. This does not download the actual digital asset.
Delete Downloaded Files	Delete the files when the deployment is complete.

4. Specify deployment settings in the Deploy tab:

Option	Description
All Devices	Deploy to all devices. Clear the check box to limit the deployment to specific labels or devices.
Restrict to Labels	Limit deployment to devices that belong to specified labels. To select labels, click **Edit**, drag labels to the *Limit Deployment to* window, then click **Save**. If you select a label that has a Replication Share or an alternate download location, the appliance copies digital assets from that Replication Share or alternate download location instead of downloading them directly from the appliance. **NOTE:** The appliance uses a Replication Share before it uses the KACE Alt Location.
Devices	Limit deployment to specific devices. In the drop-down list, select the devices to which you want to deploy the application. To filter the list, type a few characters in the *Devices* field. The number next to the field indicates the number of devices available.

Option	Description
	NOTE: Reclaiming unused software licenses only. Any devices from which you want to remove the applicable software are listed. You can edit the list of devices, as needed. To remove the software from all devices, simply select , as described above. For more information, see Reclaim unused software licenses.

5. Specify the user notification settings in the Notify tab:

Option	Description
Alert user before run	Display a message on managed devices before installation. When you select this option, the following fields appear: • **Message**: The message that appears on managed devices before installation begins. It starts with snooze options that allow the user to run the managed install at a later time. • **Timeout**: The length of time, in minutes, during which the message appears. • **Action**: The action that takes place at the end of the **Initial Message Timeout** period. Options include **Install later** or **Install now**. Select **Install now** to install the application immediately, or select **Install later** to postpone the installation until a user responds. Install later is useful when you want to notify users of an installation or reboot before it occurs.
Initial Message	Display a message on managed devices before installation. When you select this option, the following fields appear: • **Message**: The message that appears on managed devices before installation begins. • **Timeout**: The length of time, in minutes, during which the message appears. • **Action**: The action that takes place at the end of the **Initial Message Timeout** period. Options include **Install later** or **Install now**. Select **Install now** to install the application immediately, or select **Install later** to postpone the installation until a user responds. Install later is useful when you want to notify users of an installation or reboot before it occurs.
Completion Message	Display a message on managed devices after the installation is complete. When you select this option, the following fields appear: • **Message**: The message that appears on managed devices when the installation is complete. • **Timeout**: The length of time, in minutes, during which the message appears.

6. Select appropriate options in the Schedule tab:

Option	Description
Deployment Window Start End	The time, in 24-hour clock format, for package deployment to start and end. The *Deployment Window* time affects all *Action* options. Also, the run intervals defined in the appliance *Settings* interact with or override the deployment window of specific packages.
Order	The order in which to install or uninstall applications. The lowest value is deployed first. If an install action and an uninstall action both have the same order value, the uninstall action is performed first.

Option	Description
	NOTE: Managed Installations are always deployed in order, regardless of whether their specified software packages come from the Software Catalog or the Software list. Managed Installations with a lower deploy order always prevent other Managed Installations from running until they are successfully installed or exceed the specified retry times.
Maximum Attempts	The maximum number of attempts, between 0 and 99, to indicate the number of times the appliance tries to install the package. If you specify 0, the appliance attempts to install the package indefinitely.

7. Click **Save**.

Create Managed Installations for TAR.GZ files

Deploying software using a TAR.GZ file is a convenient way to package software when more than one file is required to deploy a particular software title.

For example, some applications require several files, such as RPM, configuration, and data files, for deployment. You can package these files together in a TAR.GZ file, upload them to your appliance, and create Managed Installations that use the TAR.GZ files.

To distribute applications to managed devices, you must attach the digital assets, which are the files required for installation, to applications. In addition, you must select the supported operating systems for applications. See Attach digital assets to applications and select supported operating systems.

1. Use the following two commands to create a TAR.GZ file:
   a. `tar -cvf` **filename**`.tar` **packagename**`.rpm`
   b. `gzip` **filename**`.tar`
   This creates **filename**`.tar.gz`
2. Log in to the appliance Administrator Console.
3. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
4. Create an inventory item for the target deployment.

   You can do this manually from the *Inventory* > *Software* page, or by installing the package on a managed device that regularly connects to the appliance. See About the Software page.
5. Associate the TAR.GZ file with the inventory item, and upload it to the appliance:
   a. On the left navigation bar, click **Distribution**, then click **Managed Installations**.
   b. Select **Choose Action** > **New**.
   c. Select the application title with which the TAR.GZ file is associated from the *Software* drop-down list.

      During installation, the file is uncompressed and the installation command runs against each of the RPM packages.

      If no *Additional Parameters* are provided, `-U` is used.

      You do not need to specify a full command line. The appliance runs the installation command by itself. The Linux device tries to install using:

      `rpm [-U | Run Parameters] "`**packagename**`.tgz"`
   d. **Optional**: If you have many files, create a ZIP archive that contains them, then direct the appliance to unpack the archive and run a specific file.

      To do this, place the name of the file that you want to run in the command (executable) field within the deployment package (for example, runthis.exe). Provide additional package details. See Using Managed Installations.

e. Click **Save**.

The KACE Agent automatically runs deployment packages with RPM extensions.

Create Managed Installations for macOS X devices

You can create Managed Installations for macOS X devices as needed.

To distribute applications to managed devices, you must attach the digital assets, which are the files required for installation, to the application. In addition, you must select the supported operating systems for the application. See Attach digital assets to applications and select supported operating systems.

1. Go to the *Managed Installation Detail* page:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Distribution**, then click **Managed Installations**.
   c. Select **Choose Action** > **New**.
2. Select the application in the *Software* drop-down list.

   By default, the KACE Agent attempts to install the PKG file using the following command:

   ```
   installer -pkg packagename.pkg -target / [Run Parameters]
   ```

   If you have selected a DMG, ZIP, or TGZ, the contents are unpacked and the root directory is searched for all PKG files. The installation command runs against each of these PKG files and processes them in alphabetical order.

   Next, the appliance searches for all plain applications (APP) on the top level of the archive and copies them to the *Applications* folder using the following command:

   ```
   ditto -rscs Application.app /Applications/Application.app
   ```

   To run a script or change any of these command lines, you can specify the appropriate script invocation as the Full Command Line. You can specify wildcards in the filenames you use. Enclose the filename in single or double quotation marks if it contains spaces. The files are extracted into a directory in `/tmp`, and that becomes the current working directory of the command.

   TIP: If you only want to run your script on Mac OS X, you do not need to include any other files in your archive.

3. If the package requires additional options, provide the following information:

Option	Description
Name	A name that identifies the Managed Installation. This name appears on the *Managed Installations* page.
Execution	The package deployment setting. Options include: • **Disabled**: Do not deploy the package. • **Anytime**: Deploy the package at the next opportunity, such as the next time the KACE Agent reports inventory information to the appliance. • **At bootup**: Deploy the package the next time the device starts up.

Option	Description
	NOTE: If a device has an Active Directory or Group Policy Object setting that displays a message that the user must acknowledge before logging on, packages are not deployed and scripts do not run until the message is acknowledged. • **After login**: Deploy the package after the user logs in but before the desktop loads. • **With user logged in**: Deploy the package while the user is logged on. • **With user logged off**: Deploy the package only when the device is running and the user is logged off.
Inventory	Indicate if you want to deploy the software title from **Cataloged Software** or all **Software** by selecting one of these options. • To search for a specific title, begin typing in the *Software* or *Cataloged Software* field. **NOTE: Reclaiming unused software licenses only.** The name of the software that you want to uninstall appears in this field by default. For more information, see Reclaim unused software licenses. • If you want to display only the software that has one or more associated files, select **Only Display Software With an Associated File**.
Associated File	A Software and Cataloged Software title can have one or more files attached to them, as needed. Indicate if you want to select a specific file associated with the selected software title. • **Choose associated file**: Select this option if you want to associate a file. You can select a file in the list. If you know the file name, start typing it in the box, and select it from the available entries in the list. • **Do not associate file**: Select this option if you do not want to associate a file.
Alternate Location	Specify a location from which files can be downloaded for a specific Managed Installation. **Path**: Enter the location where the KACE Agent can retrieve digital installation files. **Checksum**: Enter an alternate checksum (MD5) that matches the MD5 checksum on the remote file share. If no checksum is entered, the digital asset on the file share must match the digital asset associated with the deployment package on the appliance. Also, the target path must include the complete filename (for example, `\\fileserver_one\software\adobe.exe`). You can create the checksum using any tool, including KDeploy.exe, which is installed with the KACE Agent. **To create the checksum using KDeploy.exe:** 1. On a device with the KACE Agent installed, open a command prompt or terminal window. 2. Go to the Quest KACE installation directory. For example: Windows 32-bit devices: `C:\Program Files\Quest\KACE` Windows 64-bit devices: `C:\Program Files (x86)\Quest\KACE` Mac OS X devices: `/Library/Application Support/Quest/KACE/bin` 3. Enter the following command: KDeploy -hash=**filename** Where **filename** is the UNC path to the file. If the path contains spaces, enclose the entire path in double quotation marks.

Option	Description
	4. Press **Ctrl C** or **Command C** to copy the MD5 checksum. You can then paste it into other files, such as Notepad. **Credential**: The details of the service account required to connect to the device and run commands. Select existing credentials from the drop-down list, or select **Add credential** to add credentials not already listed. See Add and edit User/Password credentials. **NOTE:** If the target device is part of a replication label, the appliance does not fetch applications from the alternate download location. You can edit an existing label or create a label to specify the alternate location globally. Because that label cannot be specific to any Managed Installation, you cannot specify an alternate checksum that matches the checksum on the remote file share. See Distributing packages from alternate download locations and Replication Shares and Add or edit manual labels.

Default Installation	You do not need to specify an installation command. The server runs the installation command by itself. The Mac OS X device tries to install the package using this command:
	`installer -pkg packagename.pkg -target / [Run Parameters]`
	or
	`ditto -rsrc packagename.app /Applications/theapp`
	If you have specified an archive file, this command runs against all of the PKG files or APP files it can find.

Override Default Installation	Specify the full command-line parameters. See the MSI Command Line documentation for available runtime options. **NOTE:** When using a DMG package, the command line should be relative to the file path of the mounted DMG file. • **Uninstall**: Uninstall the application from the command line. • **Run Command Only (do not download file)**: Run the command line only. • **Don't Prepend msiexec.exe**: Prevent the appliance from adding `msiexec.exe` to the beginning of the file.
Delete Downloaded Files	Delete the files when the deployment is complete.

NOTE: User notification messages are not available on Mac OS X devices.

4. Specify deployment settings in the Deploy tab:

Option	Description
All Devices	Deploy to all devices. Clear the check box to limit the deployment to specific labels or devices.
Restrict to Labels	Limit deployment to devices that belong to specified labels. To select labels, click **Edit**, drag labels to the *Limit Deployment to* window, then click **Save**. If you select a label that has a Replication Share or an alternate download location, the appliance copies digital assets from that Replication Share or alternate download location instead of downloading them directly from the appliance.

Option	Description
	NOTE: The appliance uses a Replication Share before it uses the KACE Alt Location.
Devices	Limit deployment to specific devices. In the drop-down list, select the devices to which you want to deploy the application. To filter the list, type a few characters in the *Devices* field. The number next to the field indicates the number of devices available. **NOTE: Reclaiming unused software licenses only.** Any devices from which you want to remove the applicable software are listed. You can edit the list of devices, as needed. To remove the software from all devices, simply select , as described above. For more information, see Reclaim unused software licenses.

5. Select appropriate options in the Schedule tab:

Option	Description
Deployment Window Start End	The time, in 24-hour clock format, for package deployment to start and end. The *Deployment Window* time affects all *Action* options. Also, the run intervals defined in the appliance *Settings* interact with or override the deployment window of specific packages.
Order	The order in which to install or uninstall applications. The lowest value is deployed first. If an install action and an uninstall action both have the same order value, the uninstall action is performed first. **NOTE:** Managed Installations are always deployed in order, regardless of whether their specified software packages come from the Software Catalog or the Software list. Managed Installations with a lower deploy order always prevent other Managed Installations from running until they are successfully installed or exceed the specified retry times.
Maximum Attempts	The maximum number of attempts, between 0 and 99, to indicate the number of times the appliance tries to install the package. If you specify 0, the appliance attempts to install the package indefinitely.

6. Click **Save**.

For more information, see:

- Distributing software and using Wake-on-LAN
- Using Managed Installations

Create and use File Synchronization

Using File Synchronization, you can push out any type of file to Agent-managed devices.

File Synchronization enable you to distribute files to managed devices. Unlike Managed Installations, however, File Synchronization do not install files; they simply distribute files. Use File Synchronization to copy files of any type to managed devices.

The string `KACE_ALT_Location` in the *Alternate Location* field is replaced with the value assigned by the corresponding label. You should not have a device in more than one label with an Alternate Location specified.

1. Go to the *File Synchronizations* list:

a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
b. On the left navigation bar, click **Distribution**, then click **File Synchronizations**.
c. Select **Choose Action** > **New**.

If this option is unavailable, there are no applications with the associated files in inventory. See Attach digital assets to applications and select supported operating systems.

2. In the *Configure* section, provide the following information:

Option	Description
Persist	Confirm that the file does not already exist on target devices before attempting to distribute it.
Delete Temporary Files	Delete the files when the deployment is complete.
Name	A name that identifies the File Synchronization. This name appears on the *File Synchronizations* page.
Path	The directory location, on target devices, to which you want to save the file.
Create Path	Create the location specified in the *Path* field if it does not already exist.
Credentials	The details of the service account required to connect to the device and run commands. Select existing credentials from the drop-down list, or select **Add credential** to add credentials not already listed. See Add and edit User/Password credentials.
File	The file to be distributed to target devices. To appear on the list, applications must have associated files in inventory. See Attach digital assets to applications and select supported operating systems.
Do Not Uncompress Distribution	Prevent the appliance from uncompressing files.
Enabled	Enable the File Synchronization. When the KACE Agents on selected devices check into the appliance, the file is distributed.
Create Shortcut	Create a desktop shortcut to the file location on the device.
Name	The display name for the desktop shortcut.
Alternate Location	Specify a location from which files can be downloaded for a specific Managed Installation. **Path**: Enter the location where the KACE Agent can retrieve digital installation files. **Checksum**: Enter an alternate checksum (MD5) that matches the MD5 checksum on the remote file share. If no checksum is entered, the digital asset on the file share must match the digital asset associated with the deployment package on the appliance. Also, the target path must include the complete filename (for example, `\\fileserver_one\software\adobe.exe`). You can create the checksum using any tool, including KDeploy.exe, which is installed with the KACE Agent.

Option	Description
	To create the checksum using KDeploy.exe: 1. On a device with the KACE Agent installed, open a command prompt or terminal window. 2. Go to the Quest KACE installation directory. For example: Windows 32-bit devices: `C:\Program Files\Quest\KACE` Windows 64-bit devices: `C:\Program Files (x86)\Quest\KACE` Mac OS X devices: `/Library/Application Support/Quest/KACE/bin` 3. Enter the following command: KDeploy -hash=**filename** Where **filename** is the UNC path to the file. If the path contains spaces, enclose the entire path in double quotation marks. 4. Press **Ctrl C** or **Command C** to copy the MD5 checksum. You can then paste it into other files, such as Notepad. **Credential**: The details of the service account required to connect to the device and run commands. Select existing credentials from the drop-down list, or select **Add credential** to add credentials not already listed. See Add and edit User/Password credentials. **NOTE:** If the target device is part of a replication label, the appliance does not fetch applications from the alternate download location. You can edit an existing label or create a label to specify the alternate location globally. Because that label cannot be specific to any Managed Installation, you cannot specify an alternate checksum that matches the checksum on the remote file share. See Distributing packages from alternate download locations and Replication Shares and Add or edit manual labels.

3. Specify deployment settings in the Distribute tab:

Option	Description
All Devices	Deploy to all devices. Clear the check box to limit the deployment to specific labels or devices.
Restrict to Labels	Limit deployment to devices that belong to specified labels. To select labels, click **Edit**, drag labels to the *Limit Deployment to* window, then click **Save**. If you select a label that has a Replication Share or an alternate download location, the appliance copies digital assets from that Replication Share or alternate download location instead of downloading them directly from the appliance. **NOTE:** The appliance uses a Replication Share before it uses the KACE Alt Location.
Devices	Limit deployment to specific devices. In the drop-down list, select the devices to which you want to deploy the application. To filter the list, type a few characters in the *Devices* field. The number next to the field indicates the number of devices available.
Blackout Window	The time during which Agents on managed devices are prevented from performing File Synchronizations.

4. Specify the following options in the **Notify** tab:

Option	Description
Initial Message	Display a message on devices before installation.

Option	Description
Completion Message	Display a message on devices after the installation is complete.

5. Click **Save**.

TIP: To distribute files previously deployed after the deployment window has closed, go to the *File Synchronization Detail* page for the File Synchronization, then click **Save and Resend Files** at the bottom of the page.

Using Wake-on-LAN

Wake-on-LAN enables you to power-on devices remotely from the appliance regardless of whether the devices have the KACE Agent installed.

NOTE: To use Wake-on-LAN, devices must be equipped with Wake-on-LAN-enabled network interface card (NIC) and BIOS.

For Wake-on-LAN, the appliance broadcasts UDP traffic on your network on port 7. The appliance sends 16 packets per Wake-on-LAN request because it must guess the broadcast address that is required to get the “Magic Packet” to the target device. This traffic is ignored by devices that are not being powered-on remotely, and the traffic should not have a noticeable impact on the network.

You can power on devices belonging to the same subnet as the appliance, or on different subnets. To power on a device associated with a different subnet, you must designate a KACE Agent as a Wake-on LAN Relay.

Issue Wake-on-LAN requests

To wake multiple devices at once, you can specify a label to which those devices belong, or you can wake devices individually.

If the device you want to wake is not inventoried by the appliance but you know the MAC (hardware) address and the device’s last-known IP address, you can manually enter the information to wake the device.

1. Go to the *Wake-on-LAN Schedules* list.
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Distribution**, then click **Wake-on-LAN**.
2. Select **Choose Action** > **New** > **Simple**.
3. Select the type of device to work with:
    - **To wake devices that belong to labels, select labels in the *Labels* drop-down list.**
    - **To wake individual devices, select devices the *Managed Devices* field. To search the list, begin typing in the field.**
    - **To wake Discovered devices, select devices in the *Discovered Devices* field. To search the list, begin typing in the field.**
4. To enter device information manually, do one of the following:
    - **In the *Manual IP Address* field, specify the IP address of a device.**
    - **In the *Manual MAC Entry* section, specify the MAC address of a device.**
5. Click **Run Now**.

The results at the top of the page indicate the number of devices that received the request and the labels, if any, to which those devices belong.

Schedule Wake-on-LAN requests

Scheduling a Wake-on-LAN request is useful when you want to wake devices on a regular basis. This is useful for recurring tasks, such as performing monthly maintenance.

If you want to wake devices belonging to a different subnet, you must find a machine belonging to the device's subnet and running a KACE Agent instance, and designate that machine as a relay by assigning it a label. For more information about labels, see Setting up and using labels to manage groups of items.

1. Go to the *Wake-on-LAN Schedules* list:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Distribution**, then click **Wake-on-LAN**.
2. Select **Choose Action** > **New** > **Advanced**.
3. In the *Configure* tab, select the type of device to work with:
    - **To choose devices that belong to labels, in the *Configure* section, under *Labels*, click Manage Associated Labels. In the *Select Labels* dialog box that appears, select one or more labels associated with the devices that you want to select. Close the dialog box.**
    - **To choose devices by operating system, click Manage Operating Systems. In the Operating Systems dialog box that appears, select the OS versions in the navigation tree, as applicable.**

      You have an option to select OS versions by their family, product, architecture, release ID, or build version. You can choose a specific build version, or a parent node, as needed. Selecting a parent node in the tree automatically selects the associated child nodes. This behavior allows you to select any future OS versions, as devices are added or upgraded in your managed environment. For example, to select all build current and future versions associated with the Windows 10 x64 architecture, under **All** > **Windows** > **Windows 10**, select **x64**.
4. To wake a device that belongs to a different subnet, select a relay machine.
    a. In the *Configure* tab, under *Relay Labels*, click **Manage Associated Labels**.
    b. In the *Select Labels* dialog box that appears, select the label associated with the relay device.
    c. Close the dialog box.
5. On the *Wake-on-LAN Settings* page, in the *Schedule* tab, specify the schedule settings:

Option	Description
None	Run in combination with an event rather than on a specific date or at a specific time.
Every n hours	Run at a specified interval.
Every day/specific day at HH:MM	Run daily at a specified time, or run on a designated day of the week at a specified time.
Run on the nth of every month/ specific month at HH:MM	Run on the same day every month, or a specific month, at the specified time.
Run on the nth weekday of every month/specific month at HH:MM	Run on the specific weekday of every month, or a specific month, at the specified time.
Custom	Run according to a custom schedule.

Option	Description

	Use standard 5-field cron format (extended cron format is not supported):
	`* * * * *`
	`| | | | +————————day of week (0-6)(Sun=0)`
	`| | | +————————month (1-12)`
	`| | +————————day of month (1-31)`
	`| +————————hour (0-23)`
	`+————————minute (0-59)`
	Use the following when specifying values:
	• **Spaces ( )**: Separate each field with a space.
	• **Asterisks (*)**: Include the entire range of values in a field with an asterisk. For example, an asterisk in the hour field indicates every hour.
	• **Commas (,)**: Separate multiple values in a field with a comma. For example, `0,6` in the day of the week field indicates Sunday and Saturday.
	• **Hyphens (-)**: Indicate a range of values in a field with a hyphen. For example, `1-5` in the day of the week field is equivalent to `1,2,3,4,5`, which indicates Monday through Friday.
	• **Slashes (/)**: Specify the intervals at which to repeat an action with a slash. For example, `*/3` in the hour field is equivalent to `0,3,6,9,12,15,18,21`. The asterisk (`*`) specifies every hour, but `/3` restricts this to hours divisible by 3.
	Examples:
	• `15 * * * * Run 15 minutes after every hour every day`
	• `0 22 * * * Run at 22:00 every day`
	• `0 0 1 1,6 * Run at 00:00 on January 1 and June 1`
	• `30 8,12 * * 1-5 Run weekdays at 08:30 and 12:30`
	• `0 2 */2 * * Run every other day at 02:00`

View Task Schedule	Click to view the task schedule. The *Task Schedule* dialog box displays a list of scheduled tasks. Click a task to review the task details. For more information, see View task schedules.

6. Click **Save**.

The *Wake-on-LAN* page appears with the scheduled request listed.

Troubleshooting Wake-on-LAN

Under certain conditions, a Wake-on-LAN request might fail.

Conditions that might cause Wake-on-LAN failures include:

- The device does not have a Wake-on-LAN-capable network card or is not configured properly.
- The appliance has incorrect information about the subnet to which the device is attached.
- UDP traffic is not routed between subnets or is being filtered by a network device.
- Broadcast traffic is not routed between subnets or is being filtered by a network device.
- Traffic on port 7 is being filtered by a network device.

For more information, go to http://www.intel.com/content/www/us/en/support/network-and-i-o/ethernet-products/000005793.html.

Exporting Managed Installations

If you have multiple organizations or appliances, you can export Managed Installations and transfer them among organizations and appliances as needed.

See About importing and exporting resources.

Broadcasting alerts to managed devices

You can send messages to users by broadcasting alerts, which are displayed as pop-up messages, on Agent-managed devices.

Displaying alerts is useful when you need to communicate urgent information, or notify users before running actions or scripts on their devices.

In addition, you can create email notifications that can be sent automatically when specified criteria are met. See Scheduling notifications.

NOTE: Displaying a message on a managed device requires a connection between the Agent and the appliance. For information about Agent connections, see .

NOTE: This type of alert is generated at the appliance, to be broadcast to Agent-managed devices. The other type of alert is the monitoring alert, which comes into the appliance from your server devices if you have enabled monitoring on them to perform basic performance monitoring. See Monitoring devices.

Create alerts to be broadcast

You can create and schedule alerts to be broadcast to Agent-managed devices as needed.

1. Go to the *Alert Detail* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Distribution**, then click **Alerts**.
    c. Select **Choose Action** > **New**.
2. Provide the following information in the **Configuration** tab:

Option	Description
Message	Type the content of the alert to be displayed. The message can contain up to 500 characters.
All Devices	Display the message on all devices whose KACE Agents are connected to the appliance.
Urgent	Display the message in the center of the screen, without allowing the user to move it, or to send it to the background. The alert must be addressed before any work can continue.
Devices	Display the message on specified devices. Use **Ctrl**-click or **Command**-click to select multiple devices.

Option	Description
Restrict to Labels	Display the message only on devices assigned to selected labels. click **Manage Associated Labels** to select device labels. Use **Ctrl**-click or **Command**-click to select multiple labels.
Expiration	Specify the length of time for the message to be valid. When target devices are connected to the appliance, the message is broadcast and is displayed until the user acknowledges the message by clicking **OK**. **NOTE:** If a device is not connected to the appliance, the alert message is sent to the Agent Command Queue, and it remains there until the device connects to the appliance. When the target device connects, the message appears regardless of whether the *Expiration* time has elapsed.

3. In the *Schedule* tab, specify the schedule settings:

Option	Description
None	Run in combination with an event rather than on a specific date or at a specific time.
Every	Run every number of set hours.
Run Every day/ specific day at HH:MM	Run daily at a specified time, or run on a designated day of the week at a specified time.
Run on the nth of every month/ specific month at HH:MM	Run on the same day every month, or a specific month, at the specified time.
Run on the nth weekday of every month/specific month at HH:MM	Run on the specific weekday of every month, or a specific month, at the specified time.

Custom	Run according to a custom schedule.
	Use standard 5-field cron format (extended cron format is not supported):
	`* * * * *`
	`| | | | +----------day of week (0-6)(Sun=0)`
	`| | | +----------month (1-12)`
	`| | +----------day of month (1-31)`
	`| +----------hour (0-23)`
	`+----------minute (0-59)`

Option	Description
	Use the following when specifying values: • **Spaces ( )**: Separate each field with a space. • **Asterisks (*)**: Include the entire range of values in a field with an asterisk. For example, an asterisk in the hour field indicates every hour. • **Commas (,)**: Separate multiple values in a field with a comma. For example, `0,6` in the day of the week field indicates Sunday and Saturday. • **Hyphens (-)**: Indicate a range of values in a field with a hyphen. For example, `1-5` in the day of the week field is equivalent to `1,2,3,4,5`, which indicates Monday through Friday. • **Slashes (*/*)**: Specify the intervals at which to repeat an action with a slash. For example, `*/3` in the hour field is equivalent to `0,3,6,9,12,15,18,21`. The asterisk (`*`) specifies every hour, but `/3` restricts this to hours divisible by 3. Examples: • `15 * * * * Run 15 minutes after every hour every day` • `0 22 * * * Run at 22:00 every day` • `0 0 1 1,6 * Run at 00:00 on January 1 and June 1` • `30 8,12 * * 1-5 Run weekdays at 08:30 and 12:30` • `0 2 */2 * * Run every other day at 02:00`
View Task Schedule	Click to view the task schedule. The *Task Schedule* dialog box displays a list of scheduled. Click a task to review the task details. For more information, see View task schedules.

4. Click **Save**.

Running scripts on managed devices

You can create scripts and run them on managed devices to automate tasks and configure settings.

About scripts

Scripts provide a point-and-click interface to perform tasks that typically require a manual process or advanced programming. You can create scripts and run them to perform tasks on target devices across your network.

Scripts automate tasks such as:

- Configuring power management settings
- Installing software
- Checking antivirus status
- Changing registry settings
- Scheduling software deployment

You can create these types of scripts:

Option	Description
Offline KScripts	Scripts that run at a scheduled time, based on the target device's clock. Offline KScripts can run even when target devices are not connected to the appliance, such as when devices start up or when users log in. You can create these scripts using the scripting templates.
Online KScripts	Scripts that run only when a target device is connected to the appliance. Online KScripts run at scheduled times based on the appliance clock. You can create these scripts using the scripting templates.
Online shell scripts	Scripts that run at scheduled times based on the appliance clock, but that run only when the target device is connected to the appliance. Online shell scripts are created using simple text-based scripts, such as Bash, Perl, batch, and so on, that are supported by the target device's operating system. Batch files are supported on Windows, along with the different shell script formats supported by the specific operating system of the target devices.

Each script consists of:

- Metadata.
- Dependencies, including any supporting executable files that are necessary to run a script, for example, ZIP and BAT files.
- Rules to obey, such as offline KScripts and online KScripts.
- Tasks to complete, such as offline KScripts and online KScripts. Each script can have any number of tasks, and you can configure whether each task must complete successfully before the next one runs.
- Deployment settings.
- Schedule settings.

Obtaining script dependencies

Script dependencies include files and other items that are used by scripts. If scripts have dependencies, and those dependencies are present on target devices, those dependencies are used. Otherwise, scripts look for dependencies on repositories in a specified order.

Scripts obtain dependencies from the target device and repositories in the following order:

1. The target device
2. An alternate download location (KACE_ALT_LOCATION)
3. A Replication Share
4. The appliance

NOTE: For information about alternate download locations and Replication Shares, see Distributing packages from alternate download locations and Replication Shares.

Tracking changes to scripting settings

If History subscriptions are configured to retain information, you can view the details of the changes made to settings, assets, and objects.

This information includes the date the change was made and the user who made the change, which can be useful during troubleshooting. See About history settings.

About default scripts

Default scripts are pre-configured scripts you can use to force devices to report inventory, enable and disable debugging on devices, shutdown devices, and perform other tasks on devices remotely.

Table 27. Default scripts

Script Name	Description
Defragment the C: drive	Defragments drive C on the device.
Force Check-In	Forces Windows devices with the KACE Agent installed to take inventory and sync with the appliance. **IMPORTANT: Do not run Force Check-In with more than 50 devices selected because it can overload the appliance with requests.**
Force Check-In (Mac/Linux)	Force Mac and Linux devices with the KACE Agent installed to take inventory and sync with the appliance. **IMPORTANT: Do not run Force Check-In with more than 50 devices selected because it can overload the appliance with requests.**
Inventory Startup Programs Fix	On some devices, a missing registry entry causes all the contents of the system32 directory to be reported as Startup Programs. This script fixes the registry entry if it is missing.
Issue a DOS Command Example	Issues the `DOS-DIR` command on a Windows device. Used as an example for how to run a DOS command.
Issue a Mac Command Example	Issues the `AppDir.txt` command to list the contents of the Mac OS X Applications directory. Used as an example of how to run a command on Mac OS X.
K1000 Enable Detailed DDPE Inventory (Windows)	Sets a registry key that causes the Dell Data Protection | Encryption agent to write policy data to the file system, which enables the KACE Agent to perform more detailed inventory collection. Windows PowerShell 2.0 or higher is required.
K1000 Remote Control Disabler	Disables the appliance Remote Control functionality on Windows XP Professional by configuring Terminal Services properly.
K1000 Remote Control Enabler	Enables the appliance Remote Control functionality on Windows XP Professional by configuring Terminal Services properly.
Make Removable Drives Read-Only	Allows removable drives to be mounted only as read-only. This action controls unauthorized access to data.
Make Removable Drives Read-Write	Sets the properties of removable drives so that they can be mounted as read-write enabled.

Script Name	Description
Message Window Script Example	Illustrates the use of the Message Window. Your script must have properly paired create/destroy Message Window commands to work properly. The Message Window appears until one of the following occurs: • The user dismisses the message. • The script runs to completion. • A timeout period expires.
Put a Mac to sleep	Places a Mac OS X device in Sleep mode. **NOTE:** This script works with Mac OS X 10.5 and higher. It does not work with earlier versions of Mac OS X.
Reset KUID	Deletes the registry key that identifies a Windows device so that a new key can be generated. Runs once per device using the `ResetKUIDRunOnce` registry flag.
Shutdown a Mac	Powers-off a Mac OS X device.
Shutdown a Mac with snooze	An example online KScript that uses the **Alert user before run** feature to allow administrators to snooze the shutdown.
Shutdown a Windows system	Specifies a delay (in seconds) while the message in quotes is displayed to the user. Omit the `-t` parameter to silently and immediately shut down devices.
Shutdown a Windows system with Snooze	An example online KScript that uses the **Alert User Before Run** feature to allow the administrator to snooze the shutdown.
USB Drives Disable	Disables the use of USB drives.
USB Drives Enable	Enables the use of USB drives.

Adding and editing scripts

You can add or edit scripts using the **Administrator Console**.

To add and edit scripts, do one of the following:

- Import an existing script in XML format. See Structure of importable scripts.
- Duplicate an existing script. See Duplicate scripts.
- Create a script. See Add offline KScripts, online KScripts, or online shell scripts.

TIP: The process of creating scripts is an iterative one. After creating a script, deploy it to a limited number of devices to verify that it runs as expected before deploying it to all managed devices. You can create a test label to do this verification. Enable scripts only after you have tested them.

Token replacement variables

Use token replacement values to add variables to scripts. The following list shows the token replacement values that can be used in the XML of scripts. At run time, these variables are replaced on the device with the appropriate values.

Table 28. Token replacement values

Item	Description
$(KACE_DEPENDENCY_DIR)	This is the folder where any script dependencies for this script are downloaded to the client. **5.2 or higher**: `$(KACE_DATA_DIR)\kbots_cache\packages\kbots\xxx` **5.1**: `$(KACE_INSTALL)\packages\kbots\xxx`
$(KACE_SYS_DIR) **$(KBOX_SYS_DIR)**	Agent device's system directory. Both are synonymous. Preferred: **$(KACE_SYS_DIR)**. **Windows**: `C:\Windows\System32` **Mac OS X**: `/` **Linux**: `/`
$(KACE_MAC_ADDRESS) **$(MAC_ADDRESS)** **$(KBOX_MAC_ADDRESS)**	Agent device's primary Ethernet MAC address. All are synonymous. Preferred: **$(KACE_MAC_ADDRESS)**
$(KACE_IP_ADDRESS) **$(KBOX_IP_ADDRESS)**	Agent's local IP address (corresponds with network entry of KACE_MAC_ADDRESS) (`http://kace.kbox.com:80`). Both are synonymous. Preferred: **$(KACE_IP_ADDRESS)**
$(KACE_SERVER_URL)	Combination of server, port, and URL prefix. (http://kace.kbox.com:80)
$(KACE_SERVER)	Hostname of appliance server. (kbox)
$(KACE_SERVER_PORT)	Port to use when connecting to the appliance server. (80/433)
$(KACE_SERVER_URLPREFIX)	Web protocol to use when connecting to the appliance server. (http/https)
$(KACE_COMPANY_NAME)	Agent's copy of the setting from server's config page.
$(KACE_KUID) **$(KBOX_MACHINE_ID)**	The unique Quest KACE ID assigned to this Agent. Both are synonymous. Preferred: **$(KACE_KUID)**
$(KACE_APP_DIR)	Installation directory for the Quest KACE Agent and plugins.

Item	Description
	For older Agents this is mapped to **$(KACE_INSTALL)**. **Windows**: `C:\Program Files\Quest\KACE\` or `C:\Program Files (x86)\Quest\KACE\` **Mac OS**: `/Library/Application Support/Quest/KACE/bin` **Linux**: `/opt/quest/kace/bin`
$(KACE_DATA_DIR)	Installation directory for executables, scripts, packages, and so on. For older Agents this is mapped to **$(KACE_INSTALL)**. **Windows Vista and later**: `C:\ProgramData\Quest\KACE\` **Mac OS**: `/Library/Application Support/Quest/KACE/data` **Linux**: `/var/quest/kace`
$(KACE_AGENT_VERSION)	Substitutes the version number of the installed Agent. "5.2.12345". **5.2 or higher only**.
$(KACE_AGENT_ARCH)	Substitutes the architecture of the installed Agent. "x86/x64". **5.2 or higher Windows only**.
$(KACE_HARDWARE_ARCH)	Substitutes the architecture of the physical hardware. "x86/x64". **5.2 or higher Windows only**.
$(KACE_OS_FAMILY)	Substitutes Windows, Mac, or Linux depending on the operating system of the Agent-managed device. **5.2 or higher only**.
$(KACE_OS_ARCH)	Substitutes x86 or x64 depending on the installed version of Microsoft Windows. **5.2 or higher Windows only**.

Add offline KScripts, online KScripts, or online shell scripts

You can add KScripts, specify the devices on which you want to run the scripts, and schedule scripts to run as needed.

Offline and online KScripts include one or more tasks. Within each *Task* section, there are *Verify* and *Remediation* sections where you can further define the script behavior. If a section is blank, it defaults to *Success*.

1. Go to the *Script Detail* page:

a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.

b. On the left navigation bar, click **Scripting**, then click **Scripts**.

c. Select **Choose Action** > **New**.

2. In the *Configure* tab, specify script settings:

Option	Description
Name	A meaningful name for the script that distinguishes it from others on the *Scripts* list. **TIP:** You can enable or disable one or more scripts on the *Scripts* page. To do that, select them in the table, click , then click **Enable** or **Disable**, as required.
Enabled	Whether the script is enabled to run on the target devices. Do not enable a script until you are finished editing and testing it and are ready to run it. Enable the script on a test label before you enable it on all devices.
Category	The script category. Choose an existing category from the drop-down list, or click **New Category** to add a category. If you do not to assign a category to this script, ensure this field is set to **None**. • You can assign a category to one or more scripts on the *Scripts* page. To do that, select them in the table, click **Choose Action** > **Category**, then select a category in the list. • You can remove a category by assigning all scripts currently under a **Category** to None.
Type	The script type. Script types include: • **Online KScripts**: Scripts that run only when a target device is connected to the appliance. Online KScripts run at scheduled times based on the appliance clock. You can create these scripts using the scripting templates. • **Offline KScripts**: Scripts that run at a scheduled time, based on the target device's clock. These scripts can run even when target devices are not connected to the appliance, such as when devices start up or when users log in. You can create these scripts using the scripting templates. • **Online shell scripts**: Scripts that run at scheduled times based on the appliance clock, but that run only when the target device is connected to the appliance. Online shell scripts are created using simple text-based scripts, such as Bash, Perl, batch, and so on, that are supported by the target device's operating system. Batch files are supported on Windows, along with the different shell script formats supported by the specific operating system of the target devices. PowerShell scripts are also supported on Windows-based target devices. **IMPORTANT: You must ensure the proper file extension is associated with the script to enable it to run on the target OS. For example, you can run `.sh` scripts on Mac and Linux devices, and `.ps1` PowerShell scripts on Windows devices.**
Status	Whether the script is in development (**Draft**) or has been rolled out to your network (**Production**). Use the **Template** status if you are building a script to use as the basis for future scripts.

Option	Description
Description	(Optional) A brief description of the actions the script performs. This field helps you to distinguish one script from another on the *Scripts* list.
Notes	Any additional information you want to provide.

3. In the *Deploy* tab specify deployment options:

Option	Description
All Devices	Deploy to all devices. Clear the check box to limit the deployment to specific labels or devices.
Restrict to Labels	Limit deployment to devices that belong to specified labels. To select labels, click **Edit**, drag labels to the *Limit Deployment to* window, then click **OK**. If you select a label that has a Replication Share or an alternate download location, the appliance copies digital assets from that Replication Share or alternate download location instead of downloading them directly from the appliance. **NOTE:** The appliance uses a Replication Share before it uses the KACE Alt Location.
Devices	Limit deployment to one or more devices. To find devices, begin typing in the field.
Operating Systems	The operating systems on which the application runs. Applications are deployed only to devices with the selected operating systems. 1. Click **Manage Operating Systems**. 2. In the **Operating Systems** dialog box that appears, select the OS versions in the navigation tree, as applicable. You have an option to select OS versions by their family, product, architecture, release ID, or build version. You can choose a specific build version, or a parent node, as needed. Selecting a parent node in the tree automatically selects the associated child nodes. This behavior allows you to select any future OS versions, as devices are added or upgraded in your managed environment. For example, to select all build current and future versions associated with the Windows 10 x64 architecture, under **All** > **Windows** > **Windows 10**, select **x64**.

4. Specify *Windows Run As* settings (for online shell scripts and KScripts that run on Windows devices only):

Option	Description
Local System	Run the script with administrative privileges on the local device. Use this setting for all scripts created with a template.
Logged-in user	Run the script as the user who is logged in to the local device. This affects the user's profile.
All logged-in users	Run the script once for every user that is logged in to the device. This affects the profiles of all users.
Credentials	Run the Online Shell Script and KScripts in the context of credentials that are specified here. Select existing credentials from the drop-down list, or select **Add new credential** to add credentials not already listed. See Add and edit User/Password credentials.

Option	Description
	NOTE: When running online KScripts on Windows devices, message windows are not displayed on target devices when you select the option to run the script as a specific credentialed user. To display message windows, run the script as Local System, Logged-in user, or All logged-in users.

5. In the *User Notify* tab, specify user alert settings. Alerts are available only for online KScripts and online shell scripts on Windows and Mac devices running the KACE Agent version 5.1 and higher:

Option	Description
Notify User Before Run	Allow the user to run, cancel, or delay the action. This is especially important when reboots are required. If no user is logged in, the script runs immediately.
Options	Options presented to the user in the alert dialog (available when you select **Alert user before run**): • **OK**: Run immediately. • **Cancel**: Cancel until the next scheduled run. • **Snooze**: Prompt the user again after the *Snooze Duration*. If the time specified in the *Timeout* elapses without a user response, the script runs at that time. Interaction with *Run As*: • Only the console user can see the alert dialog, and therefore choose to Snooze or Cancel, regardless of the *Run As* setting. • Enabling an alert prompts the console user even if the script is set to run as all users or another user.
Timeout	The amount of time, in minutes, for the dialog to be displayed before an action is performed. If this time period elapses without the user pressing a button, the appliance performs the action specified in the *Timeout* drop-down list.
Timeout Action	The action to be performed when the **Timeout** period elapses without the user choosing an option.
Snooze Duration	The amount of time, in minutes, for the period after the user clicks **Snooze**. When this period elapses, the dialog appears again.
Initial Message	The message to be displayed to users before the action runs. To customize the logo that appears in the dialog, see Configure appliance General Settings without the Organization component.

6. In the *Schedule* tab, specify run options:

Option	Description
None	Run in combination with an event rather than on a specific date or at a specific time.
Every n hours	Run at a specified interval.
Every day/specific day at HH:MM	Run daily at a specified time, or run on a designated day of the week at a specified time.

Option	Description
Run on the nth of every month/ specific month at HH:MM	Run on the same day every month, or a specific month, at the specified time.
Run on the nth weekday of every month/specific month at HH:MM	Run on the specific weekday of every month, or a specific month, at the specified time.

Custom	Run according to a custom schedule.
	Use standard 5-field cron format (extended cron format is not supported):
	`* * * * *`
	`| | | | +———————day of week (0-6)(Sun=0)`
	`| | | +———————month (1-12)`
	`| | +———————day of month (1-31)`
	`| +———————hour (0-23)`
	`+———————minute (0-59)`
	Use the following when specifying values:
	• **Spaces ( )**: Separate each field with a space.
	• **Asterisks (*)**: Include the entire range of values in a field with an asterisk. For example, an asterisk in the hour field indicates every hour.
	• **Commas (,)**: Separate multiple values in a field with a comma. For example, `0,6` in the day of the week field indicates Sunday and Saturday.
	• **Hyphens (-)**: Indicate a range of values in a field with a hyphen. For example, `1-5` in the day of the week field is equivalent to `1,2,3,4,5`, which indicates Monday through Friday.
	• **Slashes (/)**: Specify the intervals at which to repeat an action with a slash. For example, `*/3` in the hour field is equivalent to `0,3,6,9,12,15,18,21`. The asterisk (`*`) specifies every hour, but `/3` restricts this to hours divisible by 3.
	Examples:
	• `15 * * * * Run 15 minutes after every hour every day`
	• `0 22 * * * Run at 22:00 every day`
	• `0 0 1 1,6 * Run at 00:00 on January 1 and June 1`
	• `30 8,12 * * 1-5 Run weekdays at 08:30 and 12:30`
	• `0 2 */2 * * Run every other day at 02:00`

View Task Schedule	Click to view the task schedule. The *Task Schedule* dialog box displays a list of scheduled tasks. Click a task to review the task details. For more information, see View task schedules.

7. In the *Schedule Options* tab, select the applicable options.

Option	Description
Also run once at next device	Runs the offline KScript once when new scripts are downloaded from the appliance.

Option	Description
checkin (for offline KScripts only)	
Also Run before login (for offline KScripts only)	Runs the offline KScript when devices start up. This might cause devices to start up more slowly than normal. **NOTE:** If a device has an Active Directory or Group Policy Object setting that displays a message that the user must acknowledge before logging on, scripts do not run until the message is acknowledged.
Also run once at next device checkin (for offline KScripts only)	Runs the offline KScript after users enter Windows login credentials.
Allow run while disconnected (for offline KScripts only)	Allows the offline KScript to run even if the target device cannot contact the appliance to report results. In such a case, results are stored on the device and uploaded to the appliance during the next connection.
Allow run without a logged-in user	Allows the script to run even if a user is not logged in. To run the script only when the user is logged in to the device, clear this option.
Run on next connection if offline	For online KScripts or Shell Scripts, this option enables the script to run on offline machines when they become online again. When a script runs, it calculates the number of machines it is supposed to run on based on their labels, or their operating systems, or by manually identifying selected machines. Given that set of machines, the script then determines which of those machines are currently online, and then queues up a task for the online machines in the Konductor. When you select this option, the script skips the step that identifies online machines and it runs on the online machines. For the offline machines, the task is added to the Konductor's queue, and it runs when those machine become online. Any subsequent tasks for running the same script (for example, for an offline machine that already exists in the Konductor's queue) overwrite the existing tasks, so there can never be more than one task in the Konductor's queue for the same machine. Having a high number of tasks in the Konductor may affect the appliance's performance, so the best practice is to use offline scripts for those machines that are typically offline, and only use this option with online scripts when the target machines are expected to be online, to avoid an overpopulating the Konductor's queue. By default, this option is disabled.

8. To upload files required by the script:
    a. In the *Dependencies* section, click **Add new dependency**.
    b. Click **Browse** or **Choose File**.
    c. Select a file, then click **Open** or **Choose**.

If a Replication Share is specified and enabled, the dependencies are downloaded from the specified Replication Share.

NOTE: If the Replication Share is inaccessible, the dependencies are downloaded from the appliance. To enable this setting, select the *Failover To Appliance* check box on the *Replication Schedule Detail* page. See Create Replication Shares.

Repeat this step to add dependencies as needed.

9. **Online or Offline KScripts only**. In the *Tasks* tab, click **Add New Task** to add a task.

The process flow of a task is a script similar to the following:

```
IF Verify THEN
            Success
ELSE IF Remediation THEN
            Remediation Success
ELSE
            Remediation Failure
```

a. In the *Policy* or *Job Rules* section, specify the following settings for Task 1:

Option	Description
Attempts	Enter the number of times the appliance attempts to run the script. If the script fails but remediation is successful, you might want to run the task again to confirm the remediation step. To do this, set the number of attempts to 2 or more. If the *Verify* section fails, the script runs the number of times specified in this field.
On Failure	• Select **Break** to stop running upon failure. • Select **Continue** to perform remediation steps upon failure.

b. In the *Verify* section, click **Add** to add a step, then select one or more steps to perform.

See Adding steps to task sections of scripts.

c. In the *On Success* and *Remediation* sections, select one or more steps to perform.

See Adding steps to task sections of scripts.

d. In the *On Remediation Success* and *On Remediation Failure* sections, select one or more steps to perform.

See Adding steps to task sections of scripts.

TIP: To remove a dependency, click the **Delete** button next to the item: . This button appears when you mouse over an item.

TIP: Click the **Edit** button next to *Policy or Job Rules* to view the token replacement variables that can be used anywhere in the script: . The variables are replaced at runtime with appropriate values.

TIP: See Token replacement variables.

10. **Online shell scripts only**. In the *Script* section, specify the following settings:

Option	Description
Script Text	Type the script contents.
Script File Name	Enter the name and extension of the file that will contain the specified script. **IMPORTANT: You must ensure the proper file extension is associated with the script to enable it to run on the target OS. For example, you can run `.sh` scripts on Mac and Linux devices, and `.ps1` PowerShell scripts on Windows devices.**
Timeout (minutes)	Specify the maximum number of minutes the script can run on the target device.

Option	Description
Upload File	If the script creates a file, and you want to upload that file to the appliance, select this option, and provide the following information: • **Upload File Name**: Enter the name of the file. • **Upload File Directory Path**: Specify the directory where you want to store the file. If you want to use the default script directory (`<appliance_installation_directory>/scripts`), leave this field blank.
Delete Downloaded Files	If the script requires any other files to run, such as installers, and you want to delete them after the script execution, select this option.

11. Do one of the following:
    - **Click Run Now to immediately push the script to all devices.**

      Use this option with caution. See Using the Run and Run Now commands.
    - **Click Save.**

Edit scripts

You can edit the three types of scripts: offline KScripts, online KScripts, and online Shell Scripts. You can also edit offline KScripts and online KScripts with the XML editor.

Scoped users can view the details of all scripts, but they can save changes only to those to scripts that affect the devices or labels that are associated with their scope. For more information about scoped users, see Add or edit User Roles.

1. Go to the *Script Detail* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Scripting**, then click **Scripts**.
    c. Display the *Script Detail* page by doing one of the following:
    # Click the name of a script.
    # Select **Choose Action** > **New**.
2. Modify the script as needed.
3. Select options for configuration, deployment, and scheduling. See Add offline KScripts, online KScripts, or online shell scripts.
4. To edit the raw XML of the script, scroll to the *Schedule* section, then click **Edit XML**.
5. Click **Save**.

Delete scripts from the Scripts page

You can delete scripts from the Scripts page.

1. Go to the *Scripts* list:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Scripting**, then click **Scripts**.
2. Select the check box next to one or more scripts.
3. Select **Choose Action** > **Delete**, then click **Yes** to confirm.

Delete scripts from the Script Detail page

You can delete scripts from the *Script Detail* page.

1. Go to the *Script Detail* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Scripting**, then click **Scripts**.
    c. Click the name of a script.
2. Click **Delete**, then click **Yes** to confirm.

Structure of importable scripts

You can create a script in an external XML editor and import it to the appliance.

Imported scripts must conform to the following structure:

- The root element `<kbots></kbots>` includes the URL of the KACE DTD `"kbots xmlns="http://kace.com/Kbots.xsd">...<kbots>`
- One or more `<kbot>` elements.
- Exactly one `<config>` element within each `<kbot>` element.
- Exactly one `<execute>` element within each `<config>` element.
- One or more `<compliance>` elements within each `<kbot>` element.

The following is an example of the XML structure for an appliance script:

```
<?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>
```

In the preceding example, the `</config>` element corresponds to the *Configuration* section on the *Script Detail* page. This element is where you specify the name of the policy or job (optional), and the script type (policy or job). Within this element you can also indicate whether the script can run when the target device is disconnected or logged off from the appliance.

You can specify whether the script is enabled and describe the specific tasks the script is to perform within the <compliance> element.

TIP: To create a script that performs some of the same tasks as an existing script, duplicate the existing script, and open it in an XML editor. The script's <compliance> element gives you an idea of how the script works, and how you can change it. See Duplicate scripts.

Import scripts

You can import scripts to the appliance as needed.

1. Go to the *Scripts* list:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Scripting**, then click **Scripts**.
2. Select **Choose Action** > **Import**.
3. Paste the existing script into the space provided, then click **Save**.

Duplicate scripts

If there is a script that is similar to a script you want to create, you can duplicate that script and edit it as needed. Using duplication can be faster than creating a script from scratch.

1. Go to the *Script Detail* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Scripting**, then click **Scripts**.
    c. Click the name of a script.
2. At the bottom of the page, click **Duplicate** to display the *Scripts* page.

    The duplicated script appears on the list.
3. Click the linked name of the duplicated script to open it for editing.

See Edit scripts.

Using the Run and Run Now commands

The **Run** and **Run Now** commands enable you to run scripts on target devices immediately without setting a schedule.

Running scripts without setting a schedule is useful when:

- You suspect that devices on your network are infected with a virus or other vulnerability, and they might compromise the entire network if not resolved right away.
- You want to test and debug scripts on a specific device or a set of devices during development.

To run Online KScripts, target devices must have an Agent connection to the appliance.

TIP: To minimize the risk of deploying scripts to unintended devices, create a label that represents the devices on which you want to perform the **Run Now** command.

The **Run Now** command is available on these **Administrator Console** pages:

- *Run Now* and *Script Detail* pages: Running scripts from the *Scripting* > *Run Now* page enables you to run the selected script on target devices.
- *Scripts* page: Running scripts from the *Scripts* page using the **Run Now** option in the *Choose Action* menu enables you to run multiple scripts at the same time.

NOTE: In case you encounter an error while running a script, refer to Error codes caused by patching and scripting for a list of error codes that may help you diagnose the issue.

Run scripts from the Run Now page

You can run scripts on target devices from the *Run Now* page.

CAUTION: Scripts are deployed immediately when you click Run Now.

- Use Run Now cautiously.
- Do not click **Run Now** unless you are certain that you want to run the script on the target devices.

1. Go to the *Run Now* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Scripting**, then click **Run Now**.
2. In the *Scripts* drop-down list, select a script. To find a script, begin typing in the field.
3. In the *Deploy* section, specify deployment options:

Option	Options and Descriptions
Restrict to Labels	Limit deployment to devices that belong to specified labels. To select labels, click **Edit**, drag labels to the *Limit Deployment to* window, then click **Save**. If you select a label that has a Replication Share or an alternate download location, the appliance copies digital assets from that Replication Share or alternate download location instead of downloading them directly from the appliance. **NOTE:** The appliance uses a Replication Share before it uses the KACE Alt Location.
Devices	Limit deployment to one or more devices. To find devices, begin typing in the field. Scoped users can see only those devices that are associated with their role, when the role is assigned a label. For more information about scoping devices to user roles, see Add or edit User Roles.

4. Click **Run Now**.

    The *Run Now Status* page appears.

Run scripts from the Script Detail page

You can run scripts on target devices from the *Script Detail* page.

1. Go to the *Script Detail* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Scripting**, then click **Scripts**.
    c. Click the name of a script.
2. Scroll to the bottom of the page, then click **Run Now**.

    The *Run Now Status* page appears.

Run scripts from the Scripts page

You can run scripts from the *Scripts* page.

1. Go to the *Scripts* list:

a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
b. On the left navigation bar, click **Scripting**, then click **Scripts**.

2. Select the check box next to one or more scripts.
3. Select **Choose Action** > **Run Now**.

The *Run Now Status* page appears.

Monitor Run Now status and view script details

You can view the status of scripts that have been started using the **Run Now** command and access script details.

Ensure that firewall settings do not block the KACE Agent from listening on port 443.

The **Run Now** command communicates over port 443. Scripts might fail to deploy if firewall settings block the KACE Agent from listening on that port. For more information about port requirements, see Verifying port settings, NTP service, and website access.

1. Go to the *Run Now Status* list:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Scripting**, then click **Run Now Status**.
2. Review the information on the *Run Now Status* list.

Information on this page includes:

- **Started**: The time the **Run Now** command was issued.
- **Name**: The name of the script. Click this script name to view the *Run Now Detail* page.
- **Targeted**: The number of devices on which the script is scheduled to run.
- **Pushed, Running, Pending**: The number of devices on which the script is attempting to run.
- **Succeeded, Failed, Completed**: The number of devices on which the script has run.
- **Success Rate**: The percentage of scripts that ran successfully on target devices.

The numbers in the *Pushed*, *Running*, *Pending*, *Succeeded*, *Failed*, and *Completed* columns increment accordingly as the script is deployed to target devices. If errors occur in pushing the scripts to the selected devices, you can search the scripting logs to determine the cause. See Search the scripting logs.

3. Click the link in the *Started* column of a script to display the *Run Now Status Detail* page.

Information on this page includes:

- **Run Now Statistics**: The results of a script that was pushed, the push failures, push successes, completed devices, running devices, and successes and failures in numbers and percentage.
- **Failed Deployment**: The devices that the appliance could not contact and therefore did not receive the policy. When the script is pushed, it might take some time for the device to complete a policy.
- **Running**: The devices that have received the policy but have not reported its results. After the policy runs, it reports either success or failure. The results are sorted under the appropriate section. Each individual device page also has the results of the Run Now events run on that device.
- **Failed Execution**: The devices on which the script failed.
- **Successful Execution**: The devices on which the script ran successfully.

Edit policies and scripts

You can edit policies and scripts as needed.

1. Go to the *Script Detail* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Scripting**, then click **Scripts**.
    c. Display the *Script Detail* page by doing one of the following:
    # Click the name of a script.
    # Select **Choose Action** > **New**.
2. Change options for configuration, deployment, and scheduling.

See Add offline KScripts, online KScripts, or online shell scripts.

Search the scripting logs

You can search for text strings in the scripting logs. If the organization component is enabled on your appliance, you search scripting logs for each organization separately.

When scripts run on managed devices, logs are created and uploaded to the appliance. You can search for text strings in the scripting logs, and apply labels to devices whose logs match the search text. You can then run actions on the labeled devices as needed.

1. Go to the *Search Scripting Logs* page.
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Scripting**, then click **Search Scripting Logs**.
2. In the *Search for* field, enter the search criteria or text string you want to find. Text strings must be at least four characters in length. Searches with shorter text strings result in zero matches.

    Use the following operators when entering search criteria:

Operator	Function
+	Use a leading plus sign to find entries that include the text.
-	Use a leading minus sign to find entries that do not include the text.
*****	Use a trailing asterisk to find logs that contain words that begin with the specified characters.
"	Enclose text in double quotes to find exact matches for the phrase.

3. Select search criteria:

Option	Description
All uploaded logs	Search all available scripting logs. If the Organization component is enabled on the appliance, the search searches all logs for the selected organization.

Option	Description
	NOTE: Scripting logs are deleted during appliance upgrades. If the appliance has been upgraded, logs that were uploaded before the upgrade are no longer available.
Last uploaded logs	Search the most recent scripting logs. If the Organization component is enabled on the appliance, the search searches all logs for the selected organization.
Script	Search logs related to all scripts, or search only the specified script.
Log	Search all logs, or search only the specified log.
Label	Search for logs uploaded by all devices, or search for logs uploaded by devices associated with the specified label.

4. Click **Search**.

   The search results display the logs and the devices that have uploaded those logs.
5. To apply a label to the devices that are displayed, select a label in the drop-down list under the search results.

Exporting scripts

If you have multiple organizations or appliances, you can export scripts and transfer them among organizations and appliances as needed.

See About importing and exporting resources.

Using Task Chains

Task Chains allow you to create a sequence of tasks to run in a specific order.

You can add one or more Patch Schedules, online Scripts, File Synchronization items, and Wake-On LAN Requests to a Task Chain. Use Task Chains, for example, when you need to deploy managed installations and then run scripts on target devices. The order of tasks in a Task Chain can be easily changed, as required.

NOTE: You cannot add individual Managed Installations to a Task Chain.

Each Task Chain runs against a configured set of devices, as defined in the Task Chain.

If a target device in a Task Chain is offline, you can configure the Task Chain to run when the device becomes connected. When a target device is referenced in multiple Task Chains, only one Task Chain runs against the device at a time.

The following concepts apply to device selections in a Task Chain:

- Devices selected in a Task Chain override those set for patching schedules and scripts when they run as part of a Task Chain.
- Devices selected in a Task Chain do not affect any Managed Installation (MI) or File Synchronization (FS) items associated with those devices. Any Inventory, MI, and FS tasks are queued for each device in the Task Chain, and any MI and FS that are configured to run on each machine are deployed.
- Wake-on-LAN (WoL) schedules run once per Task Chain, when the first device in the Task Chain encounters the WoL Task. The WoL Task runs against the devices selected in the Task Chain.

NOTE: A WoL Task should always be scheduled as a first Task in a Task Chain. This causes WoL packets to be pushed to all devices at once and the devices will wait for this task, since it is the first Task. When a WoL task is not the first task in the Task Chain, WoL packets are pushed to all devices at once regardless of the current state of the task running in the task chain.

Add and edit Task Chains

A Task Chain is a collection of tasks that can run in a specific order. Use the *Task Chain Detail* page to add and edit Task Chains.

1. Go to the *Task Chains* list page:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Distribution**, then click **Task Chains**.
2. Do one of the following:
   # Select **Choose Action** > **New**.
   # Click the name of a task chain.
3. In the *Configure* tab, specify the following options:

Option	Description
Enabled	Select this check box to allow this task chain to run.
Name	The name of the task chain.
Description	A brief description of the task chain.

4. Still in the *Configure* tab, specify the devices on which you want the Task Chain to run.
   - **To choose devices that belong to labels, in the *Configure* section, under *Labels*, click Manage Associated Labels. In the *Select Labels* dialog box that appears, select one or more labels associated with the devices that you want to select. Close the dialog box.**
   - **To choose devices by operating system, click Manage Operating Systems. In the Operating Systems dialog box that appears, select the OS versions in the navigation tree, as applicable.**

     You have an option to select OS versions by their family, product, architecture, release ID, or build version. You can choose a specific build version, or a parent node, as needed. Selecting a parent node in the tree automatically selects the associated child nodes. This behavior allows you to select any future OS versions, as devices are added or upgraded in your managed environment. For example, to select all build current and future versions associated with the Windows 10 x64 architecture, under **All** > **Windows** > **Windows 10**, select **x64**.
5. In the *Schedule* tab, specify the schedule settings:

Option	Description
None	Run in combination with an event rather than on a specific date or at a specific time.
Every n hours	Run at a specified interval.
Every day/specific day at HH:MM	Run daily at a specified time, or run on a designated day of the week at a specified time.
Run on the nth of every month/	Run on the same day every month, or a specific month, at the specified time.

Option	Description
specific month at HH:MM	
Run on the nth weekday of every month/specific month at HH:MM	Run on the specific weekday of every month, or a specific month, at the specified time.

Custom	Run according to a custom schedule.
	Use standard 5-field cron format (extended cron format is not supported):
	`* * * * *`
	`| | | | +————————day of week (0-6)(Sun=0)`
	`| | | +————————month (1-12)`
	`| | +————————day of month (1-31)`
	`| +————————hour (0-23)`
	`+————————minute (0-59)`
	Use the following when specifying values:
	• **Spaces ( )**: Separate each field with a space.
	• **Asterisks (*)**: Include the entire range of values in a field with an asterisk. For example, an asterisk in the hour field indicates every hour.
	• **Commas (,)**: Separate multiple values in a field with a comma. For example, `0,6` in the day of the week field indicates Sunday and Saturday.
	• **Hyphens (-)**: Indicate a range of values in a field with a hyphen. For example, `1-5` in the day of the week field is equivalent to `1,2,3,4,5`, which indicates Monday through Friday.
	• **Slashes (*/*)**: Specify the intervals at which to repeat an action with a slash. For example, `*/3` in the hour field is equivalent to `0,3,6,9,12,15,18,21`. The asterisk (`*`) specifies every hour, but `/3` restricts this to hours divisible by 3.
	Examples:
	• `15 * * * * Run 15 minutes after every hour every day`
	• `0 22 * * * Run at 22:00 every day`
	• `0 0 1 1,6 * Run at 00:00 on January 1 and June 1`
	• `30 8,12 * * 1-5 Run weekdays at 08:30 and 12:30`
	• `0 2 */2 * * Run every other day at 02:00`

View Task Schedule	Click to view the task schedule. The *Task Schedule* dialog box displays a list of scheduled tasks. Click a task to review the task details. For more information, see View task schedules.

6. In the *Tasks* tab, add one or more Tasks.
    a. Click **New Task** to add a Task.
    b. In the *New Task* area that appears, click **Task Type** and select from the available types, as required.

Some task types:

- Have an **Abort on Failure** option. Selecting this option causes the task chain to stop executing on a given machine if it fails on that machine.
- Allow you to select a specific user-defined task, such as Wake-On-LAN, Scripts, and Patch Schedules.
- Run all applicable Tasks on the machine, such as the Managed Installation (MI) and File Synchronization (FS) tasks.

  Also, certain task types, allow you to select a specific user-defined task. Other task types, such as the Managed Installation (MI) and File Synchronization (FS) tasks run all applicable MI or FS tasks on the machine.

  The selected Task appears in the *Tasks* tab.

7. To reorder the Tasks in the Task Chain, in the top-right corner of the task area, click , and drag and drop the Task into a desired place in the sequence.
8. To delete a Task from the Task Chain, in the bottom-right corner of the task area, click .
9. Click **Save**. The Task Status displays the list of tasks.
10. To run a task chain, select it on the *Task Chains* list page, and click **Choose Action** > **Run**.

Patching devices and maintaining security

The appliance enables you to patch managed devices to improve software functionality and protect devices and networks from vulnerabilities.

Using the Security Dashboard

The Security Dashboard provides an overview of patching processes for the selected organization (if applicable), or the appliance.

If the Organization component is enabled on the appliance, and you are logged in to the Administrator Console (`http://`**appliance_hostname**`/admin`), the Security Dashboard shows information for the selected organization.

You can access the Security Dashboard if one or more roles associated with your user account grants access to this dashboard. If you want to hide it, edit your user roles, as needed. For more information, see Add or edit User Roles.

TIP: The appliance updates the summary widgets periodically. To update most of the widgets any time, click the icon and then the **Force Refresh** button. To update an individual widget, hover over the widget, then click the **Refresh** button above the widget. Some widgets may require additional steps.

About the Security Dashboard widgets

Security Dashboard widgets contain information about the overall patch compliance for your managed devices.

This section describes the widgets available on the Security Dashboard. If the Organization component is enabled on your appliance, the widgets show the information for the selected organization at the Admin level.

This dashboard provides an overview of patch compliance in your environment, and the information about patching processes. Use it to quickly review the level of system patches installed on managed devices and look for any indicators that can improve your system security. For example, you can focus on the device patch compliance and review your patching schedules to ensure the latest system updates are installed and running on your managed devices.

Widget	Description
Critical Patch Compliance	This widget shows the deployment progress of patches that are marked as critical. If the Organization component is enabled on your appliance, the widget shows the information for the selected organization.
Dell Updates	This widget displays the number of Dell applications, BIOSs, and firmware updates that can be applied to managed devices. The updates are categorized as *Moderate*, *Important*, or *Critical*, depending on the urgency of the update. After a Dell Update schedule is created, data appears in the widget. See Configure Dell Update schedules. If the Organization component is enabled on your appliance, the widget shows the information for the selected organization.

Widget	Description
Compliance By Machine	This widget displays a donut chart, where each section of the chart indicates the percentage of patch compliance for each managed device. Hovering over each section of the chart displays the percentage of the patch compliance for the selected device. You can change the information that appears in the widget by choosing the patch publisher, operating system, label, classification, severity, KB number, and availability date. You can also switch between any chart type that is applicable. You can also install multiple instances of this widget on the Security Dashboard using a different set of parameters in each instance.
Compliance By Patch	This widget provides a donut chart, where each section of the chart indicates the percentage of compliance for each applicable patch. Hovering over each section of the chart displays the percentage of the compliance for the selected patch. You can change the information that appears in the widget by choosing the patch publisher, operating system, label, classification, severity, KB number, and availability date. You can also switch between any chart type that is applicable. You can also install multiple instances of this widget on the Security Dashboard using a different set of parameters in each instance.
Patch Installation Progress	This widget shows the progress of patching tasks that are running on managed devices. If the Organization component is enabled on your appliance, the widget shows the information for the selected organization.
Patches Deployed	This widget displays the number of patches that are currently deployed. You can change the information that appears in the widget by choosing the patch publisher, operating system, label, classification, severity, KB number, and availability date. You can also switch between any chart type that is applicable. You can also install multiple instances of this widget on the Security Dashboard using a different set of parameters in each instance.
Patches Failed	This widget displays the number of patches that failed to deploy. You can change the information that appears in the widget by choosing the patch publisher, operating system, label, classification, severity, KB number, and availability date. You can also switch between any chart type that is applicable. You can also install multiple instances of this widget on the Security Dashboard using a different set of parameters in each instance.
Patches Released	This widget displays the number of patches that are released and available for deployment. You can change the information that appears in the widget by choosing the patch publisher, operating system, label, classification, severity, KB number, and availability date. You can also switch between any chart type that is applicable. You can also install multiple instances of this widget on the Security Dashboard using a different set of parameters in each instance.
Patching Tasks Completed	This widget shows the progress of patching tasks, such as detect, deploy, and rollback tasks, on managed devices. If the Organization component is enabled on your appliance, the widget shows the information for the selected organization.
Security Reports	This widget contains links to common patching reports. Use them to quickly generate a specific report, such as *Critical and Recent Bulletin List* , *Devices not compliant by patch*, and others.

Widget	Description
Security Views	This widget contains links to common patching pages and wizards, including any custom views that you created. Use them to quickly navigate to specific pages, such as the *Patch Catalog*. If you have any custom views, they are sorted alphabetically. If you want the custom views to appear in a specific order, you can prefix their names with numbers, as needed.
Windows 10 Releases	This widget shows a bar chart, with each item in the chart representing a particular Windows 10 release and the number of managed devices running that version. This can give you an idea of how many devices are candidates for published Windows 10 updates.
Windows 11 Releases	This widget shows a bar chart, with each item in the chart representing a particular Windows 11 release and the number of managed devices running that version. This can give you an idea of how many devices are candidates for published Windows 11 updates.
Device Patch Status Breakdown by CVSS	This widget shows the number of patched and unpatched devices by CVSS severity scores.
Patch Status Breakdown by CVSS	This widget shows the number of patches by patch status and CVSS severity scores.
Patch by CVSS Score	This widget shows the patch counts by CVSS severity scores.
Exposure by CVSS Score	This widget shows the number of unpatched devices and patches by CVSS severity levels.

Customize the Security Dashboard

You can customize the Security Dashboard to show or hide widgets as needed.

1. Go to the *Security Dashboard*.
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.

b. On the left navigation bar, click **Security**, then click **Dashboard**.

2. Hover over the widget, then use any of the following buttons:

   # : Refresh the information in the widget.

   # : Display information about the widget.

   # : Edit the widget.

   # : Remove the widget.

   # : Resize the widget.

   # : Drag the widget to a different position on the page.

3. The widgets are editable, allowing you to filter the information that they display. To edit an editable widget, click and in the dialog box that appears, select the patch publisher, operating system, label, classification, severity, KB number, and availability date. You can also switch between any chart type that is applicable.

4. Click the button in the top-right corner of the page to view available widgets.

   For information on how to add widgets to the dashboard refer Adding Widget to Security Dashboard

Work with the Security Dashboard Settings

When you click the icon, the dashboard settings panel displays. You get to see the following options:

Dashboard Name	Description
Dashboard Settings	You can customize the look and feel of the widgets. For more information, refer Setting a Security Dashboard
Add Widget	You can add a new widget. For more information, refer Adding Widget to Security Dashboard
Email Dashboard	You can share a dashboard snapshot through email. For more information, refer Emailing a Security Dashboard
Force Refresh	You can refresh all the widget data on the dashboard. For more information, refer Refreshing Security Dashboard Data Manually

Setting a Security Dashboard

You can customize the look and feel of the widgets and the dashboards.

You can change the color used in the dashboard charts, edit the dashboard name and its description, change the display of the widgets.

To customize a dashboard,

1. Click the icon to open the Dashboard Settings panel.
2. Make changes to the fields as required:

Fields	Description

Name	Add/Edit name for the dashboard. This is displayed on the dashboard.
Description	Add/Edit description of the dashboard. This describes the dashboard.
Choose Your Colors	Click on the color selector to choose your dashboard chart colors. Drag and drop the colors to arrange them in the desired order. The colors at the top of the list will be used first by each chart.
Layout	Chose one of the layout options. The widgets and other elements are displayed in the selected layout.

3. Click **Save**.

   The changes gets reflected on the dashboard.

Adding Widget to Security Dashboard

You can add widgets to the Dashboard.

There is a list of widgets in the panel. You can enter a keyword in the Search text box to refine the list, then click on your selection.

To add widgets to the dashboard,

1. Click the icon to open the **Add Widget** panel.
2. Search for the desired widget in the following ways:
   - **In the Sort By drop-down, select the widget by title or newest.**
   - **In the Search field, enter a keyword to refine the list.**

   The refined result displays.
3. Click the desired widget.

   The widget gets added to the dashboard.

Emailing a Security Dashboard

You can share a snapshot of dashboard through email, send it to multiple users, and configure the frequency of email.

To email a dashboard,

1. Click the icon to open the dashboard settings panel.
2. Click the Email Dashboard option to open the Email Dashboard panel.
3. Select appropriate option from the given options:
   a. **Send Now**: You can send an email immediately.
   b. **Schedule**: You can set the frequency of sending a snapshot of dashboard through email.

The detailed steps for each option are given below:

Send email now

To send email immediately,

1. Click **Send Now** to open the Email Dashboard dialog.
2. Enter details in the Email Address, Subject, and Message fields.
3. Choose the layout in which you want the widgets to appear.
4. Click Send.

   The dashboard is sent through email.

Schedule

To set the frequency of sending a snapshot of dashboard through email,

1. Click **Schedule** to open the Schedule dialog.
2. Enter details in the Subject and **Message** fields.
3. Choose the layout in which you want the widgets to appear.
4. To add recipients, select the names from the **Select user to add drop down list**.

   NOTE: You can add multiple recipients from the list.

5. Select the frequency from the drop down list.
6. In the **Next Run** field that appears after you select the **Frequency**, set the date, month, and time for the next email delivery.
7. Click Save. The dashboard is sent through email according to the set schedule.

Refreshing Security Dashboard Data Manually

You can refresh the widgets data to show the latest results on the dashboard.

To update the widgets,

1. Click the icon to open the dashboard settings panel.
2. Click **Force Refresh** to open the Confirm dialog box.
3. Click Yes to confirm refresh all widget data on the dashboard.

About patch management

Patch management is the process of obtaining, testing, and installing patches for software on devices. The appliance enables you to automate patch management, which helps to improve software functionality and protect devices and networks from vulnerabilities.

With patch management you can detect and deploy the latest security patches and software updates for Windows and Mac devices that use the appliance.

NOTE: The Patch Management component is supported on Windows and Mac devices only. Patch Management is not available for Linux devices.

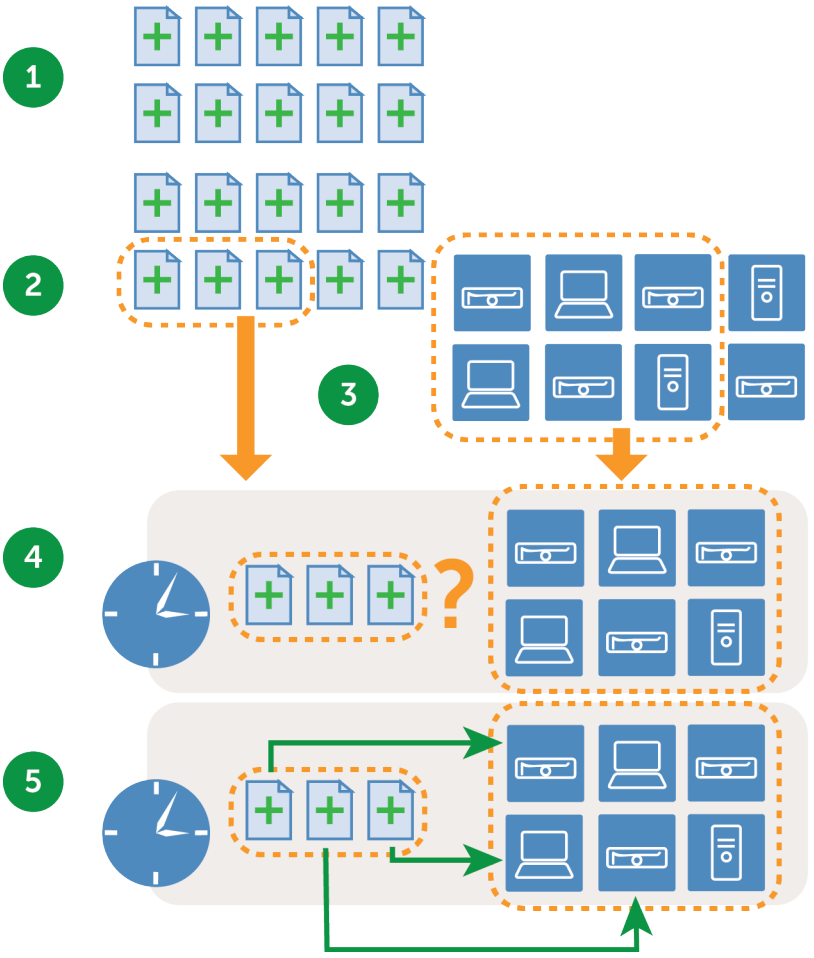
Patching workflow

Patching workflow includes subscribing to patches, selecting patch download settings, using labels to identify patches and the devices to be patched, and scheduling patching jobs.

The patching workflow includes the following tasks.

- Subscribing to the patches that you want to download. If the Organization component is installed on your appliance, you set subscription settings for each organization separately. Additional workflow details are available for first-time patch subscription. See Subscribing to patches and configuring download settings.
- Selecting patch download settings on the *Patch Subscription Settings* page. See Select patch and feature update download settings.
- Creating Smart Labels to group devices for patching and patches for deployment. See Using Smart Labels for patching.
- Creating patching schedules to detect and deploy packages. If the Organization component is installed on your appliance, you create patch schedules for each organization separately. See Configuring patch schedules.

Figure 11. Patching workflow



Legend number	Action
1	Signature files for patches you subscribe to are downloaded to the appliance from Quest. Patch packages are downloaded from Quest and from software vendors.
2	Smart Labels group the downloaded patches.
3	Smart Labels select devices to patch.

Legend number	Action
4	Patches needed by the devices are detected according to a schedule.
5	Patches are deployed to devices according to a schedule.

About patch signature files

Patch signature files include the security bulletins and other files that define patches; they do not include the patch packages that are used to install patches.

Patch signature files are downloaded from Quest according to the subscription and download options you select. For more information on downloading patch signature files, see Select patch and feature update download settings.

About patch packages

Patch packages are the files required to install patches.

Patch packages are downloaded from Quest according to the subscription and download options you select. In some cases, patch packages are also downloaded directly from vendors, such as Microsoft and Adobe.

There are two options for downloading patch packages:

- **Downloading only those patches that you need**: You can choose to download only those packages that have been detected as required by managed devices. Downloading this way reduces download time and disk space. In addition, you can choose to automatically remove patches after a specified time if detect results show that the patches are not needed.
- **Maintaining a full cache of patches**: You can choose to maintain a full cache of packages regardless of whether the patches are required by managed devices. This method keeps packages available for quick deployment, but it requires more download time and disk space than downloading only those packages that you need.

For more information about package download options, see Select patch and feature update download settings.

About patch testing and security

Quest provides safe, timely, and high-quality patch signatures for Windows and Mac operating systems, and many popular applications.

Before patch signatures are made available to the appliance, Quest performs the following security checks:

- Verification of patch metadata produced by each content development team.
- Validation of patch installation and uninstallation processes.
- Confirmation that the patch does not disrupt the stability of the targeted operating systems and applications.

About the patch testing environment

Quest uses VMware® ESX®, VMware® vCenter™, Microsoft® Azure®, and custom hardware bench testing.

Testing methods include verification that patch-naming conventions comply with Quest policies.

About assessment testing

Assessment testing verifies that the Patch Management component is performing properly.

The testing verifies that:

- An applicable non-patched device shows as applicable and not patched.
- A patched device shows as installed and not applicable.
- No false positives exist in the detection of the digital fingerprint.
- Patch content is compliant with mandatory baselines.
- Vulnerability is correctly displayed in the Update Server.
- All Smart Label, sorting, and other visual features are functioning properly.

About deployment testing

Deployment testing verifies that patches are being deployed appropriately.

The testing verifies that:

- The package is deployable.
- The suppress-reboot functionality works.
- The uninstallation functionality works.
- On-demand package caching works.
- Automatic deployment scheduling works.
- Agent package download works.
- SHA1 checksum ensures package integrity.
- The Agent automatically runs assessment after patch deployment.
- The Agent restarts automatically after reboot.

About the patch quality assurance process

Quest provides Patch Management customers more value through the content development and quality assurance processes. The quality assurance teams verify the patch install and uninstall processes as well as the patch metadata produced by the content development team. Providing quality content to our customers is a high priority. To ensure successful delivery of content, Quest executes test cases covering the following test components.

Testing environment

Quest invests heavily in testing infrastructure. The content development and quality assurance teams have access to a virtual enterprise environment representing nodes of various configurations. Quest uses a mix of virtual desktops and servers in addition to custom physical bench testing to ensure that our testing infrastructure is state of the art.

Application testing

Quest tests with various applications as necessary to ensure the requirements of the patch are satisfied.

Testing strategy

Quest uses the following types of testing:

- **General testing** verifies the following:
  - # Patch-naming convention complies with the Quest policies.
- **Assessment testing** verifies the following:
  - # An applicable non-patched system shows applicable and not patched.
  - # An patched system shows installed and not applicable.
  - # False positives in the detection of digital fingerprint.
  - # The content complies with mandatory baselines.
  - # The patch is correctly displayed in Patch Server, including all filtering, sorting and other visual functionality.
- **Deployment testing** verifies the following:
  - # The package can be successfully deployed.
  - # The suppress reboot functionality works correctly.
  - # The uninstall functionality works correctly.
  - # On-demand package caching works correctly.
  - # Automatic deployment scheduling works correctly.
  - # Agent package downloads.
  - # The package hash ensures the package integrity.
  - # The agent automatically runs assessment after each patch deployment.
  - # The agent restarts automatically after a reboot.

Trusted delivery and flexibility

Quest processes are designed and implemented to maximize global availability through a secure content distribution network. All communications with Quest are conducted through encrypted, secure channels to ensure the integrity of security content.

Using a best practice approach, critical security patches are automatically downloaded to customer locations, based on their subscription options. Additional security patches may be downloaded, as necessary, to create a customized version of the KACE Patch Content Repository within the customer's own secure enterprise environment.

Best practices for patching

Best practices for patching devices include testing patches, using labels to organize devices and patches, and notifying users when systems are being patched.

- **Test patches before deploying them**

  Test patches on selected devices before deploying them to all devices. This testing ensures that patches do not break anything before they are widely deployed.
  When choosing test devices, look for these characteristics:

  - # Devices whose users are technically sophisticated and can communicate problems effectively.
  - # Devices that have access to the systems and software that reflect the working environment.

  For a thorough test, devices should function normally for at least a week after being patched. If no problems are reported after a week, the patch can be deployed to the remaining devices on the network.

- **Use labels to organize devices and patches**

You can use Smart Labels to automatically group devices by type, such as laptop, desktop, and server. In addition, you can use Smart Labels to automatically group patches by importance, such as critical operating system patches and lower priority patches for other applications. You can then create patching schedules to match each type of device and patch.
See:

Using Smart Labels for patching

Creating and managing patch schedules

- **Use either Windows Update or the appliance to patch Windows devices**

There are two options for patching Windows devices:

Use Windows Feature Update: Windows Update is a Microsoft feature that downloads and installs updates to Windows operating systems. If you enable Windows Update on managed devices, use Patch Management on the appliance only to detect Windows operating system patches, not to deploy them. Patches will be deployed by Windows Update.

Use the Patch Management: You can download and deploy patches for Windows operating systems using Patch Management. If you use Patch Management on the appliance, disable Windows Update on managed devices, because patches will be deployed by the appliance.

TIP: The appliance enables you to create a policy that specifies whether or not managed devices use Windows Update. See .

- **Minimize downtime during patching**

Schedule patch deployment during periods when device use is lower to minimize downtime. Keep in mind that device use varies depending on the device type:

Servers: These require careful and well-publicized upgrades. When patching servers, you might need to plan ahead by several weeks.

Desktops: These have more flexible options for patching, because they are often left running when they are not in use.

Laptops: These are the most difficult to patch, because they are often only available to patch while being used.

For more information about creating patch schedules for each type of device, see:

About scheduling critical OS patches for desktops and servers

About scheduling critical patches for laptops

- **Notify users when devices are being patched**

Be sure to notify users when the devices they use are being patched. This is especially important if devices need to be restarted as part of the patching process. There are several ways to inform users of patching schedules:

Send email or use other messaging systems: Notify users in advance through email and other messaging systems outside the appliance **Administrator Console**. This notification is especially useful when patching might prevent access to critical systems, such as servers, for a time.

Send an alert message from the appliance: Use the appliance **Administrator Console** to create an alert and broadcast it to all devices or to selected devices. These broadcast alerts can be used to remind users that patching is about to start.

For more information on creating alerts, see Broadcasting alerts to managed devices.

Provide alerts during patching: When you schedule patching, choose to alert users before patching, and prompt users before rebooting their devices. You can also enable users to snooze or postpone reboots if necessary. See Configuring patch schedules.

For more information about scheduling patching for various devices, see:

About scheduling critical OS patches for desktops and servers

About scheduling critical patches for laptops

- **Set time limits on patching jobs to reduce impact on users**

  Patching jobs can require extensive bandwidth and resources. To reduce the impact on users, you can set time limits on patching jobs. For example, you could configure patching jobs to start at 04:00 and stop at 07:00. Any patching jobs that are in progress at 07:00 are suspended. Jobs resume where they left off when the next scheduled patching job begins. See Configuring patch schedules.

- **Use Replication Shares to optimize network resources**

  Use Replication Shares to optimize network resource requirements and download time. Replication Shares are devices that keep copies of files for distribution, which can be useful for managed devices that are deployed across multiple geographic locations. For example, using a Replication Share, a device in New York could download patch files from another device at the same office, rather than downloading those files from an appliance in Los Angeles.
  For more information on setting up and using Replication Shares, see Using Replication Shares.

- **Find information on the Quest Knowledge Base**

  Quest Support has a Knowledge Base of articles about the appliance, which you can access at https://support.quest.com/kace-systems-management-appliance/kb. The Knowledge Base is continually updated with solutions to real-world appliance problems that administrators encounter. To view patching articles, go to the Knowledge Base and search for *Security*.

Subscribing to and downloading patches

To enable patching, you need to subscribe to patches and schedule patch downloads to the appliance.

About patch subscription and downloads

Patch subscription is the process of selecting the operating systems and applications for which you want to receive patches.

If the Organization component is enabled on your appliance, you select subscription settings for each organization separately.

After you subscribe to patches, the appliance downloads them according to the schedule you set. When patches are downloaded, you can test and deploy them. You can choose to automatically deploy patches as well, but such deployment is recommended for low-risk or time-important patches only. See:

- Select patch and feature update download settings
- Using Smart Labels for patching

Applications that the appliance can patch

For a list of applications that the appliance can patch, go to https://support.quest.com/kb/112030, and open the attachment.

NTP service requirement

When downloading patches using HTTPS, the NTP (Network Time Protocol) service must be running on the appliance. The NTP service is required because the secure protocol uses the current date stamps from the appliance to ensure certificate validity. If the NTP service is not running, patch download failures, suggesting invalid certificates, might result.

Websites that must be accessible to the appliance

To complete patch downloads, access product information, and interact with **Quest Support**, the firewall, DNS server, and proxy server settings must allow the appliance to access specific domains on both port 80 and port 443.

Refer to the link for the websites that must be accessible to the appliance:

https://go.kace.com/to/k1000-network-ports-url-whitelist

Overview of first-time patch-subscription workflow

Patch detection signatures and patch packages are not downloaded to the appliance by default. You must subscribe to the patches you want and then schedule a time to download them.

To save network bandwidth and disk space, Quest recommends that you download patch definition signatures first, because they are much smaller in size than patch packages. Then you can detect the patches that you need, and select the download settings that work best for your network.

The following workflow is for first-time patch-subscription.

1. **Gather information**: Identify the operating systems, language packages, and applications installed on managed devices so that you know what you need to subscribe to. You can find this information on the appliance *Dashboard* page as well as by running reports. See View details about operating systems and applications.
2. **Select initial patch subscription settings**: Subscribe to the operating systems and languages required by managed devices. See Subscribing to patches and configuring download settings.
3. **Download patch detection signatures**: Patch detection signatures are smaller files that can be downloaded quickly and do not require much disk space. Download the patch detection signatures of the patches you subscribe to. Downloading these signatures enables you to view available patches and identify the patch packages you want to download later. See Select patch and feature update download settings.
4. **Run a detect-only patching job**: Schedule a Detect-only patching job to identify the patches required by managed devices. A detect-only patching job is a one-time operation that shows how large the first patching job is going to be. Also, it indicates how to allocate resources based on device availability for patch installations and reboots. To run a detect-only patching job, create a patching schedule that detects patches on all devices. See Configuring patch schedules.
5. **Select patch package download settings**: After you have identified the patch packages that you need, set a time for package downloads to occur. See Select patch and feature update download settings.

View details about operating systems and applications

You can view information about the operating systems and applications installed on managed devices on the *Summary Detail* page.

Before you subscribe to patches, gather information about the operating systems, language packages, and software installed on managed devices so that you know what subscriptions you need.

1. Do one of the following:
   - **If your appliance has the Organization component enabled, and you want view information for the appliance, log in to the System Administration Console: `http://appliance_hostname/system`, or select System from the drop-down list in the top-right corner of the page.**
   - **If your appliance does not have the Organization component enabled, or if you want to view organization-level information, log in to the Administrator Console : `http://appliance_hostname/admin`. Or, if the *Show organization menu in admin header* option is enabled, select an organization in the drop-down list in the top-right corner of the page next to the login information.**
2. Click **Home** to display the *Dashboard* page.
3. In the top-right corner of the page, click **View Details**.

   The *Dashboard Detail* page appears. The *Devices* section shows the operating systems of managed devices for the appliance or for the selected organization.
4. In the *Software* section, click **Software Titles**.

The appliance runs a report that displays the software installed on managed devices. See About reports.

Subscribing to patches and configuring download settings

To establish a patching workflow, you can subscribe to patches and configure patch download settings.

Subscribe to patches

You can subscribe to patches for the operating systems and applications on your managed devices.

Before you subscribe to and download patches, identify the operating systems and applications installed on managed devices, and verify patching requirements. See View details about operating systems and applications.

1. Go to the *Patch Subscription Settings* page:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Security**, then click **Patch Management**.
   c. On the *Patch Management* panel, in the **Subscriptions** section, click the **Define available patches** link .
2. The *Patch Status* tab provides several details about the latest patch download and appliance disk space. Here you can also determine if newly downloaded patches should be marked as active or inactive by default.

Option	Description
Activate New Patches	Mark new patches as Active. This setting enables patches that match your subscription settings after every download. If this option is not selected, new patches are marked as Inactive. This enables you to test patches before they are deployed.

3. Specify the settings in the *Subscription* tab. The operating systems and locales specified in the subscription control the patches that are downloaded.

Option	Description
Windows Operating Systems	Download patches for the selected Windows operating systems. Click the edit button to manage the list of operating systems: . Select **All Windows in Inventory** to select the Windows operating systems based on managed devices. To ignore Windows operating system patches, select **Disabled**. Or, select the check boxes next to one or more Windows operating systems. Selected items are displayed after you save the settings.
Mac Operating Systems	Download patches for the selected Mac operating systems. Click the edit button to manage the list of operating systems: . Select **All Mac in Inventory** to select the Mac operating systems based on managed devices. To ignore Mac operating system patches, select **Disabled**. Or, select the check boxes next to one or more Mac operating systems. Selected items are displayed after you save the settings.
Locales	Download patches for the selected languages. Click the edit button to manage the list of locales: . Select **All Locales** to download patches regardless of the locale or select the check boxes next to one or more locales. Selected items are displayed after you save the settings.

NOTE: At least one operating system and one locale must be selected for a patch subscription.

4. Specify the *Application Patches* settings. These settings are used to determine the patch status once the patch files are downloaded. This can be active, inactive or disabled.

Option	Description
Publishers	Subscribe to applications patches based on its vendor. Click the edit button to manage the selected types: . Select **All Publishers** to select patches from all available publishers. Or, select the check boxes next to one or more publishers. Selected items are displayed after you save the settings.

5. Specify the subscription's *Advanced Options*.

Option	Description
Classification	Click and select a type of this subscription. You can choose to select **All Classifications**, to make it **Disabled**, or click **Select Classification**, and choose one or more of the existing values, as applicable: **Critical Updates**, **Definition Updates**, **Feature Packs**, **Full Software**, **Hotfix**, **Security Updates**, **Service Packs**, **Tools**, **Update Rollups**, **Updates**, and **Upgrades**.
Severity	Click and select a severity of this subscription. You can choose to select **All Severities**, to make it **Disabled**, or click **Select Severity**, and choose one or more of the existing values, as applicable: **Critical**, **Important**, **Low**, **Moderate**, and **Recommended**.
Labels	Download only those patches that match the selected labels. Click **Manage Associated Labels** to select the labels. This refinement is important when disk space is limited. If the total disk space required for selected patches exceeds the space available on the appliance, patches cannot be downloaded.

Option	Description
	NOTE: Appliance disk space information appears in the *Patch Status* section at the top of the page.
Disable Windows Embedded Patches	Identify and disable any embedded Windows patches. When this option is selected, the signatures for embedded patches are downloaded, but they cannot be deployed unless they meet the subscription criteria.
Inactivate Superseded Patches	Mark patches that have been superseded to the *Inactive* state after every download. Inactive Superseded Patches are identified with **Inactive** on the *Patch Catalog* page.
Detect Disabled Patches	Enable the appliance to identify disabled patches when it runs a Detect job. If this option is selected, the signatures for disabled patches are downloaded for detection purposes only. Patches cannot be deployed unless they meet the subscription criteria.

6. Click **Save**.

Selected patches are downloaded automatically at the next scheduled download time. If a patch does not match the subscription settings after download, it appears as **Disabled**. If a patch matches the subscription settings but it is either superseded or manually set to inactive, the state appears as **Inactive**.

Select patch and feature update download settings

The patches and Widows Feature Updates you subscribe to are downloaded to the appliance according to the settings you choose.

Be aware that the first patch download might use a large amount of network bandwidth.

1. Go to the *Patch and Feature Update Download Settings* page.
   - **If the Organization component is not enabled on the appliance, on the left navigation bar click *Security*.**
   - **If the Organization component is enabled on the appliance, log in to the appliance System Administration Console, `https://appliance_hostname/system`, or select System in the drop-down list in the top-right corner of the page, then select Settings > Control Panel.**
2. In the *Patch and Feature Update Download Settings* section, click the *Configure File Downloads* link.
3. In the *Configure File Downloads* tab, select the following options.

Option	Description
Patching	• **Disabled**: Prevents the downloading of patch packages. This prevention includes the installers that are required to install the patches. • **All subscribed files**: Maintains a full cache of subscribed packages on your appliance. This option downloads all deployment packages to which you subscribe, without checking to determine whether they are required for your environment. It is important for some environments to maintain a full cache. For example, if you select the **Offline Target** or **Online Source** option, full caching is required. • **Files detected as missing**: Allows the appliance to determine which packages to download based on the results of Detect jobs. If a patch detection signature has been detected as Not Installed on any managed device, the patch package is downloaded.

Option	Description
	If no managed devices are detected as Not Installed, no packages for this patch are downloaded.
Feature Updates	• **Disabled**: Prevents the downloading of Windows Feature Updates. This prevention includes the installers that are required to install the patches. • **Files detected as missing**: Allows the appliance to determine which packages to download based on the results of Detect jobs. If a Feature Update signature has been detected as Not Patched on any managed device, the Windows Feature Update package is downloaded. If no managed devices are detected as Not Updated, no packages for this Windows Feature Updates are downloaded.
Delete unused files after __ days	Deletes patches and Windows Feature Updates that have not been deployed in the specified number of days. Patches and Windows Feature Updates that are marked as *Inactive* or *Disabled* are automatically deleted during the patch download process.

4. In the *Configure Offline Update* tab select the following options.

Option	Description
Offline Update	The action to take if the appliance is offline when the update process is scheduled to start. Clear the *Offline Update* option if the appliance is expected to be connected to the internet and can download patches or Windows Feature Updates directly.
Offline Target	The Offline Target to use if the appliance is not connected to the internet, and you want to upload the patch and Windows Feature Update files from a local directory. If you have a appliance that is connected to the internet, you can configure that appliance as an Offline Source. Then you can manually copy the patch files from the Offline Source Patches file share to the following directory on the Offline Target: `\\`**appliance_host**`\patches`. Click **Upload** to load patch TAR files.
Online Source	Whether the appliance is used as a source for a different appliance. When this option is selected, patch files are downloaded to the appliance's Patch and Windows Feature Update file share.

5. In the *Actions* tab, select the following options.

Option	Description
Update Description Actions	For each type of updates (*Signature*, *Feature Update Files*, *Patch Files*), it provides a description and access to the available actions: • **Check for Update**: Click to download patch signature files. • **Delete**: Click to immediately remove all patches or Windows Feature Updates from the appliance. This can be useful if you no longer need any patches and you want to quickly reclaim the disk space that they used. • **Run Now**: Click to immediately download the patches or Windows Feature Updates to which you have subscribed, regardless of the subscription schedule.

6. Select schedule options for patch and Windows Feature Update signatures in the *Schedule* section. File signatures include the security bulletins and other files that define patches and Windows Feature Updates downloaded from Quest.

Option	Description
Signature Download	Select **None** to prevent the downloading of patch and Windows Feature Update signatures.
Every __ hours	Downloads signatures at a specified interval. Use caution when specifying frequent intervals (4, 8 or 12 hours), because this can increase bandwidth requirements.
Every day at the specified time	Select **day** to download patch or Windows Feature Update detection signatures every day, or select a day of the week to download once a week. Select the time to start the download. Time is displayed in 24-hour clock format, where 0 is midnight, 1:00 a.m. is 1 and 11:00 p.m. is 23. **NOTE:** When setting up patch or Windows Feature Update downloads, timing is important. The appliance activity log is created at 1:30, and maintenance tasks occur between 01:00 and 01:30. Quest recommends that you schedule downloads to occur after the log and maintenance tasks are complete, which is about 3:00.
On the nth of every month or on a specific month at HH:MM	Select the day of the month to download patch or Windows Feature Update detection signatures on a monthly basis.

7. Set the *Schedule* options for feature update and patch files.

Option	Description
After signature download	Downloads packages after the signatures have been downloaded. This option is not available if **Patching** is disabled in the *Configure File Downloads* section.
Every __ minutes	Specifies the frequency with which packages are downloaded. This option is available only if *Files detected as missing* in the *Configure File Downloads* section is selected.
Download Blackout: Start __ End __	Specifies a time period during which files cannot be downloaded. For example, use an early morning stop time to prevent the process from using a large amount of network bandwidth during regular working hours. If you select this option, the appliance stops file downloads at the specified time. It does not start file downloads again until the next specified download time. When the download resumes, it starts up where it left off. Downloads that are incomplete might not appear on the *Patch Catalog* or *Windows Feature Update Catalog*page.

8. Click **Save**.

To schedule patch detection and deployment for managed devices, see Creating and managing patch schedules. To schedule Windows Feature Update detection and deployment for managed Windows 10 devices, see Configure Windows Feature Update schedules.

Viewing available patches and download status

You can review the available patches and set appropriate patch download filters to download only the patches you need.

For example, once the patch packages are downloaded, you can set a filter to view patches based on category; view Operating System patches only.

View available patches

After you have subscribed to patches, and the patches have been downloaded, you can view available patches.

You must subscribe to patch detection signatures and select patch download settings to view patches. See:

- Subscribe to patches
- Select patch and feature update download settings

1. Go to the *Patch Catalog* list:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Security**, then click **Patch Management**.
    c. On the *Patch Management* panel, click **Display available patches** under **Catalog**.
2. Search for application patches.
    a. Click the **Filter** tab above the list on the right to display the *Filter* panel.
    b. Enter search criteria:

        `Patch Listing Information: Category | is | Application`

    c. Click **Search**.

View patch download status

After you have subscribed to patches, you can view patch download status.

You must subscribe to patches to view patch download status. See Subscribe to patches.

1. Go to the *Patch Catalog* list:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Security**, then click **Patch Management**.
    c. On the *Patch Management* panel, click **Display available patches** under **Catalog**.
2. Do one of the following:
    - **In the *View By* drop-down list, which appears above the table on the right, select Download Status > Downloaded or Download Status > Not Downloaded.**
    - **Click the Filter tab, which appears above the table on the right, then select search criteria. For example:**

        `Patch Listing Information: Download Status | is | Downloaded`

See Viewing patch information.

Best practices for resolving patch subscription issues

Occasionally you may see an error message indicating that your patch subscription license has expired:

The error message

`Your patch subscription has expired. Please contact support for assistance.`

Before engaging the KACE support, you can take some preliminary steps to resolve the issue.

This error may be caused by one of the following issues:

- In most cases, it happens when your license key has passed its three year validation period.
- A new license key is provided, but the account may not be synchronized yet with the KACE database.

If a new key has been requested but not yet delivered:

Ensure the following email message has not been stopped by a spam filter. This is the message format of the new license key notification sent by the KACE licensing team:

```
Sender: license@quest.com

Subject: KACE Systems Management Appliance License Number for (PO# <PO number>)
order# <order number>
```

If a new key has been applied but the error persists:

1. Validate your product license:
   a. Go to the appliance *Control Panel*.
      # If the Organization component is not enabled on the appliance, click **Settings**.
      # If the Organization component is enabled on the appliance, log in to the appliance **System Administration Console**, `http://`**appliance_hostname**`/system`, or select **System** in the drop-down list in the top-right corner of the page, then click **Settings**.
   b. On the left navigation bar, click **Appliance Updates** to display the *Appliance Updates* page.
   c. On the right of the *License Information*, click ⓘ.
   d. Select *Validate License*, then click **Yes** to confirm.

      TIP: For complete information about this page, see Update the appliance license key.

2. Perform a manual patch signature download.
   a. Go to the appliance *Patch Download Settings* page.
      # If the Organization component is not enabled on the appliance, click **Settings**.
      # If the Organization component is enabled on the appliance, log in to the appliance , `http://`**appliance_hostname**`/system`, or select **System** in the drop-down list in the top-right corner of the page, then click **Settings**.
      # Go to **Security** > **Patch Management** > **Patch Download Settings**.
   b. Click **Run Now**. After the patch download is completed, the error message disappears.

      TIP: For complete information about this page, see Select patch and feature update download settings.

If you completed the above step, but the issue remains:

1. Go to https://support.quest.com/create-service-request and create a new service request (SR).

2. Provide the answers to the following questions in the request:
   # When did the issue start for the first time?
   # Did something change before the issue?
   # Verify and confirm the issue in the patch download log. Document the findings in the SR or upload the log files into the SR.
   # Which license key is currently in use? The complete license key is required. If this is not possible, the last five characters are acceptable.
   # If available, what is the old (previous) license key?
   # What is the static IP Address of the appliance?
   # What is the MAC Address of the appliance?
3. Upload your appliance log files as an attachment to the SR.
   a. Go to the appliance *Control Panel*.
      # If the Organization component is not enabled on the appliance, click **Settings**.
      # If the Organization component is enabled on the appliance, log in to the appliance **System Administration Console**, `http://`**appliance_hostname**`/system`, or select **System** in the drop-down list in the top-right corner of the page, then click **Settings**.
   b. On the left navigation bar, click **Support**.
   c. In the *Troubleshooting Tools* section, click **Retrieve appliance activity logs**.
   d. Click **Save File** to download the logs.

NOTE: Clear your browser's cache after encountering an error situation during a patch download. Failing to do so may prevent the appliance from downloading patches after this error is encountered.

Creating and managing patch schedules

You can manage patch schedules that detect, deploy, and rollback the patches to which you subscribe.

For information on subscribing to patches, see Subscribing to and downloading patches.

About scheduling critical OS patches for desktops and servers

You can configure the appliance to install critical OS patches on desktops and servers according to a schedule.

Desktops are usually less crucial than servers and less mobile than laptops, so it is easier to schedule a time to patch them. Usually, you can schedule routine updates for the early morning hours before users arrive.

Servers run critical services that your organization requires. Schedule patching for servers in advance, and warn users of the temporary service outages that patching requires. Push server patches in the early morning hours or other times when the fewest number of users require the server resources.

Workflow for critical OS patches for desktops and servers

The workflow includes identifying devices, identifying patches, scheduling actions, and deploying patches.

- **Identify desktops**: Create a Smart Label that identifies all devices that are desktops. This excludes servers and laptops. See Add a Smart Label for desktops.
- **Identify servers**: Create a Smart Label that identifies all servers. See Add a Smart Label for servers.
- **Identify critical OS patches**: Create a Smart Label that identifies all critical OS patches. See Add a Smart Label for critical OS patches.
- **Schedule detect and deploy actions**: Schedule a detect and deploy job that identifies whether the devices in the Smart Label need to be updated, deploys critical patches to them, and forces a reboot if required. See Configuring patch schedules.
- **Deploy patches individually to servers**: Schedule a job that deploys patches to servers as needed. See Configuring patch schedules.
- **Notify users**: When you schedule patching, be sure to notify users of the schedule so that they know when the devices they use are being patched. This is especially important if devices need to be restarted and might be unavailable as part of the patching process. You can notify users by sending email and other messaging services outside the appliance Administrator Console. See Best practices for patching.

About scheduling critical patches for laptops

Because laptops are often powered off or disconnected from the network, it can be difficult to find a good time to patch them. The two most popular choices for patching laptops are at the start of the business day or during lunch time.

Most Quest KACE customers patch laptops using two schedules, one for detecting and one for deploying.

Workflow for critical patches for laptops

The workflow for applying critical patches to laptops includes identifying devices, identifying patches, scheduling actions, and deploying patches.

Setting up automatic detect and deploy actions consists of the following workflow:

- **Identify critical patches**: Create a patch Smart Label to automatically identify critical patches for laptops. See Using Smart Labels for patching.
- **Schedule Detect actions**: Create and run a schedule to periodically detect critical patches on laptops. See Configuring patch schedules.
- **Schedule Deploy actions**: Create and run a schedule to periodically deploy critical patches on laptops. See Configuring patch schedules.
- **Check patching status**: Periodically check patching status using reports and the patch. See Viewing patch schedules, status, and reports.
- **Notify users**: Notify users of the patching schedule. You can notify users by sending email and other messaging services outside the appliance **Administrator Console**. See "Notify users when devices are being patched" in Best practices for patching.

About scheduling non-critical patches

You can configure the appliance to install non-critical patches according to a schedule.

To schedule non-critical patches:

- **Detect patches**: Create a patching schedule to detect patches on all devices to determine the size of the patching job. See Configuring patch schedules.
- **Inactivate patches**: If there are patches you do not want to deploy, mark them as **Inactive**.
- **Test patches**: Create a schedule to detect and deploy patches to your test devices. See Configuring patch schedules.
- **Identify patches for desktops and servers**: Create a patch Smart Label to automatically capture the patches to deploy on servers. See Using Smart Labels for patching.
- **Detect and deploy desktop and server patches** (see Configuring patch schedules):
  # Create a schedule to periodically detect and deploy patches on your desktops.
  # Create a schedule to periodically detect and deploy patches on your servers.
- **Detect and deploy laptop patches** (see Configuring patch schedules):
  # Create a schedule to periodically detect patches on your laptops.
  # Create a schedule to periodically deploy patches on your laptops.
- **Check patching status**: Periodically check the patching status. See Viewing patch schedules, status, and reports.

Configuring patch schedules

You can create and configure patch schedules and set a time for them to run. Patch schedules do not interfere with Managed Installations or other distributions.

Fields in the Patch Schedule Detail pages

Fields in the *Schedule Detail* wizard and the *Schedule Detail* page enable you to configure and schedule patch actions.

General Information Tab

Option	Description
Name	A name that identifies the schedule. This name appears on the *Patch Schedules* page.
Description	A brief description of the patch schedule.

Action tab

The action associated with the patch schedule.

The patch action behavior is dependent on the combination of reboot, detect, deploy, and rollback selections you make. Whenever a patch action does both a Detect pass and something else, as is the case with Detect and Deploy and Detect and Rollback, the action is repeated cyclically until the Detect action finds no further patches to deploy or roll back. This behavior might result in multiple Reboot actions for a single scheduled run. In addition, the type of device you are patching affects the type of patch action to use.

The following actions are available:

- **Detect**: Detects patches that are installed on, or missing from, managed devices. Detect-only actions are recommended when the *Patch Download Settings* are configured to download only . Running a detect-only action before the deploy creates a list of patch files to download before deployment begins.
- **Detect and Stage**: Detects patches that are installed or missing from managed devices, and downloads patch files to the agent device for later deployment.
- **Detect and Deploy**: Detects and deploys patches to managed devices. These types of actions are used when managing desktops and servers. Detect and Deploy patching jobs require a connection between the device and the appliance; they do not run offline. For more information about messaging protocol connections, see Configure Agent communication and log settings.
- **Detect, Stage and On-demand Deploy**: Detects patches that are installed or missing from managed devices, downloads patch files to the agent device, and causes the Windows system tray on the agent device to alert the user that the patches are ready for deployment. The user can then initiate the deployment process at their convenience.

  # These schedules are only available for Windows devices with agents version 11.0 or later.

  # The *Agent Status Icon On Device* option must be enabled in the agent communication settings. You can find these settings on the *Organization Detail* page, under *Communication and Agent Settings* (if one or more Organization components are enabled), or on the *Communication Settings* page (if you do not have an Organization component). For more information, see Configure Agent communication and log settings.

- **Deploy**: Deploys applicable patches to managed devices. This is useful when you know that specific patches need to be deployed to managed devices. A final Detect job runs either after the patch is deployed or, if a reboot is required, after the device reboots and the Agent reconnects to the appliance.
- **Detect and Rollback**: Detects and removes unwanted patches from managed devices. Rollbacks may not be available for some patches. See Determine whether a patch can be rolled back.
- **Rollback**: Removes unwanted patches from managed devices. Rollbacks may not be available for some patches. See Determine whether a patch can be rolled back.

Detect section

Option	Description
All Patches	Detect all available patches. This process can take a long time. Also, it might detect patches for software that is not installed on, or required by, managed devices. For example, if managed devices use anti-virus applications from only one vendor, you might not need to detect patches for all anti-virus vendors. *All Patches*, however, detects all missing patches regardless of whether they are required by managed devices. To refine patch detection, set up labels for the patches you want to detect, then use the *Patch Labels* option.
Patch Labels	Restrict the action to the patches in the labels that you select. This is the most commonly used option. 1. Click **Manage Associated Labels**. 2. In the *Select Labels* dialog box that appears, drag one or more labels (as applicable) to the *Limit Detect to* area, then click **OK**. To use this option, you must already have Smart Labels for the applicable patches. See Using Smart Labels for patching.
Select from suggested criteria	Select a patch using a pre-defined criteria. This allows you to focus on a specific type of patches based on your OS. For example, you can choose the critical Windows patches issued in the past 30 days. 1. Click **Select from suggested criteria**.

Option	Description
	2. In the *Select Suggested Criteria* dialog box that appears, click **Select Suggested Criteria**, then click **Save**.
Detect Timeout	The amount of time, in hours, for the patching action to complete.

Deploy section

Option	Description
All Patches	Deploy all patches to the selected devices.
Patch Labels	Restrict the action to the patches in the labels that you select. This is the most commonly used option. 1. Click **Manage Associated Labels**. 2. In the *Select Labels* dialog box that appears, drag one or more labels (as applicable) to the *Limit Deploy to* area, then click **OK**. To use this option, you must already have Smart Labels for the applicable patches. See Using Smart Labels for patching.
Select from suggested criteria	Select a patch using a pre-defined criteria. This allows you to focus on a specific type of patches based on your OS. For example, you can choose the critical Windows patches issued in the past 30 days. 1. Click **Select from suggested criteria**. 2. In the *Select Suggested Criteria* dialog box that appears, click **Select Suggested Criteria**, then click **Save**.
Maximum Deploy Attempts	The maximum number of attempts the appliance deploys or rolls back the patch. Specify a number between one '1' and ten "10". If you specify zero '0', the deployment or rollback does not run. A value higher than ten "10" results in an error message. As a last step in patch deployment or rollback, the appliance verifies whether the patch was deployed or rolled back successfully. If a deployment or rollback fails, the appliance attempts to deploy or rollback the patch again until one of the following occurs: • The deployment or rollback succeeds. • The maximum number of attempts is reached. • The scheduled deployment or rollback period ends and patching is suspended.
Deploy Timeout	The amount of time, in hours, for the patching action to complete.

Rollback section

Option	Description
All Patches	Roll back all patches on the selected devices.
Patch Labels	Restrict the action to the patches in the labels that you select. This is the most commonly used option. 1. Click **Manage Associated Labels**. 2. In the *Select Labels* dialog box that appears, drag one or more labels (as applicable) to the *Limit Rollback to* area, then click **OK**.

Option	Description
	To use this option, you must already have Smart Labels for the applicable patches. See Using Smart Labels for patching.
Select from suggested criteria	Select a patch using a pre-defined criteria. This allows you to focus on a specific type of patches based on your OS. For example, you can choose the critical Windows patches issued in the past 30 days. 1. Click **Select from suggested criteria**. 2. In the *Select Suggested Criteria* dialog box that appears, click **Select Suggested Criteria**, then click **Save**.
Maximum Rollback Attempts	The maximum number of attempts, between 0 and 99, to indicate the number of times the appliance tries to deploy or rollback the patch. If you specify 0, the appliance attempts to deploy or rollback the patch indefinitely. As a last step in patch deployment or rollback, the appliance verifies whether the patch was deployed or rolled back successfully. If a deployment or rollback fails, the appliance attempts to deploy or rollback the patch again until one of the following occurs: • The deployment or rollback succeeds. • The maximum number of attempts is reached. • The scheduled deployment or rollback period ends and patching is suspended.
Deploy Timeout	The amount of time, in hours, for the patching action to complete.

On-demand Deployment Timeout Settings section

Option	Description
Automatically Deploy After	The amount of time after which the deployment takes place if the agent device does not receive any input from the user.

Devices section

Option	Description
All Devices	To apply this schedule to all managed devices, select this options. Clear the check box to limit the patch acton to specific labels or devices.
Device Labels	Restrict the action to the patches in the labels that you select. This is the most commonly used option. 1. For assigning Device labels, click the edit icon. 2. In the *Select Labels* dialog box that appears, drag one or more labels (as applicable) to the *Limit Run to* area, then click **OK**. To use this option, you must already have Smart Labels for the applicable patches. See Using Smart Labels for patching.

Option	Description
Devices	Run patch actions on the devices that you select. • To search for devices, begin typing in the field. • To remove all specified devices and start again, click **Remove All**. • Scoped users can see only those devices that are associated with their role, when the role is assigned a label. For more information about user roles, see Add or edit User Roles.
Operating Systems	Select the operating systems of the devices that you want to patch. The default is all operating systems. When this option is configured, the schedule only applies to devices with the selected operating systems. 1. For selecting **Operating Systems**, click the edit icon. 2. In the **Operating Systems** dialog box that appears, select the OS versions in the navigation tree, as applicable. You have an option to select OS versions by their family, product, architecture, release ID, or build version. You can choose a specific build version, or a parent node, as needed. Selecting a parent node in the tree automatically selects the associated child nodes. This behavior allows you to select any future OS versions, as devices are added or upgraded in your managed environment. For example, to select all build current and future versions associated with the Windows 10 x64 architecture, under **Windows** > **Windows 10**, select **x64**.

Notify tab

Option	Description
Options	The alerts displayed to users when patch actions run. To perform the action without notifying the user, leave the *Options* field blank. • **OK**: Run immediately. • **Cancel**: Cancel until the next scheduled run. • **Snooze**: Prompt the user again after the *Snooze Duration*.
Timeout	The amount of time, in minutes, for the dialog to be displayed before an action is performed. If this time period elapses without the user pressing a button, the appliance performs the action specified in the *Timeout* drop-down list.
Timeout Action	The action to be performed when the **Timeout** period elapses without the user choosing an option.
Snooze Duration	The amount of time, in minutes, for the period after the user clicks **Snooze**. When this period elapses, the dialog appears again.
Snooze Until Limit	Select the **Snooze Until Limit** check box to enable the user to Snooze the patch action a specified number of times. Specify the number of **Attempts**.
Initial Message	The message to be displayed to users before the action runs. To customize the logo that appears in the dialog, see Configure appliance General Settings with the Organization component enabled.
Progress Message	The message displayed to users during the patch action.

Option	Description
Completion Message	The message displayed to users when the patch action is complete.

Reboot tab

Option	Description
Options	The options for rebooting the managed device: • **No Reboot**: The device does not reboot even though a reboot might be required for the patch to take effect. This option is not recommended because deploying patches without rebooting when required can leave systems unstable. Further, patches that require reboots are only shown as deployed after the reboot. • **Prompt User**: Waits for the user to accept the reboot before restarting the device. If the user snoozes or cancels the reboot, patching stops until a reboot occurs. Selecting a Snooze Duration in the agent dialog box that appears on the target device pauses the reboot prompt for the specified snooze interval. • **Force Reboot**: Reboots as soon as a patch requiring it is deployed. Forced reboots cannot be canceled. Force Reboot works well for desktops and servers. You might not want to force reboot on laptops. Force Reboot works well with servers because they usually have no dedicated users. However, it is important to warn users that services will not be available when servers are being patched and re-booted. See Best practices for patching.
Automatically reboot when no one is logged in	Automatically reboot the managed device if no users are logged in.
Message	The message to be displayed to the user before the device reboots. For information about adding a custom logo to the message dialog, see Configure appliance General Settings with the Organization component enabled.
Timeout	The amount of time, in minutes, for the dialog to be displayed before an action is performed. If this time period elapses without the user pressing a button, the appliance performs the action specified in the *Timeout* drop-down list. When *Force Reboot* is selected, the timeout behavior takes into consideration the `KUSerAlert` and global KACE Agent process timeouts. The global timeout, set through the *Agent and Communication Settings* section, always determines how long any agent-launched processes can run for, including the `KUserAlert` timeout. For example, if the `KUserAlert` timeout is set to two hours, and you set the global timeout to one hour, the agent will stop the `KUserAlert` because it runs too long. Therefore the global timeout must be set to the desired timeout that is longer than the `KUserAlert` timeout. This value must be set accordingly. For more information about agent settings, see Configure Agent communication and log settings.
Timeout Action	The action to be performed when the **Timeout** period elapses without the user choosing an option.
Reboot Delay (countdown)	Postpone the reboot using a countdown. The countdown is in minutes.
Reboot Now	Reboot the device immediately.

Option	Description
Reboot Later	Reboot the device later.
Number of prompts	The number of prompts the user receives before the device reboots. For example, if you enter a value of 5, the device automatically reboots the fifth time the user receives the reboot prompt. In other words, the user can delay the reboot only four times if the **Number of prompts** value is set to 5.
Reprompt Interval	The time that elapses before the user is reprompted to reboot.

Schedule section

Option	Description
None	Run in combination with an event rather than on a specific date or at a specific time. This option is useful if you want to patch servers manually, or perform patch actions that you do not want to run on a schedule.
Every _ hours	Run at a specified interval.
Every day/specific day at HH:MM	Run daily at a specified time, or run on a designated day of the week at a specified time.
Run on the nth **of every month/ specific month at HH:MM**	Run on the **n**th day every month, (for example, the first or the second) day of every month, or a specific month, at the specified time.
Run on the nth weekday of every month/specific month at HH:MM	Run on the specific weekday of every month, or a specific month, at the specified time.

Custom	Run according to a custom schedule.
	Use standard 5-field cron format (extended cron format is not supported):
	`* * * * *`
	`| | | | +----------day of week (0-6)(Sun=0)`
	`| | | +----------month (1-12)`
	`| | +----------day of month (1-31)`
	`| +----------hour (0-23)`
	`+----------minute (0-59)`

Option	Description
	Use the following when specifying values: • **Spaces ( )**: Separate each field with a space. • **Asterisks (*)**: Include the entire range of values in a field with an asterisk. For example, an asterisk in the hour field indicates every hour. • **Commas (,)**: Separate multiple values in a field with a comma. For example, `0,6` in the day of the week field indicates Sunday and Saturday. • **Hyphens (-)**: Indicate a range of values in a field with a hyphen. For example, `1-5` in the day of the week field is equivalent to `1,2,3,4,5`, which indicates Monday through Friday. • **Slashes (*/*)**: Specify the intervals at which to repeat an action with a slash. For example, `*/3` in the hour field is equivalent to `0,3,6,9,12,15,18,21`. The asterisk (`*`) specifies every hour, but `/3` restricts this to hours divisible by 3. Examples: • `15 * * * * Run 15 minutes after every hour every day` • `0 22 * * * Run at 22:00 every day` • `0 0 1 1,6 * Run at 00:00 on January 1 and June 1` • `30 8,12 * * 1-5 Run weekdays at 08:30 and 12:30` • `0 2 */2 * * Run every other day at 02:00`
View Task Schedule	Click to view the task schedule. The *Task Schedule* dialog box displays a list of scheduled. Click a task to review the task details. For more information, see View task schedules.
Timezone	The timezone to use when scheduling the action. Select **Server** to use the timezone of the appliance. Select **Agent** to use the timezone of the managed device.
Run on next connection if offline	Run the action the next time the managed device connects to the appliance, if the device is currently offline. This option is useful for laptops and other devices that are periodically offline. If this option is not selected, and the device is offline, the action does not run again until the next scheduled time.
Delay run after reconnect	Delay the schedule by a specified amount of time. The time delay period begins when the patch action is scheduled to run.
End after	The time limit for patching actions. For example, if you schedule patches to run at 04:00, you might want all patching actions to stop at 07:00 to prevent bandwidth issues when users start work. To do so, you could specify **180** in the minutes box. When this time limit is reached, any patching tasks that are in progress are suspended, and their status on Security logs is *Suspended*. These patching tasks do not resume on the next run and instead start from the beginning with each scheduled patching action.

Configure patch schedules

You can create and configure patch schedules and set a time for them to run. Patching schedules do not interfere with Managed Installations or other distributions.

1. Start the *Schedule Detail* wizard:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Security**, then click **Patch Management**.
    c. On the *Patch Management* panel, in the **Schedules** section, click **Detect, Deploy, Rollback missing patches**.

    Or

    On the *Patch Management* panel, in the Schedules section, click New Schedule.

    d. On the *Patch Schedules* list page, do one of the following:

    # To create a new patch schedule, click **Choose Action** > **New (Wizard)**.

    # To edit an existing schedule, click the schedule name in the list, then on the *Patch Schedule Summary* page that appears, click **Edit**.

    The *Schedule Detail* wizard appears, as selected. The same options are available on the *Schedule Detail* page. You can switch between the page and wizard by clicking Classic View or Wizard View in the top-right corner, as applicable.

2. In the *Schedule Detail* wizard, in the *General Information* tab, specify the general details for this schedule.

    See General Information Tab for descriptions of the options.

3. Click **Next**.
4. In the *Action* tab, select the action that you want to associate with the schedule.

    See Action tab for descriptions of the options.

5. **Detect, Detect and Stage, Detect and Deploy, Detect, Stage and On-demand Deploy, Detect and Rollback schedules only**. On the *Action* page, in the *Detect* section, specify the detection options for the schedule.

    See Detect section for descriptions of the options.

6. **Detect and Deploy, Detect, Stage and On-demand Deploy, and Deploy schedules only**. In the *Deploy* section, specify the detection options for the schedule.

    See Deploy section for descriptions of the options.

7. **Detect and Rollback and Rollback schedules only**. In the *Rollback* tab, specify the rollback options for the schedule.

    See Rollback section for descriptions of the options.

8. **Detect, Stage and On-demand Deploy schedules only**. In the *OnDemand Deployment Timeout Settings* section, specify the deployment timeout option for the Detect, Stage and On-demand Deploy schedule.

    See On-demand Deployment Timeout Settings section for descriptions of the options.

9. Click **Next**.
10. On the *Devices* page, specify the devices you want to associate with this schedule.

    See Devices section for descriptions of the options.

11. Click **Next**.
12. **Detect and Deploy, Deploy, Detect and Rollback, and Rollback schedules only**. On the *Notification* page, configure the notification options for the schedule.

See Notify tab for descriptions of the options.

13. Click **Next**.
14. In the *Reboot* tab, specify the reboot options for the schedule.

    See Reboot tab for descriptions of the options.

15. Click **Next**.
16. In the *Schedule* section, specify options for the schedule.

    See Schedule section for descriptions of the options.

17. Click **Save**.

    The *Patch Schedule Summary* page appears, displaying the newly created or updated schedule. For more information about this page, see Review patch schedule details. If you added any devices that match the Smart Label criteria, they are automatically included in the patching schedule.

Error codes caused by patching and scripting

The following Fail error codes that can be encountered during patching (Detection or Deployment phase only) or scripting.

Table 29. Error codes encountered during patching or scripting

Error code	Description
8001	The command sent to the plugin unrecognized by the `KPluginsKacePatch`
8002	Failure parsing the command sent to the plugin
8003	Failure downloading a Manifest file
8004	Failure to extract the downloaded Manifest file
8005	General failure while handling the PreDetect command (for example, invalid function inputs)
8007	Failure to generate PreDetect results
8008	General failure while handling the Detect command (for example, invalid function inputs)
8009	Failure parsing the Detect Manifest file
8010	Failure to generate Detect results
8011	A reboot is pending
8012	Failure to upload a results log
8013	General failure while handling the Detect file (for example, invalid function inputs)
8014	Failure downloading a patch Detect file
8015	Checksum mismatch between the patch Detect file and the detection Manifest record

Error code	Description
8016	Failure to create a checksum file for the patch Detect file
8017	Failure to load the patch Detect file
8018	Failure to decrypt the patch Detect file
8019	Failure to unzip the patch Detect file
8020	Failure to parse the json in the patch Detect file
8021	Detection type in the patch Detect file not recognized as a valid detection method
8100	Failure parsing the Manifest file
8101	General failure while handling the Deploy command (for example, invalid function inputs)
8102	General failure while handling the Rollback command (for example, invalid function inputs)
8103	Invalid Handler Specific Data (HSD) type
8150	Checksum mismatch between the requested file and the Manifest record
8151	Failure downloading a requested file
8152	Failure to create a checksum file for a downloaded file
8200	Invalid command scalar operation
8201	Invalid command string operation
8202	Invalid command
8250	Invalid path to the results file
8251	Failure to create a results file

Viewing patch schedules, status, and reports

You can view patch schedules as well as the status of patches, either in general or by device. In addition, you can search for individual packages within patches, and you can view patch-related reports.

View a list of patch schedules

You can view summary information for the patch schedules that have been created on the appliance. If the Organization component is enabled on your appliance, you view patch schedules for each organization separately.

1. Go to the *Patch Schedule* page:

a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
b. On the left navigation bar, click **Security**, then click **Patch Management**.
c. On the *Patch Management* panel, in the **Schedules** section, click **Detect, Deploy, Rollback missing patches**.

Columns available on the *Patch Schedules* page include:

Option	Description
Last Update	The date and time the patch schedule was updated.
Name	The name of the patch schedule. Click to see more details on the *Patch Schedule Summary* page. For more information, see Review patch schedule details.
Schedule	The frequency at which the patch schedule is set to run. Disabled indicates that the patch is not set to run on a schedule.
Action	The type of patch action to be performed.
Reboot Option	Whether the patch schedule requires managed devices to reboot when the patch runs.
All Devices	Whether the patch schedule is targeting all devices (Yes) or selected devices (No).
Pending	The number of managed devices on which the patch is scheduled to run. Patches with this status show one of the following in the *Security* section of the *Device Detail* page: • *waiting to connect* • *scheduled* • *waiting to schedule*
Downloading	The number of managed devices that are downloading the patch. Patches with this status show the following in the *Security* section of the *Device Detail* page: *downloading*
Executing	The number of managed devices on which the patch is running. Patches with this status show one of the

Option	Description
	following in the *Security* section of the *Device Detail* page: • *handshake* • *detecting* • *rolling back* • *deploying* • *cleanup* • *verifying* • *alerting* • *upload*
Rebooting	The number of managed devices that are rebooting as part of the patching process. Patches with this status show one of the following in the *Security* section of the *Device Detail* page: • *rebooting* • *reboot pending* • *connecting*
Paused	The number of managed devices on which the patching process is paused or snoozed. Patches with this status show one of the following in the *Security* section of the *Device Detail* page: • *reboot snoozed* • *snoozed*
Completed	The number of managed devices on which the patching process finished successfully. Patches with this status show the following in the *Security* section of the *Device Detail* page: *completed*.
Failed	The number of managed devices for which errors were reported during the patching process. Patches with this status show one of the following in the *Security* section of the *Device Detail* page: • *suspended* • *cancelled*
Offline	The number of managed devices that were not connected when the patching process was scheduled to run. Patches with this status show the following in the *Security* section of the *Device Detail* page: *not scheduled*.

Option	Description
% Complete	The number of managed devices on which the patching process completed with a status of *Succeeded*, *Failed*, or *Offline*.

2. (Optional) To change column visibility, select **Column Visibility** from the *Table Options* drop-down list above the table on the right.

Review patch schedule details

When you configure a patching schedule, this page displays details about the schedule configuration and its status.

1. Go to the *Patch Schedule Summary* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Security**, then click **Patch Management**.
    c. On the *Patch Management* panel, in the **Schedules** section, click **Detect, Deploy, Rollback missing patches**.
    d. Click the name of a patch schedule.
2. Review the contents of the *Configuration* section.

Option	Description
Created	The date and time the schedule is created.
Modified	The date and time the schedule is last modified.
Last Run	The date and time the schedule is last run.
Name	The name of the schedule.
Action	The action associated with the schedule: • **Detect**: Detects patches that are installed on, or missing from, managed devices. Detect-only actions are recommended when the *Patch Download Settings* are configured to download only . Running a detect-only action before the deploy creates a list of patch files to download before deployment begins. • **Detect and Stage**: Detects patches that are installed or missing from managed devices, and downloads patch files to the agent device for later deployment. • **Detect and Deploy**: Detects and deploys patches to managed devices. These types of actions are used when managing desktops and servers. Detect and Deploy patching jobs require a connection between the device and the appliance; they do not run offline. For more information about messaging protocol connections, see Configure Agent communication and log settings. • **Detect, Stage and On-demand Deploy**: Detects patches that are installed or missing from managed devices, downloads patch files to the agent device, and causes the Windows system tray on the agent device to alert the user that the patches are ready for deployment. The user can then initiate the deployment process at their convenience. # These schedules are only available for Windows devices with agents version 11.0 or later. # The *Agent Status Icon On Device* option must be enabled in the agent communication settings. You can find these settings on the *Organization Detail*

Option	Description
	page, under *Communication and Agent Settings* (if one or more Organization components are enabled), or on the *Communication Settings* page (if you do not have an Organization component). For more information, see Configure Agent communication and log settings. • **Deploy**: Deploys applicable patches to managed devices. This is useful when you know that specific patches need to be deployed to managed devices. A final Detect job runs either after the patch is deployed or, if a reboot is required, after the device reboots and the Agent reconnects to the appliance. • **Detect and Rollback**: Detects and removes unwanted patches from managed devices. Rollbacks may not be available for some patches. See Determine whether a patch can be rolled back. • **Rollback**: Removes unwanted patches from managed devices. Rollbacks may not be available for some patches. See Determine whether a patch can be rolled back.
Description	A brief description of the patch schedule.
Devices	This field only appears when the schedule is configured to apply to all devices.
Device Label	One or more Smart Labels associated with the devices against which the schedule runs. For more information, see Using Smart Labels for patching. This field only appears when the schedule is configured to apply to selected devices.
Device Name	One or more selected devices against which the schedule runs. This field only appears when the schedule is configured to apply to selected devices.
Patches to Detect	**Detect schedules only**. This field only appears when the schedule is configured to detect all patches.
Detect Label	**Detect schedules only**. One or more Smart Labels associated with the scheduled patches. For more information, see Using Smart Labels for patching. This field only appears when the schedule is configured to detect selected patches.
Patches to Deploy	**Deploy schedules only**. This field only appears when the schedule is configured to deploy all patches.
Deploy Label	**Deploy schedules only**. One or more Smart Labels associated with the scheduled patches. For more information, see Using Smart Labels for patching. This field only appears when the schedule is configured to deploy selected patches.
Patches to Rollback	**Rollback schedules only**. This field only appears when the schedule is configured to remove all patches.
Rollback Label	**Rollback schedules only**. One or more Smart Labels associated with the scheduled patches. For more information, see Using Smart Labels for patching. This field only appears when the schedule is configured to remove selected patches.

Option	Description
Alerts	**Schedules without the Deploy action only**. The alerts displayed to users when patch actions run: • **OK**: Run immediately. • **Cancel**: Cancel until the next scheduled run. • **Snooze**: Prompt the user again after the *Snooze Duration*.
Reboot	**Schedules without the Deploy action only**. The options for rebooting the managed device: • **No Reboot**: The device does not reboot even though a reboot might be required for the patch to take effect. This option is not recommended because deploying patches without rebooting when required can leave systems unstable. Further, patches that require reboots are only shown as deployed after the reboot. • **Prompt User**: Waits for the user to accept the reboot before restarting the device. If the user snoozes or cancels the reboot, patching stops until a reboot occurs. Selecting a Snooze Duration in the agent dialog box that appears on the target device pauses the reboot prompt for the specified snooze interval. • **Force Reboot**: Reboots as soon as a patch requiring it is deployed. Forced reboots cannot be canceled. Force Reboot works well for desktops and servers. You might not want to force reboot on laptops. Force Reboot works well with servers because they usually have no dedicated users. However, it is important to warn users that services will not be available when servers are being patched and re-booted. See Best practices for patching.
Schedule	The selected schedule details. Click **View Task Schedule** to see a detailed task scheduler. In the dialog box that appears, click a task to review the task details. For more information, see View task schedules.
Run on Next Connection in Offline	Indicates if the schedule runs the action the next time the managed device connects to the appliance, if the device is currently offline.
Delay Run After Reconnect	If configured, this option indicates the amount of time the schedule is delayed for. The time delay period begins when the patch action is scheduled to run.
End After	If configured, this option indicates the maximum amount of time the schedule can run for. When this time limit is reached, any patching tasks that are in progress are suspended.

3. In the *Schedule Status* section, review the overall patch schedule status on any of the following tabs:

Tab	Contents
By Machine	Devices selected for patching. Each entry displays the device name, its IP address, the patching status (see Patching status definitions), patch results, and the date the patching completed. You can expand a device node to view the applicable patches. Each patch entry shows the patch ID, associated Knowledge Base article number, patch name, and the current status (Patched, Not Patched, Staged, and Detect, Stage, or Deploy Failure).
By Patch	Patches selected for detection, staging, and deployment. Each entry displays the patch ID, associated Knowledge Base article number, patch name, and the numbers

Tab	Contents
	of devices that are patched, not patched, and those that encountered detect or deploy failures.
Patched	Patches successfully installed on devices. Each entry displays the patch ID, associated Knowledge Base article number, and the patch name. You can expand a patch node to view the devices on which the patch is installed.
Not Patched	Patches that are not installed on devices. Each entry displays the patch ID, associated Knowledge Base article number, and the patch name. You can expand a patch node to view the devices on which the patch is to be installed.
Staged	Patches that are staged for installation. Staging refers to patch files being copied to the agent device for later deployment. Each entry displays the patch ID, associated Knowledge Base article number, and the patch name. You can expand a patch node to view the devices on which the patch is to be installed.
Detect Failures	Incomplete patches that resulted in a detection failure. Each entry displays the patch ID, associated Knowledge Base, patch name, and the associated error code (see Error codes caused by patching and scripting). You can expand a patch node to view the devices on which the failure is encountered.
Stage Failures	Incomplete patches that resulted in a staging failure. Each entry displays the patch ID, associated Knowledge Base article number, patch name, and the associated error code (see Error codes caused by patching and scripting). You can expand a patch node to view the devices on which the failure is encountered.
Deploy Failures	Incomplete patches that resulted in a deployment failure. Each entry displays the patch ID, associated Knowledge Base, patch name, and the associated error code (see Error codes caused by patching and scripting). You can expand a patch node to view the devices on which the failure is encountered.

4. **Optional**. After reviewing the schedule details, you can perform any of the following actions:
   - To edit the patching schedule, click **Edit**. For more information, see Configure patch schedules.
   - To run the patching schedule, click **Run Now**.
   - To make a copy of the patching schedule, click **Duplicate**.
   - To delete the patching schedule, click **Delete**.

Patching status definitions

A patching status indicates the state of the current task. This information appears on the *Patch Schedule Summary* page, in the *Schedule Status* section. For more information, see Review patch schedule details.

Table 30. Patching status definitions

Patching status	Definition
alerting	Alert sent to user, waiting for confirmation.
cancelled	Task cancelled by user.
cleanup	Payload files from agent not accessed since last 90 days.

Patching status	Definition
completed	Task completed.
connecting	Agent reconnecting after reboot.
deploy	Patch deployment in progress.
detect	Patch detection in progress.
downloading	Patch deployment waiting for packages to download.
error	Task not completed due to time out or other error.
not scheduled	Task not yet created for this device.
predetect	Pre-detection with the Agent in progress.
reboot pending	Patches deployed, reboot required to continue.
reboot snoozed	Patches deployed, reboot required to continue. After a configured interval the end user is reminded to reboot.
rolling-back	Patch rollback in progress.
scheduled	Task scheduled and is waiting to run.
snoozed	Task snoozed, user to be reminded after the configured snooze duration.
stage	Downloading files for later deployment.
suspended	Task suspended before reaching completion.
uploading logs	Uploading pre-detection, detection, deployment, verification, or rollback logs.
verifying	Post-deployment verification detection in progress.
version check	Task checking the patch version.
waiting on-demand deploy	Task waiting for the user action to deploy the schedule.
waiting to connect	Device disconnected.
waiting to schedule	Task waiting to schedule in the Agent's time zone.

View patch status

You can view the status of patches, including a list of the devices on which patches have been deployed.

1. Go to the *Patch Detail* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Security**, then click **Patch Management**.
    c. On the *Patch Management* panel, click **Display available patches** under **Catalog**.
2. Scroll down to the *Deployment Status* table.

    The table shows details about the patch, including a list of the devices on which the patch has been deployed.

View patch status by device

You can view patch status for each managed device.

1. Go to the organization *Device Detail* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Inventory**, then click **Device**s.
    c. Click the name of a device.
2. Scroll down to the *Security* section, then click the **Patching Detect/Deploy Status** link.

The list of the patches installed on the device appears.

View files within patches

You can view the files contained in each patch.

1. Go to the *Patch Detail* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Security**, then click **Patch Management**.
    c. On the *Patch Management* panel, click **Display available patches** under **Catalog**.
2. Scroll down to the *Associated Files* table.

View patch reports

You can view reports related to patching.

1. Go to the Patch Management *Reports* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Security**, then click **Patch Management**.
    c. On the *Patch Management* panel, click Display patch-related reports in **Reporting** section.

The *Reports* page appears, with Patching selected in the *View By* drop-down list. This page provides links to patch-related reports.

Managing patch rollbacks

If rollback is supported for patches, you can roll back patches to remove them from managed devices.

Some vendors and patch-types do not support rollbacks, however. For example, large software patches, such as Service Packs, cannot be rolled back.

Determine whether a patch can be rolled back

You can search the *Patch Catalog* page to find out whether patches can be rolled back after they are deployed to managed devices.

1. Go to the *Patch Detail* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Security**, then click **Patch Management**.
    c. On the *Patch Management* panel, click **Display available patches** under **Catalog**.
    d. Click the name of a patch.
2. Click the **Filter** tab above the list on the right to display the *Filter* panel.
3. Enter the following search criteria:

    ```
    Patch Listing Information: Support Rollback | is | True
    ```

4. **Optional**: Enter additional search criteria.
5. Click **Search**.

Patches that support rollback appear.

Undo the last patching job

If the patch vendor supports a rollback, you can undo the last patch deployment by creating and running a Rollback or Detect and Rollback patching schedule.

1. Go to the *Patch Schedule Detail* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Security**, then click **Patch Management**.
    c. On the *Patch Management* panel, in the **Schedules** section, click **Detect, Deploy, Rollback missing patches**.
    d. Click the name of a patch schedule.
2. In the *Choose Action* drop-down list, select **Rollback** or **Detect and Rollback**.
3. Select the patches to rollback, in the same way that you specified them in the original schedule, by creating a Smart Label.

    See Using Smart Labels for patching.

    This option is supported only for removing the last installed patch on a software application. See Managing patch rollbacks.

4. Specify additional settings for the patch schedule as needed.

    For more information, see Configure patch schedules.

Managing patch inventory

Patches that have been downloaded to the appliance are referred to as patch inventory. You can view details and statistics about patch inventory, and you can mark patches as active or inactive. In addition, you can use labels to manage patches.

Prerequisites for managing patch inventory

Before managing patch inventory, you need to subscribe to and download patches.

See:

- Subscribing to patches and configuring download settings
- Select patch and feature update download settings

Viewing patch information

You can view information about patches and view patch information for devices as needed.

View downloaded patches

The *Patch Catalog* list displays the patch detection signatures that have been downloaded for subscribed patches.

1. Go to the patch *Catalog* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Security**, then click **Patch Management**.
    c. On the *Patch Management* panel, click **Display available patches** under **Catalog**.
2. Use this drop-down list to list the patches.
    - **View By: Control the patches shown in the list based on the drop-down list selection.**

Column	Description
All Patches	View all patches.
New Patches	View new patches.
Newly Enabled Patches	View the patches that are recently enabled.
Label	View patches tagged with a label. This information is only visible if there are labels created.
Status	View **Active**, **Disabled**, or **Inactive** patches.
Download Status	View patches that are **Downloaded** or **Not Downloaded**.

Column	Description
Severity	Filter the patch list by the importance specified by vendors, such as Microsoft. Severity levels include **Critical**, **Important**, **Low**, and so on.
CVSS Base Score	Filters the patches based on the CVSS Base Score ranges: • Critical: 9.0 - 10.0 • High: 7.0 - 8.9 • Medium: 4.0 - 6.9 • Low: 0.1 - 3.9
Known Expoit	Filter patches based on: • Known Exploit Vulnerability (KEV) • Used in Ransomware Campaigns
Most Recent	View patches that were most recently added. You can display the patches added in the **Last 1 Month**, **Last 6 Months**, **Last 1 Year**, or **Last 2 Years**.
Year	Filter the patch list by the year the patch was released.
Operating System	Filter the patch list by operating system.

3. The following information appears in columns on the *Patch Catalog* page:

Column	Description
Status	The status of the patch: Active, Inactive, or Disabled. • **Active**: Patches that you subscribe to, that are downloaded, and that are ready to detect or deploy. • **Inactive**: Patches that you subscribe to, but that have been marked as inactive to prevent them from being detected or deployed automatically. • **Disabled**: Patches that do not match your subscription. These patches can only be detected when the *Detect Disabled Patches* option is enabled in your patch subscription. These patches cannot be deployed unless they meet the subscription criteria.
Package	The patch identification information. Labels applied to the patch are also displayed in this column.
Name	The name of the patch.
Released	The date the patch became available.
Publisher	The name of the publisher of the patch.
Severity	The importance of the patch as determined by the publisher, such as Microsoft.
Reboot	Whether devices must be rebooted to complete the patching process.

Column	Description
Compliance	The percentage of patches installed versus scheduled.
Installed	The number of devices that have received the patch.
Missing	The number of devices that have been detected as needing the patch and that are waiting for deployment.
Staged	The number of devices that have received the patch and that are waiting for deployment.
Error	The number of devices that have failed the maximum number of deployment attempts. The maximum number of deployment attempts is configured in the patch schedule. See Configuring patch schedules.
Size	The size of the patch file. • **Black color**: Inactive or Disabled patches. • **Red color**: Patches to which you are subscribed; however, no associated packages for this patch have been downloaded at this time. To see which associated packages are missing, click the patch name to view the patch detail page. • **Size = 0**: None of the patch packages are downloaded. • **Actual size** (other than zero): At least one of the patch packages has been downloaded.
Superseded	Patches that have been replaced by other patches and are no longer required.

View patch details

Patch details include vendor information, deployment status, and notes. In addition, you can assign labels to patches when you view patch details.

1. Go to the *Patch Detail* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Security**, then click **Patch Management**.
    c. On the *Patch Management* panel, click **Display available patches** under **Catalog**.
    d. Click a patch name.

    The *Patch Detail* page appears, displaying complete information about the patch.

Resetting the number of patch deploy attempts

When a patch deployment has been attempted the configured maximum number of times, the number of retries can be reset.

To configure a maximum number of deploy attempts, see Configuring patch schedules.

There are two places the number of deployment attempts can be reset: the *Catalog* list and the *Patch Detail* page.

- To reset the number of patch deploy attempts from the patch catalog list, see Reset the number of patch deploy attempts from the patch Catalog.
- To reset the number of patch deploy attempts from the patch detail page, see Reset the number of patch deploy attempts from the patch detail page.

Reset the number of patch deploy attempts from the patch Catalog

When a patch deployment has been attempted the configured maximum number of times, the number of retries can be reset from the patch *Catalog* page.

1. Go to the patch *Catalog* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Security**, then click **Patch Management**.
    c. On the *Patch Management* panel, click **Display available patches** under **Catalog**.
2. Select the check box next to one or more patches/bulletins in the list then select **Choose Action** > **Reset Tries**.

    The number of deploy attempts are reset to 0.

Reset the number of patch deploy attempts from the patch detail page

When a patch deployment has been attempted the configured maximum number of times, the number of retries can be reset from the patch detail page.

1. Go to the *Catalog* list:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Security**, then click **Patch Management**.
    c. On the *Patch Management* panel, click **Display available patches** under **Catalog**.
2. Do one of the following to display the *Patch Detail* page:
    # If the **Show** drop-down list is set to **Applicable Packages** or **All Packages**, click the name of the package, and then click the name of a patch within the package.
    # If the **Show** drop-down list is set to **Individual Patches**, click the name of a patch.
3. Scroll down to the *Deployment Status* section and click the **Reset Tries** button.

    The number of deploy attempts is reset to 0.

View patch information for devices in inventory

The *Inventory* section contains detailed patch information for managed devices.

This information includes:

- The list of patches deployed on the device.
- Details of the patch schedules that apply to the device.
- Information about successful and failed patching and rollback attempts.

1. Go to the organization *Device Detail* page
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Inventory**, then click **Device**s.

c. Click the name of a device.

2. In the *Device Details* page, go to the *Security* tab.
3. Click **Patching Detect/Deploy Status** to expand the *Patching Detect/Deploy Status* details.
4. For more information, click the **Help** buttons next to *Scheduled Task Status* and *Deployment Status:* ⓘ.

View devices missing patches

View the devices that are missing patches so you can determine why they have not been updated.

1. Go to the *Patch Catalog* list:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Security**, then click **Patch Management**.
   c. On the *Patch Management* panel, click **Display available patches** under **Catalog**.
2. Above the catalog list, click on the number following *Devices missing patches*.

   The *Devices* list is opened displaying all devices that have missing patches.

Leveraging CVSS and EPSS for effective Patching

The Patch Catalog includes Common Vulnerability Scoring System (CVSS) and Exploit Prediction Scoring System (EPSS) scores. Utilizing this enhances the ability to prioritize vulnerabilities for effective patch management. The combined use of CVSS and EPSS allows administrators to make informed decisions, prioritize critical updates, and improve overall endpoint security.

What is CVSS, EPSS, and CVE?

CVSS:

- provides a standardized metric for assessing the severity of vulnerabilities.
- CVSS v3.1 scores range from 0.0 to 10.0, indicating the potential impact on systems.

EPSS:

- estimates the probability of vulnerability being exploited within the next 30 days.
- expressed as a percentage from 0.0% to 100%, indicating the likelihood of exploitation.

CVE:

CVE (Common Vulnerabilities and Exposures) help standardize vulnerability references across platforms and tools, making it easier to assess and track risks.

By integrating CVSS and EPSS scores into patch filtering criteria, an administrator can:

- Assess the severity and exploitability of each patch.
- Filter and prioritize patches based on risk indicators. The CVSS Score (Critical, High, Medium, Low) and the EPSS Score for patches included in patch filter determines which patches need urgent attention in the environment.
- Filter patches based on specific CVSS and EPSS values, ensuring a precise and prioritized approach to vulnerability management.
- Take focused remediation actions on high-risk devices.

What can you do with the CVE, CVSS, and EPSS?

1. You can view detailed vulnerability data in a **CVE Information** section on the **Patch Detail** page.

   NOTE: If a patch is linked with one or more CVEs, the Patch Detail page displays relevant data in the **CVE Information** section. If no vulnerabilities are associated, this section remains blank.

2. You can filter Patches on the *Patch List* page, using the options from the **View By** drop-down list. The filters are as follows:
   # CVSS Base Score
   # Known Exploit
   # Missing Patches with CVSS Score
3. You can create widgets on the *Dashboard* page to display devices missing patches with Critical or High CVSS scores, devices affected by patches and so on.

Related Information:

Click the links for more information on CVSS or EPSS.

Viewing patch statistics and logs

Patch statistics and logs provide an overview of appliance patching tasks.

View patch statistics

You can view patch statistics on the *Patch Management* panel.

1. Go to the *Patch Management* panel.
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Security**, then click **Patch Management**.

The *Patch Management* panel appears, showing patch statistics.

View the patch log

You can view the patch log to check for errors in the patch download process.

1. Go to the appliance *Control Panel*:
   - **If the Organization component is not enabled on the appliance, log in to the appliance Administrator Console, `https://appliance_hostname/admin`, then select Settings > Control Panel.**
   - **If the Organization component is enabled on the appliance, log in to the appliance System Administration Console, `https://appliance_hostname/system`, or select System in the drop-down list in the top-right corner of the page, then select Settings > Control Panel.**
2. On the left navigation bar, click **Logs** to display the *Logs* page.
3. In the *Log* drop-down list, select **Patch Download Log**.

The patch log appears.

Mark patches as inactive

You can mark subscribed patches as inactive to prevent them from being detected or deployed automatically.

1. Go to the *Patch Catalog* list:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Security**, then click **Patch Management**.

c. On the *Patch Management* panel, click **Display available patches** under **Catalog**.

2. Select the check box next to a patch.
3. Select **Choose Action** > **Change Status to** > **Inactive**.

If the **Show** drop-down list is set to **Applicable Packages** or **All Packages** all patches that make up the selected bulletin will be marked as inactive. If the **Show** drop-down list is set to **Individual Patches** all selected patches will be marked as inactive. All patches marked as inactive are automatically purged from the cache during the next scheduled patch download.

Patch Mac OS X devices

You can apply patches to Mac OS X devices as needed.

1. Go to the *Patch Catalog* list:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Security**, then click **Patch Management**.
   c. On the *Patch Management* panel, click **Display available patches** under **Catalog**.
2. Do one of the following:
   - **In the *View By* drop-down list above the table, select Operating System > Mac <OS X>.**
   - **Click the Filter tab, which appears above the table, then search for Mac OS X patches.**
   - **Use the Smart Label feature to automatically search the patch list using predefined search criteria.**
3. To allow the appliance to download Apple Security updates for Mac, select the appropriate operating system in the *Mac Platform* list in the *Patch Subscription Settings* page.

You can select more than one Mac operating system. See Subscribe to patches

Managing Windows Feature Updates

Windows Feature Updates are new versions of Microsoft Windows 10, released a few times every year. The appliance allows you to automate the process of installing these update, to help you improve the performance of managed Windows 10 devices and protect them from potential OS-related vulnerabilities.

Use the appliance to detect and deploy the latest Windows Feature Updates for your Windows 10 devices managed by the appliance.

NOTE: This feature is only supported on Windows 10 devices with a Semi-Annual Channel subscription. It is not available for Mac, Linux, or Windows devices running a OS version other than 10.

Subscribe to Windows Feature Updates

You can subscribe to Windows Feature Updates for your managed Microsoft Windows 10 devices.

Before you subscribe to and download Windows Feature Updates, identify the operating systems installed on managed devices, and verify their update requirements. You can only download updates for your managed Windows 10 devices.

1. Go to the *Windows Feature Update Subscriptions* page:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Security**, then click **Windows Feature Updates**.

c. On the *Windows Feature Updates* panel, click **Choose available Windows Feature Updates** in the **Subscriptions** section.

2. Specify the *Subscription* settings. The operating systems and locales specified in the subscription control the patches that are downloaded.

Option	Description
Windows Feature Update Versions	Download selected Windows Feature Updates. Click the edit button to manage the list of operating systems: . Click **Select Versions** and select one or more update versions that you want to install on your managed Windows 10 devices,. To ignore Windows Feature Updates, select **Disabled**. Selected items are displayed after you save the settings.
Locales	Download patches for the selected languages. Click the edit button to manage the list of locales: . Select **All Locales** to download patches regardless of the locale or select the check boxes next to one or more locales. Selected items are displayed after you save the settings.

NOTE: At least one version and one locale must be selected for a Windows Feature Update subscription.

3. Click **Save**.

Selected Windows Feature Updates are downloaded automatically at the next scheduled download time.

Next, you can configure Windows Feature Update download settings. See Select patch and feature update download settings.

Configure Windows Feature Update schedules

You can create and configure Windows Feature Update schedules and set a time for them to run. Windows Feature Update schedules do not interfere with Managed Installations or other distributions.

1. Start the *Windows Feature Update Schedule Detail* wizard:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Security**, then click **Windows Feature Updates**.
   c. On the *Windows Feature Updates* panel, in the **Schedules** section, click **Detect and deploy Windows Feature Updates** in the **Subscriptions** section.

      Or

      On the *Windows Feature Updates* panel, in the **Schedules** section, click **New Schedule**.
   d. On the *Windows Feature Update Schedules* list page, do one of the following:

   # To create a new Windows Feature Update schedule using the *Schedule Detail* wizard, click **Choose Action** > **New (Wizard)**.

   # To create a new Windows Feature Update schedule using the *Schedule Detail* page, click **Choose Action** > **New (Classic)**.

   # To edit an existing schedule, click the schedule name in the list, then on the *Windows Feature Update Schedule Summary* page that appears, click **Edit**.

   The *Schedule Detail* page or wizard appears, as selected. The same options are available in each selection. You can switch between the page and wizard by clicking Classic View or Wizard View in the top-right corner, as applicable.

2. Configure general information about the schedule:

Option	Description
Name	A name that identifies the schedule. This name appears on the *Windows Feature Update Schedules* list page.
Description	A brief description of the Windows Feature Update schedule.

3. In the **Action** tab, in the *Choose Windows Feature Update* section, configure the following options:

Option	Description
Select a build	Select a version of the Windows Feature Update that you want to detect, stage, or deploy. This section lists the updates selected in your subscription.
Select editions	Select one or more editions of the selected version. This section lists all editions for the selected version, for example, Business and Consumer editions for the different platforms (32- and 64-bit).

4. Select one of the following actions.

These actions are identical to patch scheduling actions. See Configure patch schedules.

Action	Description
Detect	Scans for compatible Windows Feature Updates.
Detect and Stage	Scans for compatible Windows Feature Updates, and downloads the applicable files to the agent device for later deployment.
Detect, Stage and On-demand Deploy	Detects Windows Feature Updates that are installed or missing from managed devices, downloads the applicable files to the agent device, and causes the Windows system tray icon to alert the user. • These schedules are only available for Windows devices with agents version 11.0 or later. • The *Agent Status Icon On Device* option must be enabled in the agent communication settings. You can find these settings on the *Organization Detail* page, under *Communication and Agent Settings* (if one or more Organization components are enabled), or on the *Communication Settings* page (if you do not have an Organization component). For more information, see Configure Agent communication and log settings.
Detect and Deploy	Scans for compatible Windows Feature Updates, downloads the applicable files to the agent device, and deploys the update to the selected devices.

5. Select the target devices in the **Devices** tab using the following options.

These options are identical to the ones appearing in patch scheduling actions. See Configure patch schedules.

Action	Description
All Devices	To apply this schedule to all managed devices, select this options. Clear the check box to limit the patch action to specific labels or devices.
Device Labels	Restrict the action to the feature updates using the labels that you select here. This is the most commonly used option.

Action	Description
	1. Click **Manage Associated Labels**. 2. In the *Select Labels* dialog box that appears, drag one or more labels (as applicable) to the *Limit Run to* area, then click **OK**. To use this option, you must already have Smart Labels for the feature updates. See Using Smart Labels for patching.
Devices	Run patch actions on the devices that you select. • To search for devices, begin typing in the field. • To remove all specified devices and start again, click **Remove All**. • Scoped users can see only those devices that are associated with their role, when the role is assigned a label. For more information about user roles, see Add or edit User Roles.
Detect Timeout	Set limit to the total length of time allowed for the associated phase.

6. In the *Schedule* tab, specify the applicable options for the schedule.

These options are identical to the ones appearing in patch scheduling actions. See Configure patch schedules.

Option	Description
None	Run in combination with an event rather than on a specific date or at a specific time. This option is useful if you want to patch servers manually, or perform patch actions that you do not want to run on a schedule.
Every _ hours	Run at a specified interval.
Every day/specific day at HH:MM	Run daily at a specified time, or run on a designated day of the week at a specified time.
Run on the nth of every month/ specific month at HH:MM	Run on the **n**th day every month, (for example, the first or the second) day of every month, or a specific month, at the specified time.
Run on the nth weekday of every month/specific month at HH:MM	Run on the specific weekday of every month, or a specific month, at the specified time.

Custom	Run according to a custom schedule.
	Use standard 5-field cron format (extended cron format is not supported):
	`* * * * *`
	`| | | | +----------day of week (0-6)(Sun=0)`
	`| | | +----------month (1-12)`
	`| | +----------day of month (1-31)`
	`| +----------hour (0-23)`
	`+----------minute (0-59)`

Option	Description
	Use the following when specifying values: • **Spaces ( )**: Separate each field with a space. • **Asterisks (*)**: Include the entire range of values in a field with an asterisk. For example, an asterisk in the hour field indicates every hour. • **Commas (,)**: Separate multiple values in a field with a comma. For example, `0,6` in the day of the week field indicates Sunday and Saturday. • **Hyphens (-)**: Indicate a range of values in a field with a hyphen. For example, `1-5` in the day of the week field is equivalent to `1,2,3,4,5`, which indicates Monday through Friday. • **Slashes (*/*)**: Specify the intervals at which to repeat an action with a slash. For example, `*/3` in the hour field is equivalent to `0,3,6,9,12,15,18,21`. The asterisk (`*`) specifies every hour, but `/3` restricts this to hours divisible by 3. Examples: • `15 * * * * Run 15 minutes after every hour every day` • `0 22 * * * Run at 22:00 every day` • `0 0 1 1,6 * Run at 00:00 on January 1 and June 1` • `30 8,12 * * 1-5 Run weekdays at 08:30 and 12:30` • `0 2 */2 * * Run every other day at 02:00`
View Task Schedule	Click to view the task schedule. The *Task Schedule* dialog box displays a list of scheduled. Click a task to review the task details. For more information, see View task schedules.
Timezone	The timezone to use when scheduling the action. Select **Server** to use the timezone of the appliance. Select **Agent** to use the timezone of the managed device.
Run on next connection if offline	Run the action the next time the managed device connects to the appliance, if the device is currently offline. This option is useful for laptops and other devices that are periodically offline. If this option is not selected, and the device is offline, the action does not run again until the next scheduled time.
Delay run after reconnect	Delay the schedule by a specified amount of time. The time delay period begins when the patch action is scheduled to run.
End after	The time limit for patching actions. For example, if you schedule patches to run at 04:00, you might want all patching actions to stop at 07:00 to prevent bandwidth issues when users start work. To do so, you could specify **180** in the minutes box. When this time limit is reached, any patching tasks that are in progress are suspended, and their status on Security logs is *Suspended*. These patching tasks do not resume on the next run and instead start from the beginning with each scheduled patching action.

7. Click **Save**.

The *Windows Feature Update Schedule Summary* page appears, displaying the newly created or updated schedule. For more information about this page, see View Windows Feature Update status.

If you added any devices that match the Smart Label criteria, they are automatically included in the update schedule.

When the updates are downloaded to the agent device and are ready for deployment, the KACE Agent icon is updated in the Windows system tray and in the menu, indicating that actions are available for the agent. To install the updates, on the agent device, in the Windows system tray, click the KACE Agent, and choose **Deploy staged patches**. For more information about the KACE Agent icons, see Manage the KACE Agent on Windows devices using the Windows system tray.

View Windows Feature Update schedules

You can view summary information for the Windows Feature Update schedules that exist on the appliance. If the Organization component is enabled on your appliance, you view Windows Feature Update schedules for each organization separately.

1. Go to the *Windows Feature Update Schedules* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Security**, then click **Windows Feature Updates**.
2. On the *Windows Feature Updates* panel, click the **Detect and deploy Windows Feature Updates** link in the **Schedules** section.

Columns available on the *Windows Feature Update Schedules* page are identical to the ones on the *Patch Schedules* page. For more information about the fields on the *Patch Schedules* page, see View a list of patch schedules.

3. (Optional) To change column visibility, select **Column Visibility** from the *Table Options* drop-down list above the table on the right.

Review Windows Feature Update schedule details

When you configure a Windows Feature Update schedule, this page displays details about the schedule configuration and its status.

1. Go to the *Windows Feature Update Schedule Summary* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Security**, then click **Windows Feature Updates**.
    c. On the *Windows Feature Updates* panel, click **Detect and deploy Windows Feature Updates** in the **Subscriptions** section.
    d. Click the name of a Windows Feature Update schedule.
2. Review the contents of the *Configuration* section.

Option	Description
Created	The date and time the schedule is created.
Modified	The date and time the schedule is last modified.

Option	Description
Last Run	The date and time the schedule is last run.
Name	A name that identifies the schedule. This name appears on the *Windows Feature Update Schedules* list page.
Action	The action associated with the schedule: • **Detect**: Scans for compatible Windows Feature Updates. • **Detect and Stage**: Scans for compatible Windows Feature Updates, and downloads the applicable files to the agent device for later deployment. • **Detect, Stage and On-demand Deploy**: Detects Windows Feature Updates that are installed or missing from managed devices, downloads the applicable files to the agent device, and causes the Windows system tray on the agent device to alert the user that the updates are ready for deployment. The user can then initiate the deployment process at their convenience. # These schedules are only available for Windows devices with agents version 11.0 or later. # The *Agent Status Icon On Device* option must be enabled in the agent communication settings. You can find these settings on the *Organization Detail* page, under *Communication and Agent Settings* (if one or more Organization components are enabled), or on the *Communication Settings* page (if you do not have an Organization component). For more information, see Configure Agent communication and log settings. • **Detect and Deploy:** Scans for compatible Windows Feature Updates, downloads the applicable files to the agent device, and deploys the update to the selected devices.
Description	A brief description of the Windows Feature Update schedule.
Devices	This field only appears when the schedule is configured to apply to all devices.
Windows Feature Update	The name and version of the Windows Feature Update.
Device Label	One or more Smart Labels associated with the devices against which the schedule runs. For more information, see Using Smart Labels for patching. This field only appears when the schedule is configured to apply to selected devices.
Device Name	One or more selected devices against which the schedule runs. This field only appears when the schedule is configured to apply to selected devices.
Detect Label	One or more Smart Labels associated with the scheduled updates. For more information, see Using Smart Labels for patching. This field only appears when the schedule is configured to detect selected updates.
Alerts	**Detect and Deploy schedules only**. The alerts displayed to users when update actions run: • **OK**: Run immediately. • **Cancel**: Cancel until the next scheduled run. • **Snooze**: Prompt the user again after the *Snooze Duration*.

Option	Description
	NOTE: Alerts are not available in Detect and Detect and Stage schedules.
Reboot	**Detect and Deploy schedules only**. The options for rebooting the managed device: • **No Reboot**: The device does not reboot even though a reboot might be required for the update to take effect. This option is not recommended because deploying updates without rebooting when required can leave systems unstable. Further, updates that require reboots are only shown as deployed after the reboot. • **Prompt User**: Waits for the user to accept the reboot before restarting the device. If the user snoozes or cancels the reboot, the update stops until a reboot occurs. Selecting a Snooze Duration in the agent dialog box that appears on the target device pauses the reboot prompt for the specified snooze interval. • **Force Reboot**: Reboots as soon as an update that requires it is deployed. Forced reboots cannot be canceled. Force Reboot works well for desktops and servers. You might not want to force reboot on laptops. Force Reboot works well with servers because they usually have no dedicated users. However, it is important to warn users that services will not be available when servers are being updated and re-booted. See Best practices for patching.
Schedule	The selected update schedule. Click **View Task Schedule** to see a detailed task scheduler. In the dialog box that appears, click a task to review the task details. For more information, see View task schedules.
Run on Next Connection in Offline	Indicates if the schedule runs the action the next time the managed device connects to the appliance, if the device is currently offline.
Delay Run After Reconnect	If configured, this option indicates the amount of time the schedule is delayed for. The time delay period begins when the update action is scheduled to run.
End After	If configured, this option indicates the maximum amount of time the schedule can run for. When this time limit is reached, any update tasks that are in progress are suspended.

3. In the *Schedule Status* section, review the overall schedule status on any of the following tabs:

Tab	Contents
By Machine	Devices selected for updating. Each entry displays the device name, its IP address, the update status (see Fields in the Patch Schedule Detail pages), update results, and the date the update completed. You can expand a device node to view the applicable updates. Each entry shows the update ID, associated Knowledge Base article number, update name, and the current status (Installed, Not Installed, Staged, and Detect, Stage, or Deploy Failure).
By Feature Update	Updates selected for detection, staging, and deployment. Each entry displays the update ID, associated Knowledge Base article number, update name, and the numbers of devices that are updated, not updated, and those that encountered detect or deploy failures.
Installed	Updates successfully installed on devices. Each entry displays the update ID, associated Knowledge Base article number, and the update name. You can expand an update node to view the devices on which the update is installed.

Tab	Contents
Not Installed	Updates that are not installed on devices. Each entry displays the update ID, associated Knowledge Base article number, and the update name. You can expand an update node to view the devices on which the update is to be installed.
Staged	Update that are staged for installation. Staging refers to update files being copied to the agent device for later deployment. Each entry displays the update ID, associated Knowledge Base article number, and the update name. You can expand an update node to view the devices on which the update is to be installed.
Detect Failures	Incomplete updates that resulted in a detection failure. Each entry displays the update ID, associated Knowledge Base, update name, and the associated error code (see Error codes caused by patching and scripting). You can expand an update node to view the devices on which the failure is encountered.
Stage Failures	Incomplete updates that resulted in a staging failure. Each entry displays the update ID, associated Knowledge Base article number, update name, and the associated error code (see Error codes caused by patching and scripting). You can expand an update node to view the devices on which the failure is encountered.
Deploy Failures	Incomplete updates that resulted in a deployment failure. Each entry displays the update ID, associated Knowledge Base, update name, and the associated error code (see Error codes caused by patching and scripting). You can expand an update node to view the devices on which the failure is encountered.

4. **Optional**. After reviewing the schedule details, you can perform any of the following actions:
   - To edit the update schedule, click **Edit**. For more information, see Configure Windows Feature Update schedules.
   - To run the update schedule, click **Run Now**.
   - To make a copy of the update schedule, click **Duplicate**.
   - To delete the update schedule, click **Delete**.

View available Windows Feature Updates

After you have subscribed to Windows Feature Updates, and the updates are downloaded, you can view the available updates.

You must subscribe to Windows Feature Update versions and select Feature Update download settings to view related updates. See:

- Subscribe to Windows Feature Updates
- Select patch and feature update download settings

1. Go to the *Windows Feature Update* list page:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Security**, then click **Windows Feature Updates**.
   c. On the *Windows Feature Updates* panel, click **Display available Windows Feature Updates** in the **Catalog** section.
2. Search for Windows Feature Updates.
   a. Enter the search criteria into the search box.

For example, `1909`.

b. Press **Enter**.

The list page refreshes, showing only the Windows Feature Updates whose version is 1909.

View Windows Feature Update status

Windows Feature Update details include vendor information and deployment status.

1. Go to the *Windows Feature Update Detail* page:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Security**, then click **Windows Feature Updates**.
   c. On the *Windows Feature Updates* panel, click **Display available Windows Feature Updates** in the **Catalog** section.
   d. Click a Windows Feature Update name.

   The *Windows Feature Update Detail* page appears, displaying complete information about the selected Windows Feature Update.

Managing Dell devices and updates

You can use the appliance to manage device updates from Dell.

These updates include:

- Software and firmware for servers
- Software and firmware for client devices
- Some Dell-supplied applications

NOTE: Server and client devices refer to Dell server and client hardware, not to their server or client OS.

Any Dell devices that need to be updated must have the Dell Open Manage Inventory Agent installed, either the client or the server version, as applicable. This component is included in all Dell Updates by default and there is no need to add it manually. If the Dell Open Manage inventory client does not exist on a target device, it is installed during the first deployment process.

NOTE: Dell hardware updates only work with the KACE Agent is 11.1 or higher. Older agent versions do not support this feature.

Run the *Supported Dell Models* report to see which Dell computers Dell Client Updates are supported for. See Running single-organization and consolidated reports.

Differences between patching and Dell Updates

The differences between patching and Dell Updates include differences in the subscription processes, in action names, and in location of management processes.

Differences between patching and Dell Updates are the following:

- Any Dell devices that need to be updated must have the Dell Open Manage Inventory Agent installed, either the client or the server version, as applicable.
- The Dell Update subscription process differs from the appliance patch subscription process. For instructions on subscribing to Dell Updates, see Select Dell Update download settings.
- The names used for patching actions differ:

Action	Patching Term	Dell Updates Term	Term Used in:
Install the patch or update on the devices you manage.	Deployment	Update	Managing Dell devices and updates

- You manage and run patching and Dell Updates from different places in the **Administrator Console**:

Action	Where to find it
Run Dell Updates	**Security** > **Dell Updates**
Manage Dell Updates	If the Organization component is **not enabled** on your appliance: **Administrator Console > Settings > Dell Update Download Settings** If the Organization component **is enabled** on your appliance: **System Administration Console > System** > **Settings** > **Dell Update Download Settings**
Run Patching Schedules	**Security** > **Schedules**
Manage Patching	**Security** > **Subscriptions**

Select Dell Update download settings

You must configure and schedule catalog updates before you create schedules to update devices.

Dell Update packages are provided in **catalogs**: one for servers and one for clients.

1. Go to the *Dell Update Download Settings* page:
   - **If the Organization component is not enabled on the appliance, click *Security*, then click *Dell Updates*.**
   - **If the Organization component is enabled on the appliance, log in to the appliance System Administration Console, `https://appliance_hostname/system`, or select System in the drop-down list in the top-right corner of the page, then select Settings > Control Panel.**
2. Click **Dell Update Download Settings**.

   The current status of the Dell catalog is displayed.
3. In the *Configure File Downloads* tab, select the following options.

Option	Description
Disabled	Prevents the downloading of Dell Update packages. This prevention includes the installers that are required to install the updates.

Option	Description
All files	Maintains a full cache of subscribed packages on your appliance. This option downloads all deployment packages, without checking to determine whether they are required for your environment.
Files detected as missing	Allows the appliance to determine which packages to download based on the results of Detect jobs. If a Dell Update detection signature has been detected as Not Installed on any managed device, the package is downloaded. If no managed devices are detected as Not Installed, no packages for this update are downloaded.
Delete unused files after __ days	Deletes Dell Update packages that have not been deployed in the specified number of days. Dell Updates that are marked as *Inactive* or *Disabled* are automatically deleted during the download process.

4. In the *Actions* tab, select the following options.

Option	Description
Update **Description** **Actions**	For each type of updates (*Signature* or *Update Files*), provides a description and access to the available actions: • **Check for Update**: Click to download Dell Update signature files. • **Delete**: Click to immediately remove all Dell Updates from the appliance. This can be useful if you no longer need any update and you want to quickly reclaim the disk space that they used. • **Run Now**: Click to immediately download the Dell Updates to which you have subscribed, regardless of the subscription schedule.

5. Select schedule options for Dell Update signatures in the *Schedule* section. File signatures include the security bulletins and other files that define Dell Updates downloaded from Quest.

Option	Description
Signature Download	Select **None** to prevent the downloading of Dell Update signatures.
Every day at the specified time	Select **day** to download Dell Update detection signatures every day, or select a day of the week to download once a week. Select the time to start the download. Time is displayed in 24-hour clock format, where 0 is midnight, 1:00 a.m. is 1 and 11:00 p.m. is 23. **NOTE:** When setting up Dell Update downloads, timing is important. The appliance activity log is created at 1:30, and maintenance tasks occur between 01:00 and 01:30. Quest recommends that you schedule Dell Update downloads to occur after the log and maintenance tasks are complete, which is about 3:00.
On the nth of every month or on a specific month at HH:MM	Select the day of the month to download Dell Update detection signatures on a monthly basis.

6. Set the schedule options for Dell Updates.

Option	Description
After signature download	Downloads packages after the signatures have been downloaded. This option is not available if the **Disabled** option is cleared in the *Configure File Downloads* section.
Every __ minutes	Specifies the frequency with which packages are downloaded. This option is available only if *Files detected as missing* in the *Configure File Downloads* section is selected.
Download Blackout: Start __ End __	Specifies a time period during which files cannot be downloaded. For example, use an early morning stop time to prevent the process from using a large amount of network bandwidth during regular working hours. If you select this option, the appliance stops file downloads at the specified time. It does not start file downloads again until the next specified download time. When the download resumes, it starts up where it left off. Downloads that are incomplete might not appear on the *Dell Update Catalog* page.

7. Click **Save**.

Configure Dell Update schedules

The appliance can automatically identify and install the firmware and driver updates required for your Dell clients and servers according to the schedule you set. If the Organization component is enabled on your appliance, you create Dell Update schedules for each organization separately.

Consider creating labels to group Dell Updates and devices. You can then use those labels when you create Dell Update schedules. For example, you could create a label that groups updates by application families, such as drivers or firmware. Or, you could group all Dell servers running Microsoft Windows 7 into a single label and then run a Dell Update schedule to bring them up to date. For more information about creating labels for updates and devices, see Using Smart Labels for patching.

1. Go to the *Dell Updates* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Security**, then click **Dell Updates**.
2. **Optional**: Review the available updates and inactivate the updates that you do not want to install.

    Updates are available only if the appliance settings are configured to download Dell catalog updates.

    To review and inactivate updates:

    a. On the *Dell Updates* panel, click **Show available updates** in the **Catalog** section.
    b. Select the check box next to an update.
    c. Select **Choose Action** > **Change Status to** > **Inactive**.
3. Schedule inventory and updates.

    This is similar to creating patch schedules in the *Patch Management* section. You can collect inventory independently, or as part of an inventory and update schedule that also installs the updates. Normally, inventory is performed automatically as part of an update schedule.

    To schedule inventory and updates:

    a. On the left navigation bar, click **Security**, then click **Dell Updates**.
    b. On the *Dell Updates* panel, in the **Schedules** section, click **Detect missing updates**.

        Or

        On the *Dell Updates* panel, in the Schedules section, click New Schedule to create a new Dell Update schedule.

c. Select **Choose Action** > **New**.

d. On the *Dell Update Schedules* list page, do one of the following:

To create a new Dell Update schedule using the *Schedule Detail* wizard, click **Choose Action** > **New (Wizard)**.

To create a new Dell Update schedule using the *Schedule Detail* page, click **Choose Action** > **New (Classic)**.

To edit an existing schedule, click the schedule name in the list, then on the *Dell Update Schedule Summary* page that appears, click **Edit**.

The *Schedule Detail* page or wizard appears, as selected. The same options are available in each selection. You can switch between the page and wizard by clicking Classic View or Wizard View in the top-right corner, as applicable.

e. Configure general information about the schedule:

Option	Description
Name	A name that identifies the schedule. This name appears on the *Dell Update Schedules* list page.
Description	A brief description of the Dell Update schedule.

f. Select one of the following actions.

These actions are identical to patch scheduling actions. See Configure patch schedules.

Action	Description
Detect	Scans for compatible Dell Updates.
Detect and Deploy	Scans for compatible Dell Updates, downloads the applicable files to the agent device, and deploys the update to the selected devices.
Deploy	Deploys the update to the selected devices.

NOTE: Dell Update deployment actions require a reboot of applicable managed devices.

g. Select the target devices using the following options.

These options are identical to the ones appearing in patch scheduling actions. See Configure patch schedules.

Normally, you create different schedules for laptops, workstations, and servers, because these three types of devices have very different usage characteristics.

Action	Description
All Devices	To apply this schedule to all managed devices, select this options. Clear the check box to limit the update action to specific labels or devices.
Device Labels	Restrict the action to the Dell updates using the labels that you select here. This is the most commonly used option. 1. Click **Manage Associated Labels**. 2. In the *Select Labels* dialog box that appears, drag one or more labels (as applicable) to the *Limit Run to* area, then click **OK**.

Action	Description
	To use this option, you must already have Smart Labels for the feature updates. See Using Smart Labels for patching.
Devices	Run Dell updates on the devices that you select. Only compatible Dell devices appear in the list. • To search for devices, begin typing in the field. • To remove all specified devices and start again, click **Remove All**. • Scoped users can see only those devices that are associated with their role, when the role is assigned a label. For more information about user roles, see Add or edit User Roles.
Operating Systems	Select the operating systems of the devices that you want to update. The default is all operating systems. When this option is configured, the schedule only applies to devices with the selected operating systems. 1. Click **Manage Operating Systems**. 2. In the **Operating Systems** dialog box that appears, select the OS versions in the navigation tree, as applicable. You have an option to select OS versions by their family, product, architecture, release ID, or build version. You can choose a specific build version, or a parent node, as needed. Selecting a parent node in the tree automatically selects the associated child nodes. This behavior allows you to select any future OS versions, as devices are added or upgraded in your managed environment. For example, to select all build current and future versions associated with the Windows 10 x64 architecture, under **Windows** > **Windows 10**, select **x64**.

h. Set an alert dialog to offer users a chance to delay or cancel the action:

Option	Description
Options	1. Silent- No alerts are shown. 2. OK- The schedule runs immediately. 3. Cancel- The schedule is cancelled until its next scheduled run. 4. Snooze- The user is prompted again after the Snooze Duration.

i. Set a reboot prompt dialog to offer users a chance to delay or snooze the reboot.

Option	Description
Options	1. Prompt User- Wait for the user to accept the reboot before restarting the device 2. No Reboot- The device does not reboot even though a reboot might be required for the patch to take effect. 3. Force Reboot- Reboot as soon as a patch requiring it is deployed. 4. Automatically reboot when no one is logged in- Automatically reboot the managed device if no users are logged in

j. In the *Schedule* tab, specify the applicable options for the schedule.

These options are identical to the ones appearing in patch scheduling actions. See Configure patch schedules.

Option	Description
None	Run in combination with an event rather than on a specific date or at a specific time. This option is useful if you want to patch servers manually, or perform patch actions that you do not want to run on a schedule.
Every _ hours	Run at a specified interval.
Every day/specific day at HH:MM	Run daily at a specified time, or run on a designated day of the week at a specified time.
Run on the nth **of every month/ specific month at HH:MM**	Run on the **n**th day every month, (for example, the first or the second) day of every month, or a specific month, at the specified time.
Run on the nth weekday of every month/specific month at HH:MM	Run on the specific weekday of every month, or a specific month, at the specified time.

Custom	Run according to a custom schedule.
	Use standard 5-field cron format (extended cron format is not supported):
	`* * * * *`
	`| | | | +————————day of week (0-6)(Sun=0)`
	`| | | +————————month (1-12)`
	`| | +————————day of month (1-31)`
	`| +————————hour (0-23)`
	`+————————minute (0-59)`
	Use the following when specifying values:
	• **Spaces ( )**: Separate each field with a space.
	• **Asterisks (*)**: Include the entire range of values in a field with an asterisk. For example, an asterisk in the hour field indicates every hour.
	• **Commas (,)**: Separate multiple values in a field with a comma. For example, `0,6` in the day of the week field indicates Sunday and Saturday.
	• **Hyphens (-)**: Indicate a range of values in a field with a hyphen. For example, `1-5` in the day of the week field is equivalent to `1,2,3,4,5`, which indicates Monday through Friday.
	• **Slashes (/)**: Specify the intervals at which to repeat an action with a slash. For example, `*/3` in the hour field is equivalent to `0,3,6,9,12,15,18,21`. The asterisk (`*`) specifies every hour, but `/3` restricts this to hours divisible by 3.
	Examples:
	• `15 * * * *` Run 15 minutes after every hour every day
	• `0 22 * * *` Run at 22:00 every day
	• `0 0 1 1,6 *` Run at 00:00 on January 1 and June 1
	• `30 8,12 * * 1-5` Run weekdays at 08:30 and 12:30
	• `0 2 */2 * *` Run every other day at 02:00

Option	Description
View Task Schedule	Click to view the task schedule. The *Task Schedule* dialog box displays a list of scheduled. Click a task to review the task details. For more information, see View task schedules.
Timezone	The timezone to use when scheduling the action. Select **Server** to use the timezone of the appliance. Select **Agent** to use the timezone of the managed device.
Run on next connection if offline	Run the action the next time the managed device connects to the appliance, if the device is currently offline. This option is useful for laptops and other devices that are periodically offline. If this option is not selected, and the device is offline, the action does not run again until the next scheduled time.
Delay run after reconnect	Delay the schedule by a specified amount of time. The time delay period begins when the patch action is scheduled to run.
End after	The time limit for patching actions. For example, if you schedule patches to run at 04:00, you might want all patching actions to stop at 07:00 to prevent bandwidth issues when users start work. To do so, you could specify **180** in the minutes box. When this time limit is reached, any patching tasks that are in progress are suspended, and their status on Security logs is *Suspended*. These patching tasks do not resume on the next run and instead start from the beginning with each scheduled patching action.

NOTE: The Agent Timezone is only available if there is a Dell device in inventory to pull the Timezone information from.

k. Click **Save**.

The schedule appears on the *Dell Update Schedules* page. The schedule is disabled by default.

TIP: Before you enable a schedule, test it on a small subset of the devices to make sure everything is working the way you expect.

l. To enable the schedule, select the check box next to the schedule name, then select **Choose Action** > **Enable**.

The inventory and update runs according to the specified schedule.

View Dell Update schedules

You can view summary information for the Dell Update schedules that exist on the appliance. If the Organization component is enabled on your appliance, you view Dell Update schedules for each organization separately.

1. Go to the *Dell Update Schedules* page:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Security**, then click **Dell Updates**.
2. On the *Dell Updates* panel, click **Detect missing updates** or **Deploy available updates** in the **Schedules** section

Columns available on the *Dell Update Update Schedules* page are identical to the ones on the *Patch Schedules* page. For more information about the fields on the *Patch Schedules* page, see View a list of patch schedules.

3. (Optional) To change column visibility, select **Column Visibility** from the *Table Options* drop-down list above the table on the right.

Review Dell Update schedule details

When you configure a Dell Update schedule, this page displays details about the schedule configuration and its status.

1. Go to the *Update Schedule Summary* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Security**, then click **Dell Updates**.
    c. On the *Dell Updates* panel, in the **Schedules** section, click **Detect missing updates**.
    d. Click the name of a schedule.
2. Review the contents of the *Configuration* section.

Option	Description
Created	The date and time the schedule is created.
Modified	The date and time the schedule is last modified.
Last Run	The date and time the schedule is last run.
Name	A name that identifies the schedule. This name appears on the *Dell Update Schedules* list page.
Action	The action associated with the schedule: • **Detect**: Scans for compatible Dell Updates. • **Detect and Deploy**: Scans for compatible Dell Updates, and downloads the applicable files to the agent device for later deployment. • **Deploy**: Deploys the update to the selected devices.
Description	A brief description of the Dell Update schedule.
Devices	This field only appears when the schedule is configured to apply to all devices.
Device Label	One or more Smart Labels associated with the devices against which the schedule runs. For more information, see Using Smart Labels for patching. This field only appears when the schedule is configured to apply to selected devices.
Device Name	One or more selected devices against which the schedule runs. This field only appears when the schedule is configured to apply to selected devices.
Detect Label	One or more Smart Labels associated with the scheduled updates. For more information, see Using Smart Labels for patching. This field only appears when the schedule is configured to detect selected updates.

Option	Description
Alerts	**Detect and Deploy schedules only**. The alerts displayed to users when update actions run: • **OK**: Run immediately. • **Cancel**: Cancel until the next scheduled run. • **Snooze**: Prompt the user again after the *Snooze Duration*.
Reboot	**Detect and Deploy schedules only**. The options for rebooting the managed device: • **No Reboot**: The device does not reboot even though a reboot might be required for the update to take effect. This option is not recommended because deploying updates without rebooting when required can leave systems unstable. Further, updates that require reboots are only shown as deployed after the reboot. • **Prompt User**: Waits for the user to accept the reboot before restarting the device. If the user snoozes or cancels the reboot, the update stops until a reboot occurs. Selecting a Snooze Duration in the agent dialog box that appears on the target device pauses the reboot prompt for the specified snooze interval. • **Force Reboot**: Reboots as soon as an update that requires it is deployed. Forced reboots cannot be canceled. Force Reboot works well for desktops and servers. You might not want to force reboot on laptops. Force Reboot works well with servers because they usually have no dedicated users. However, it is important to warn users that services will not be available when servers are being updated and re-booted. See Best practices for patching.
Schedule	The selected update schedule. Click **View Task Schedule** to see a detailed task scheduler. In the dialog box that appears, click a task to review the task details. For more information, see View task schedules.
Run on Next Connection in Offline	Indicates if the schedule runs the action the next time the managed device connects to the appliance, if the device is currently offline.
Timezone	If this option is configured, it specifies the time zone to use when scheduling related action. When set to Server, the schedule uses the appliance time zone. If it's set to Agent, it uses the time zone of the managed device.
Delay Run After Reconnect	If configured, this option indicates the amount of time the schedule is delayed for. The time delay period begins when the update action is scheduled to run.
End After	If configured, this option indicates the maximum amount of time the schedule can run for. When this time limit is reached, any update tasks that are in progress are suspended.

3. In the *Schedule Status* section, review the overall schedule status on any of the following tabs:

Tab	Contents
By Machine	Devices selected for updating. Each entry displays the device name, its IP address, the update status (see Fields in the Patch Schedule Detail pages), update results, and the date the update is completed. You can expand a device node to view the applicable updates. Each entry shows the update ID, associated Knowledge Base article number, update name, the current status (Installed, Not Installed, or Deploy Failure), and the date the update is detected.

Tab	Contents
By Update	Updates selected for detection and deployment. Each entry displays the update ID, associated Knowledge Base article number, update name, and the numbers of devices that are updated, not updated, and those that encountered detect or deploy failures.
Installed	Updates successfully installed on devices. Each entry displays the update ID, associated Knowledge Base article number, and the update name. You can expand an update node to view the devices on which the update is installed.
Not Installed	Updates that are not installed on devices. Each entry displays the update ID, associated Knowledge Base article number, and the update name. You can expand an update node to view the devices on which the update is to be installed.
Detect Failures	Incomplete updates that resulted in a detection failure. Each entry displays the update ID, associated Knowledge Base, update name, and the associated error code (see Error codes caused by patching and scripting). You can expand an update node to view the devices on which the failure is encountered.
Deploy Failures	Incomplete updates that resulted in a deployment failure. Each entry displays the update ID, associated Knowledge Base, update name, and the associated error code (see Error codes caused by patching and scripting). You can expand an update node to view the devices on which the failure is encountered.

4. **Optional**. After reviewing the schedule details, you can perform any of the following actions:
   - To edit the update schedule, click **Edit**. For more information, see Configure Windows Feature Update schedules.
   - To run the update schedule, click **Run Now**.
   - To make a copy of the update schedule, click **Duplicate**.
   - To delete the update schedule, click **Delete**.

View available Dell Updates

You can review the list of Dell updates in the Dell Update Catalog.

You must select Dell Update download settings to view related updates. See Select Dell Update download settings. When all Dell Update signature files are downloaded, the Dell Update Catalog lists the related updates.

NOTE: The *Severity* column on this page uses the Microsoft security standards which do no match the Dell severity levels:

Severity level displayed	Corresponding Dell severity level
Moderate	Optional
Important	Recommended
Critical	Urgent

1. Go to the *Dell Update Catalog* list page:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.

b. On the left navigation bar, click **Security**, then click **Dell Updates**.
c. On the *Dell Updates* panel, click **Show available updates** in the **Catalog** section.

2. Search for Dell Updates.
   a. Enter the search criteria into the search box.

      For example, `2021`.

   b. Press **Enter**.

      The list page refreshes, showing only the Dell Updates whose version is 2021.

View Dell Update status

Dell Update details include vendor information and deployment status.

1. Go to the *Dell Update Catalog* page:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Security**, then click **Dell Updates**.
   c. On the *Dell Updates* panel, click **Show available updates** in the **Catalog** section.
   d. Click the name of a Dell Update.

      The *Dell Update Detail* page appears, displaying complete information about the selected update.

Managing Linux package upgrades

Linux package upgrades improve the overall performance of your managed Linux devices and protect them from potential vulnerabilities.

The appliance allows you to automate the process of installing and managing Linux package upgrades. It relies on individual Linux package repositories, and the assumption that your managed Linux devices point to the appropriate repository.

Also, the appliance only detects the packages that include security updates, that are identified as such in each Linux repository. It does not attempt to detect or upgrade all packages, or to upgrade the entire OS on managed devices to the latest version.

NOTE: Linux Raspberry Pi OS and CentOS do not make a distinction between regular and security updates. Detecting and upgrading packages for a managed Raspberry Pi OS and CentOS device results in all updated packages being installed on the device.

NOTE: The term *update* in KACE Systems Management Appliance assumes the following: if there are new versions of the packages available in the distribution's repositories, the appliance uses the standard system commands to ensure that the system installs the latest version possible. This is not in any way meant to be exactly the same way that the word *update* (or *upgrade*) is used in the underlying system commands.

View Linux package upgrade schedules

You can view summary information for the Linux package upgrade schedules that exist on the appliance. If the Organization component is enabled on your appliance, you view these schedules for each organization separately.

1. Go to the *Windows Feature Update Schedules* page:

a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.

b. On the left navigation bar, click **Security**, then click **Linux Package Upgrades**.

2. On the *Linux Package Upgrades* panel, click **Detect missing package upgrades** in the **Schedules** section.

Columns available on the *Linux Package Upgrade Schedules* page are very similar to the ones on the *Patch Schedules* page. For more information about the fields on the *Patch Schedules* page, see View a list of patch schedules.

3. (Optional) To change column visibility, select **Column Visibility** from the *Table Options* drop-down list above the table on the right.

Configure Linux package upgrade schedules

You can create and configure Linux package upgrade schedules and set a time for them to run.

1. Start the Linux package upgrade wizard:

a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.

b. On the left navigation bar, click **Security**, then click **Linux Package Upgrades**.

c. On the *Linux Package Upgrades Management* panel, click **New Schedule link** in the **Schedules** section to directly open the *Linux Package Upgrades Schedule Detail* page.

Or

On the *Linux Package Upgrades Management* panel, click Detect and Deploy package upgrades in the Schedules section.

d. On the *Linux Package Upgrade Schedules* list page, do one of the following:

To create a new Linux package upgrade schedule, click **Choose Action** > **New**.

To edit an existing schedule, click the schedule name in the list, then on the *Linux Package Upgrade Summary* page that appears, click **Edit**.

The *Schedule Detail* page appears.

2. In the *Schedule Detail* wizard, on the *General Information* page, configure general information about the schedule:

Option	Description
Name	A name that identifies the schedule. This name appears on the *Linux Package Upgrade Schedules* list page.
Description	A brief description of the Linux package upgrade schedule.

3. On the *Action* tab, complete the following steps:

a. Under *Action*, select one of the following actions.

The results of the selected action depends on whether your managed Linux devices are associated with their applicable package repository. To select all applicable devices, ensure that each of your managed devices is using the appropriate package repository.

NOTE: The appliance only scans for the packages that include security updates, that are identified such in each Linux repository, except Linux Raspberry Pi. It does not attempt to detect or upgrade all packages, or to upgrade the entire OS on managed devices to the latest version. The Linux Raspberry Pi repository, however, does not make a distinction between regular and security updates. Detecting and upgrading packages for managed Raspberry Pi OS devices results in all updated packages being installed on those devices.

Action	Description
Detect All	Scans for all Linux package upgrades that include security updates.
Detect and Upgrade All	Scans for all Linux package upgrades that include security updates, downloads the applicable files, and deploys the upgrade to the selected devices.

b. Under *Detect Timeout*, select the amount of time for the detect action to complete.

c. **Detect and Upgrade All actions only.** Under *Upgrade Timeout*, select the amount of time for the upgrade action to complete.

d. Select the *Security Patches Only* to detect the security patches. Cancel the selection to deploy all the patches.

4. Click **Next**.
5. On the *Devices* tab, specify the devices you want to associate with this schedule.

These options are identical to the ones appearing in patch scheduling actions. For instructions, see Configure patch schedules.

Action	Description
All Devices	To apply this schedule to all managed devices, select this option. Clear the check box to limit the patch action to specific labels or devices.
Device Labels	Restrict the action to the feature updates using the associated labels that you select. This is the most commonly used option. 1. Click **Manage Associated Labels**. 2. In the *Select Labels* dialog box that appears, drag one or more labels (as applicable) to the *Limit Run to* area, then click **OK**. To use this option, you must already have Smart Labels for the feature updates. See Using Smart Labels for patching.
Devices	Run patch actions on the devices that you select. The list that appears shows only applicable Linux devices. • To search for devices, begin typing in the field. • To remove all specified devices and start again, click **Remove All**. • Scoped users can see only those devices that are associated with their role, when the role is assigned a label. For more information about user roles, see Add or edit User Roles.
Operating Systems	Select the operating systems of the devices that you want to upgrade. Only applicable Linux operating systems appear in the dialog box. The default is all operating systems. When this option is configured, the schedule only applies to devices with the selected operating systems. 1. Click **Manage Operating Systems**. 2. In the **Operating Systems** dialog box that appears, select the OS versions in the navigation tree, as applicable. You have an option to select OS versions by their family, product, architecture, release ID, or build version. You can choose a specific build version, or a parent node, as needed. Selecting a parent node in the tree automatically selects the associated child nodes. This behavior allows you to select any future OS versions, as devices are added or upgraded in your managed environment. For example, to

Action	Description
	select all build current and future versions associated with the Linux Ubuntu x86_64 architecture, under **Linux** > **Ubuntu**, select **x64**.

6. Click **Next**.
7. In the *Schedule* tab, specify the applicable options for the schedule.

These options are identical to the ones appearing in patch scheduling actions. For instructions, see Configure patch schedules.

Action	Description
None	Run in combination with an event rather than on a specific date or at a specific time. This option is useful if you want to patch servers manually, or perform patch actions that you do not want to run on a schedule.
Every _ hours	Run at a specified interval.
Every day/specific day at HH:MM	Run daily at a specified time, or run on a designated day of the week at a specified time.
Run on the nth **of every month/specific month at HH:MM**	Run on the **n**th day every month, (for example, the first or the second) day of every month, or a specific month, at the specified time.
Run on the nth weekday of every month/specific month at HH:MM	Run on the specific weekday of every month, or a specific month, at the specified time.

Custom	Run according to a custom schedule.
	Use standard 5-field cron format (extended cron format is not supported):
	`* * * * *`
	`| | | | +————————day of week (0-6)(Sun=0)`
	`| | | +————————month (1-12)`
	`| | +————————day of month (1-31)`
	`| +————————hour (0-23)`
	`+————————minute (0-59)`
	Use the following when specifying values:
	• **Spaces ( )**: Separate each field with a space.
	• **Asterisks (*)**: Include the entire range of values in a field with an asterisk. For example, an asterisk in the hour field indicates every hour.
	• **Commas (,)**: Separate multiple values in a field with a comma. For example, `0,6` in the day of the week field indicates Sunday and Saturday.
	• **Hyphens (-)**: Indicate a range of values in a field with a hyphen. For example, `1-5` in the day of the week field is equivalent to `1,2,3,4,5`, which indicates Monday through Friday.
	• **Slashes (/)**: Specify the intervals at which to repeat an action with a slash. For example, `*/3` in the hour field is equivalent to `0,3,6,9,12,15,18,21`. The asterisk (`*`) specifies every hour, but `/3` restricts this to hours divisible by 3.

Action	Description
	Examples: • `15 * * * *` Run 15 minutes after every hour every day • `0 22 * * *` Run at 22:00 every day • `0 0 1 1,6 *` Run at 00:00 on January 1 and June 1 • `30 8,12 * * 1-5` Run weekdays at 08:30 and 12:30 • `0 2 */2 * *` Run every other day at 02:00
View Task Schedule	Click to view the task schedule. The *Task Schedule* dialog box displays a list of scheduled. Click a task to review the task details. For more information, see View task schedules.
Run on next connection if offline	Run the action the next time the managed device connects to the appliance, if the device is currently offline. This option is useful for the devices that are periodically offline. If this option is not selected, and the device is offline, the action does not run again until the next scheduled time.

8. Click **Save**.

   The *Linux Upgrade Package Schedule Summary* page appears, displaying the newly created or updated schedule. For more information about this page, see Review Linux package upgrade schedule details. If you added any devices that match the Smart Label criteria, they are automatically included in the upgrade schedule.

Review Linux package upgrade schedule details

When you configure a Linux package upgrade schedule, this page displays details about the schedule configuration and its status.

1. Go to the *Linux Package Upgrade Schedule Summary* page:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Security**, then click **Linux Package Upgrades**.
   c. On the *Linux Package Upgrades Management* panel, click **Detect missing package upgrades** in the **Schedules** section.
   d. Click the name of a Linux package upgrade schedule.
2. Review the *Devices Targeted* field. This number specifies the number of Linux devices that are selected for upgrade, as specified in the schedule.
3. Review the contents of the *Configuration* tab.

Option	Description
Devices Targeted	the number of Linux devices that are selected for upgrade,
Created	The date and time the schedule is created.
Modified	The date and time the schedule is last modified.

Option	Description
Last Run	The date and time the schedule is last run.
Name	A name that identifies the schedule. This name appears on the *Linux Package Upgrade Schedules* list page.
Action	The action associated with the schedule: • **Detect All**: Scans for all Linux package upgrades. • **Detect and Upgrade All:** Scans for all Linux package upgrades, downloads the applicable files, and deploys them update to the selected devices.
Description	A brief description of the Linux package upgrade schedule.
Devices	This field only appears when the schedule is configured to apply to all devices.
Device Label	One or more Smart Labels associated with the devices against which the schedule runs. For more information, see Using Smart Labels for patching. This field only appears when the schedule is configured to apply to selected devices.
Device Name	One or more selected devices against which the schedule runs. This field only appears when the schedule is configured to apply to selected devices.
Schedule	The selected update schedule. Click **View Task Schedule** to see a detailed task scheduler. In the dialog box that appears, click a task to review the task details. For more information, see View task schedules.
Run on Next Connection if Offline	Indicates if the schedule runs the action the next time the managed device connects to the appliance, if the device is currently offline.
Delay Run After Reconnect	If configured, this option indicates the amount of time the schedule is delayed for. The time delay period begins when the update action is scheduled to run.
End After	If configured, this option indicates the maximum amount of time the schedule can run for. When this time limit is reached, any update tasks that are in progress are suspended.

4. In the *Schedule Status* tab, review the overall patch schedule status on any of the following tabs:

Tab	Contents
By Machine	Devices selected for upgrading. Each entry displays the device name, its IP address, the upgrade status, upgrade results, and the date the upgrade completed, if applicable. You can expand a device node to view additional information about each package, such as the package name, version, compatible OS name, whether the package is installed on the device, and the date it is detected.
By Package	Upgrades selected for detection and installation. Each entry displays the package name, its version, compatible OS name, package ID, and indicates if the package is installed.

Tab	Contents
Needs Upgrade	Upgrades that can be installed on devices. Each entry displays the package name, version, and the compatible OS name. You can expand an update node to view the devices on which the update is to be installed.
Deploy Failures	Incomplete updates that resulted in a deployment failure. Each entry displays the update ID, associated Knowledge Base, update name, and the associated error code (see Error codes caused by patching and scripting). You can expand an update node to view the devices on which the failure is encountered.

5. **Optional**. After reviewing the schedule details, you can perform any of the following actions:
   - To edit the schedule, click **Edit**. For more information, see Configure Windows Feature Update schedules.
   - To run the schedule, click **Run Now**.
   - To make a copy of the schedule, click **Duplicate**.
   - To delete the schedule, click **Delete**.

Review Linux package upgrades

As you run the Detect All action, the appliance generates a list of packages that are available for upgrade.

Use the *Packages* list page to see the latest Linux packages that are available for upgrade, and installed on managed devices. Start by selecting a specific Linux OS, and review contents of the list to get an overall estimate of the device pool that requires an update.

For each package, the list shows the numbers of devices on which the package is installed or not installed, and the percent of the devices that are running the latest version.

1. Go to the *Packages* list page:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Security**, then click **Linux Package Upgrades**.
   c. On the *Linux Package Upgrades Management* panel, click **Package Upgrade**.
2. In the *Packages* list page, click **View By**, and select a Linux OS. For example, *RHEL* or *Ubuntu*.

   The list refreshes, showing the packages detected for the selected OS.
3. Review the contents of the list. The following columns are available:

Column	Description
Package Name	The name of the detected package.
Version	The latest package version.
Installed	The number of managed Linux devices running the selected Linux OS on which the package is installed. Click the number in this column to display a list of these devices in the *Devices* list page.
Needs Upgrade	The number of managed Linux devices running the selected Linux OS that have an earlier version of this package and are candidates for an upgrade. Click the number in this column to display a list of these devices in the *Devices* list page.
Completion	The percentage of all devices that have this package installed.

Manage quarantined file attachments

The appliance includes a malware scanning feature for Service Desk file attachments. An automated process on the appliance ensures that the virus definition lists are updated on a regular basis. Any files attached to Service Desk tickets, and also any attachments to ticket-related email are scanned before they are added to the tickets.

Quarantined files are listed on the *Antivirus Quarantine* page. Use this page to review and manage quarantined Service Desk attachments. A notification appears when a threat is detected, with a link to the device associated with the file. You can also create notifications when specific kinds of threats are detected, or based on their status change. The

1. Go to the *Antivirus Quarantine* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Security**, then click **Antivirus Quarantine**.

    By default, the *Antivirus Quarantine* page displays new threats that have not been rejected or released from the quarantine. These items are always included in the appliance backup. You can filter this list using the *View By* menu, as required.

    NOTE: The *Filename* column displays quarantined files as hyperlinks. Clicking a link opens the *Antivirus Quarantine File Details* page. This page shows details of the quarantined file, including its upload source.

2. Review the list of files and perform applicable actions.

    For each quarantined file, the list displays its name, the time the file was first and last seen, the name of the malware variant, and additional information about the file's release or rejection, as applicable.

    # To enable access to a quarantined file in the associated Service Desk ticket, select it in the list and click **Choose Action** > **Release**.
    # To block access to a quarantined file in the Service Desk ticket, select it in the list and click **Choose Action** > **Reject**.
    # To delete a quarantined file from the Service Desk ticket, select it in the list and click **Choose Action** > **Delete**

    The Choose Action menu also allows you to export the list, or to create a report.

Using reports and scheduling notifications

You can configure the appliance to run reports and send notifications to administrators when specified criteria are met.

About reports and notifications

The appliance enables you to create and schedule a variety of reports and notifications. Reports collect information about inventory items, and notifications enable the appliance to alert you by email when specified criteria are met.

About reports

The appliance includes many standard reports for software, hardware, Service Desk, and other items.

If the Organization component is enabled on your appliance, you can create and run reports for each organization and for the System-level separately. System-level reports include consolidated reports that aggregate information from all organizations, as well as standard reports for various appliance components.

About notifications

Notifications are email messages the appliance sends to administrators when devices, scan results, and assets meet specified criteria.

For example, if you want to notify administrators when devices approach disk space limits, you can set up alerts based on disk usage. Notifications are sent when devices meet the specified criteria.

The appliance checks inventory against the criteria in the notification schedules at the specified frequency. When an item meets the criteria, the appliance sends email to the specified recipients.

By default, the appliance checks inventory every hour. To change the frequency, edit the notification schedule. See Edit notification schedules.

NOTE: Notifications and daily reports come from the default address, Charlie Root, (`root@`**appliance_hostname**) and you cannot modify this address.

Tracking changes to report settings

If History subscriptions are configured to retain information, you can view the details of the changes made to settings, assets, and objects.

This information includes the date the change was made and the user who made the change, which can be useful during troubleshooting. See About history settings.

Creating and modifying reports

You can create reports from list pages using SQL queries and from the *Reporting* section using the report wizard.

Creating reports

You can create reports to collect and analyze data, such as inventory information.

There are several ways to create reports:

- Use the report wizard on the Reports page. See Create reports using the report wizard.
- Use the SQL report form on the Reports page. See Create reports using SQL queries.
- Use the menu option on list pages, such as *Devices*, *Assets*, *Managed Installations*, and so on. See Create reports from list pages.

In addition, you can create charts and graphs by generating reports in XSL (Microsoft Excel) or CSV (comma-separated value) format, then importing the data into a tool such as Microsoft Excel.

NOTE: Be aware that multibyte characters, such as those used to support Japanese and Chinese character sets, might display as "garbage characters" when CSV files are imported to Excel. For more information, contact **Quest Support** at https://support.quest.com/contact-support.

Create reports using the report wizard

You can use the report wizard to identify the information you want to collect from the database without writing SQL queries.

1. Go to the *Reports* list by doing one of the following:
   - **If your appliance has the Organization component enabled, and you want to access a System-level report:**

     Log in to the appliance System Administration Console, `https://`**appliance_hostname**`/system`, or select **System** from the drop-down list in the top-right corner of the page. Then click **Reporting**.
     System-level reports include consolidated reports that aggregate information from all organizations, as well as standard reports for various appliance components.
   - **If your appliance does not have the Organization component enabled, or if you want to access an organization-level report, log in to the appliance Administrator Console, `https://appliance_hostname/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information. Then click Reporting.**

     Organization-level reports include standard reports for various appliance components. If the Organization component is enabled on your appliance, these reports provide information specific to the selected organization.

   The *Reports* list appears.
2. Select **Choose Action** > **New > Wizard** to display the *Step 1 of 7- Title and Topic* page.
3. Specify the following settings:

Option	Description
Title	The display name of the report, which appears on the report list. Make the title as descriptive as possible, so you can distinguish the report from others in the list.
Category	The category of the report. If the category does not already exist, it is added to the drop-down list on the *Reports* page.

Option	Description
Description	A description of the report.
Show Line Numbers	Display a column with line numbers on the report.
Topic	The topic of the report. This setting determines the fields that are available for the report.
Add Subtopic	Click this link to add up to two related topics to the report. This enables you to show relationships between up to three types of data in the same report. When you generate the report in HTML format, you can expand and collapse the rows to drill down into the information as needed. When you click **add a subtopic**, additional options become available, depending on the topic you select. For example, if you select **Device**, **Software**, and **File Synchronization**, the following two check boxes appear: • Only show rows from **Device** with at least one **File Synchronization** row. • Only show rows from **File Synchronization** with at least one **Software** row. Selecting these check boxes would limit the report to devices and software that have at least one child row. Device rows would appear in the report only if they have at least one corresponding software row; Software rows would appear in the report only if they have at least one corresponding File Synchronization row. Clear these check boxes to show all device and software rows regardless of whether they contain any software or File Synchronization rows, respectively. **NOTE:** If you add Subtopic to your report, Steps 6 and 7 will no longer be available, and you will not be able to create a dashboard report.

4. Click **Next** to display the *Step 2 of 7 - Fields to Display* page.
5. Select the fields that you want to include in the report.
6. Click **Next** to display the *Step 3 of 7 - Column Order* page.
7. Drag the fields, from top to bottom, to set the order in which column headings appear. In the report output, columns headings appear in left-to-right order.
8. Click **Next** to display the *Step 4 of 7 - Sort and Breaks* page.
9. Configure how the rows are arranged:
   # **Order By**: Specify how the results are sorted. Report data is organized by the selection in the first field, and then by the second field, and then by the third field. The first sort field is populated with the first field selected to be displayed on the report output page.
   # **Sequence**: Specify whether to display the results in ascending or descending alphanumeric order.
   # **Break Header**: Choose whether to group results under a subheading using the name of the field selected in *Order By*.
10. Click **Next** to display the *Step 5 of 7 - Filters* page.
11. **Optional**: If you do not want to return the entire data set in your report, add filter criteria:
    a. Click **Specify rules to filter the records**.

       A rule set, with *Match all of the following* **appears. These rules are equivalent to and statements in Boolean logic. To appear in the report, items must match all of the rules in this section.**

    b. Specify filter criteria, then click **Save**.
    c. To add a rule to the current rule set, click the **Add** button +.

d. Select filter criteria, then click **Add** at the right of the row.

e. To add a subset of rules, click the **Add Subset** button: .

The first nested subset adds a Match any of the following set of rules. These rules are equivalent to or statements in Boolean logic. This enables you to nest or criteria under the top-level and criteria. To appear in the report, items must match the criteria in the Match all of the following rule set and at least one criterion in the Match any of the following rule set.

f. Click **Add** next to the rule set.

g. Add additional rules and rule subsets as needed.

12. Click **Finish**.

The *Reports* page appears with the new report listed. The *View By* list, which appears above the table on the right, is automatically set to the category of the new report.

NOTE: Clicking **Finish** completes the creation of a regular report. To create a dashboard report using the wizard, see Create dashboard widget using report wizard .

13. To run the report, click a format in the *Generate Report* column.

The output is generated. The first data column is automatically linked to the detail page for the item in the Administrator Console.

Create dashboard report using report wizard

The Report wizard offers a guided interface to help users create customized, interactive report widgets. You can use the report wizard to identify the information you want to collect from the database without writing SQL queries.

1. Go to the *Reports* list by doing one of the following:

   - **If your appliance has the Organization component enabled, and you want to access a System-level report:**

     Log in to the appliance System Administration Console, `https://`**appliance_hostname**`/system`, or select **System** from the drop-down list in the top-right corner of the page. Then click **Reporting**.
     System-level reports include consolidated reports that aggregate information from all organizations, as well as standard reports for various appliance components.

   - **If your appliance does not have the Organization component enabled, or if you want to access an organization-level report, log in to the appliance Administrator Console, `https://appliance_hostname/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information. Then click Reporting.**

     Organization-level reports include standard reports for various appliance components. If the Organization component is enabled on your appliance, these reports provide information specific to the selected organization.

   The *Reports* list appears.

2. Select **Choose Action** > **New** > **Wizard** to display the *Step 1 of 7- Title and Topic* page.
3. Specify the following settings:

Option	Description
Title	The display name of the report, which appears on the report list. Make the title as descriptive as possible, so you can distinguish the report from others in the list.
Category	The category of the report. If the category does not already exist, it is added to the drop-down list on the *Reports* page.
Description	A description of the report.

Option	Description
Show Line Numbers	Display a column with line numbers on the report.
Topic	The topic of the report. This setting determines the fields that are available for the report.
Add Subtopic	Dashboard report only supports a single topic. **NOTE:** If you add Subtopic to your report, Steps 6 and 7 will no longer be available, and you will not be able to create a dashboard widget.

4. Click **Next** to display the *Step 2 of 7 - Fields to Display* page.
5. Select the fields that you want to include in the report.
6. Click **Next** to display the *Step 3 of 7 - Column Order* page.
7. Drag the fields, from top to bottom, to set the order in which column headings appear. In the report output, columns headings appear in left-to-right order.
8. Click **Next** to display the *Step 4 of 7 - Sort and Breaks* page.
9. Configure how the rows are arranged:
   - **Order By**: Specify how the results are sorted. Report data is organized by the selection in the first field, and then by the second field, and then by the third field. The first sort field is populated with the first field selected to be displayed on the report output page.
   - **Sequence**: Specify whether to display the results in ascending or descending alphanumeric order.
   - **Break Header**: Choose whether to group results under a subheading using the name of the field selected in *Order By*.
10. Click **Next** to display the *Step 5 of 7 - Filters* page.
11. **Optional**: If you do not want to return the entire data set in your report, add filter criteria:
    a. Click **Specify rules to filter the records**.

       A rule set, with *Match all of the following* appears. These rules are equivalent to and statements in Boolean logic. To appear in the report, items must match all of the rules in this section.

    b. Specify filter criteria, then click **Save**.
    c. To add a rule to the current rule set, click the **Add** button +.
    d. Select filter criteria, then click **Add** at the right of the row.
    e. To add a subset of rules, click the **Add Subset** button: .

       The first nested subset adds a Match any of the following set of rules. These rules are equivalent to or statements in Boolean logic. This enables you to nest or criteria under the top-level and criteria. To appear in the report, items must match the criteria in the Match all of the following rule set and at least one criterion in the Match any of the following rule set.

    f. Click **Add** next to the rule set.
    g. Add additional rules and rule subsets as needed.
12. To apply aggregation functions to summarize key metrics, click **Create Dashboard Widget** to display the *Step 6 of 7 - Aggregation* page.

This allows you to group your report data based on selected fields and apply aggregation functions to summarize key metrics.

a. In the **Group By** section, select one or more fields to define how the data should be grouped in the widget.

NOTE: Grouping allows you to categorize data into meaningful segments, making it easier to identify patterns, and trends.

Here's an example **Patch By Severity** report,

Topic: Patch

Group By: Severity (*Critical, Important, Low, Moderate, Recommended*)

Aggregation Function: Field= Severity; Function = Count.

For more information, refer the Pie Chart in the Configuring Chart Types for a Report

b. To add a field, click the + icon, select the field from the drop-down, and then click the **Add** button .

c. In the **Aggregate Function** section, select a field to aggregate and choose an appropriate function, such as Summation, Average, Count, Minimum, or Maximum, to calculate key metrics. Aggregation helps in condensing large datasets into meaningful insights by applying these functions to grouped data.

d. To add a field, click the + icon, select the field from the drop-down, and then click the **Add** button .

e. In the **Post-Aggregate Sorting** section, select the field to sort the results. Sorting is applied after the data has been grouped and aggregated.

f. To add a field, click the + icon, select the field and its sequence from the drop-down, and then click the **Add** button .

g. In the **Limit Result** section, type the number of rows you want to display in the **Number of Rows** field. This limits how many rows of data are shown in the dashboard report

13. Click **Next** to display the *Step 7of 7 - Configure Chart* page. This step enables you to configure and preview your dashboard chart.

    a. From the **Please select the chart type you want to use** drop-down list, select the chart type. Depending upon the chart type you select, the relevant fields populate in the **Label and Axis Settings** section.

    b. In the **Label and Axis Settings** section, enter appropriate values to configure the populated key elements for the widget based on the chart type selection.

    For more information, refer the Configuring Chart Types for a Report.

    c. In the **Publish Settings** section, configure how your dashboard is published, including visibility and access permissions. For more information, refer the Configuring Chart Types for a Report.

    d. In the **Visualization Settings** section, configure visual details like legend placement, chart subtitles, fill settings. For more information, refer the Configuring Chart Types for a Report.

14. Click **Preview Chart** to view how the chart will appear using the selected configuration.
15. Click **Finish**.

    The *Reports* page appears with the new report listed. The *View By* list, which appears above the table on the right, is automatically set to the category of the new report.

16. To run the report, click a format in the *Generate Report* column.

    The output is generated. The first data column is automatically linked to the detail page for the item in the Administrator Console.

17. New report widget is created and based on the Dashboard permission user can add the widget into respective dashboards. For more information on how to add widgets to the dashboard, refer Adding a Widget.

Create reports using SQL queries

You can create reports by entering SQL queries on the report form.

If you do not know the SQL queries to use, consider using the report wizard. See Create reports using the report wizard.

1. Go to the *Reports* list by doing one of the following:

    - **If your appliance has the Organization component enabled, and you want to access a System-level report:**

      Log in to the appliance System Administration Console, `https://`**appliance_hostname**`/system`, or select **System** from the drop-down list in the top-right corner of the page. Then click **Reporting**.

System-level reports include consolidated reports that aggregate information from all organizations, as well as standard reports for various appliance components.

- **If your appliance does not have the Organization component enabled, or if you want to access an organization-level report, log in to the appliance Administrator Console, `https://appliance_hostname/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information. Then click Reporting.**

  Organization-level reports include standard reports for various appliance components. If the Organization component is enabled on your appliance, these reports provide information specific to the selected organization.

The *Reports* list appears.

2. Select **Choose Action** > **New >SQL** to display the *Report Detail* page.
3. Specify report settings:

Option	Description
Title	The display name of the report, which appears on the report list. Make the title as descriptive as possible, so you can distinguish the report from others in the list.
Description	A description of the report.
Category	The category of the report. If the category does not already exist, it is added to the drop-down list on the *Reports* page.
Break on Columns	A comma-separated list of SQL column names. The report generates break headers and subtotals for these columns.
Show Line Numbers	Display a column with line numbers on the report.
SQL	The query statement that generates the report data. For more information, go to the MySQL documentation at http://dev.mysql.com/doc/refman/5.0/en/. When writing a report or query against the Service Desk HD_Ticket table, be aware that the *User* custom field stores the user ID from the USER table in the HD_TICKET table, which is the table that holds the ticket record. If you want to display the username instead of the user ID in the report, you need to JOIN on the USER table. See Database table names.
Organization settings	These settings are available only at the System level on appliances with the Organization component enabled. Options include: • **All Organizations**: The SQL Select statement is modified to iterate across all organizations, and the report contains information for all organizations. • **Aggregate results**: The SQL Select statement is modified to combine the records of all organizations, and the report contains summary information for all organizations. Standard reports of this type are categorized as Consolidated Reports.

4. Click **Save**.

The appliance checks the report syntax and displays any errors.

5. To run the new report, click a format in the *Generate Report* column.

Create dashboard report using SQL queries

You can create report widgets by directly entering SQL queries in the report form. This method is ideal for advanced users who prefer the flexibility of writing custom queries.

If you do not know the SQL queries to use, consider using the report wizard. See Create reports using the report wizard.

1. Go to the *Reports* list by doing one of the following:
   - **If your appliance has the Organization component enabled, and you want to access a System-level report:**

     Log in to the appliance System Administration Console, `https://`**appliance_hostname**`/system`, or select **System** from the drop-down list in the top-right corner of the page. Then click **Reporting**.
     System-level reports include consolidated reports that aggregate information from all organizations, as well as standard reports for various appliance components.
   - **If your appliance does not have the Organization component enabled, or if you want to access an organization-level report, log in to the appliance Administrator Console, `https://appliance_hostname/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information. Then click Reporting.**

     Organization-level reports include standard reports for various appliance components. If the Organization component is enabled on your appliance, these reports provide information specific to the selected organization.

   The *Reports* list appears.
2. Select **Choose Action** > **New > SQL** to display the *Report Detail* page.
3. Specify report settings:

Option	Description
Title	The display name of the report, which appears on the report list. Make the title as descriptive as possible, so you can distinguish the report from others in the list.
Description	A description of the report.
Category	The category of the report. If the category does not already exist, it is added to the drop-down list on the *Reports* page.
Break on Columns	A comma-separated list of SQL column names. The report generates break headers and subtotals for these columns.
Show Line Numbers	Display a column with line numbers on the report.
SQL	The query statement that generates the report data. For more information, go to the MySQL documentation at http://dev.mysql.com/doc/refman/5.0/en/. When writing a report or query against the Service Desk HD_Ticket table, be aware that the *User* custom field stores the user ID from the USER table in the HD_TICKET table, which is the table that holds the ticket record. If you want to display the username instead of the user ID in the report, you need to JOIN on the USER table. See Database table names.

Option	Description
Organization settings	These settings are available only at the **System level** on appliances with the Organization component enabled. Options include: • **All Organizations**: The SQL Select statement is modified to iterate across all organizations, and the report contains information for all organizations. • **Aggregate results**: The SQL Select statement is modified to combine the records of all organizations, and the report contains summary information for all organizations. Standard reports of this type are categorized as Consolidated Reports.
Would you like to use this report for Dashboard?	Select the option if you want to display the report on the dashboard. Once you select this option, the following fields are displayed.
Please select the chart type you want to use	Select the type of chart you want to display. Based on the chart type you select here, the relevant fields populate in the **Label and Axis Settings** section.
Label and Axis Settings	This section allows you to define which report columns are used for chart elements such as axes, legends, and data point values across various chart types. Configure these settings to control how your data is organized and displayed. For more information, refer the Configuring Chart Types for a Report topic.
Visualization Settings	This section allows you to configure visual details like legend placement, chart subtitles, fill settings, etc. Based on the chart type you select, the relevant fields populate in this section. For more information, refer the Configuring Chart Types for a Report topic.
Publish Settings	This section allows you to configure how your dashboard report is published, including visibility and access permissions. For more information, refer the Configuring Chart Types for a Report topic.

4. Click **Preview Chart** to view the chart before saving it. Or click **Save**.

   The appliance checks the report syntax and displays any error. New report widget is created and based on the Dashboard permission user can add the widget into respective dashboards. For information on how to add widgets to the dashboard, refer Adding a Widget.

Create reports from list pages

You can create reports while viewing list pages, such as the *Devices* page.

1. Go to a list page. For example, to go to the *Devices* page, do the following:
   a. If applicable, select an organization in the drop-down list in the top-right corner of the page.
   b. On the left navigation bar, click **Inventory**, then click **Devices**.
2. Select **Choose Action** > **Create Report** to display the *Report Detail* page.
3. Specify report settings:

Option	Description
Title	The display name of the report, which appears on the report list. Make the title as descriptive as possible, so you can distinguish the report from others in the list.
Description	A description of the report.

Option	Description
Category	The category of the report. If the category does not already exist, it is added to the drop-down list on the *Reports* page.
Break on Columns	A comma-separated list of SQL column names. The report generates break headers and subtotals for these columns.
Show Line Numbers	Display a column with line numbers on the report.
SQL	The query statement that generates the report data. For more information, go to the MySQL documentation at http://dev.mysql.com/doc/refman/5.0/en/. When writing a report or query against the Service Desk HD_Ticket table, be aware that the *User* custom field stores the user ID from the USER table in the HD_TICKET table, which is the table that holds the ticket record. If you want to display the username instead of the user ID in the report, you need to JOIN on the USER table.

4. Click **Save**.

The report appears on the *Reports* page.

Configuring Chart Types for a Report

Configuring the chart type is a key step in building a report widget. The KACE System Management Appliance offers a variety of chart types such as Bar, Line, Pie, Gauge and so on, each suited to different visualization needs. The application supports multiple chart types, and based on the selected chart type, the relevant fields in the **Label and Axis Settings** and **Visualization Settings** sections are dynamically populated. This topic helps you to understand how to configure chart types and customize their settings for optimal dashboard presentation.

NOTE: You can configure charts with or without SQL. In the sections that follow, examples demonstrate both methods- some charts are built using the Report Wizard, while others are configured using SQL. This is to help you understand the differences and choose the approach that best suits your needs.

The different chart types are as follows:

Chart Type	Description
Bar	Displays data as rectangular bars on an X-Y axis. Useful for comparing counts or values across categories such as department-wise device distribution.
Pie	Displays data as slices of a circle. Ideal for showing part-to-whole relationships, such as distribution of device types or ticket statuses.
Doughnut	Similar to Pie, but with a hollow center. Useful for comparing categorical data like operating systems or patch statuses.
Line	Shows trends over time using points connected by lines. Typically used for visualizing time-series data like patch deployment trends or ticket volume.
Combo	Combines Line and Bar charts in one. Helps compare multiple datasets, such as number of patches installed vs. number of failed installs.

Chart Type	Description
Polar Area	Displays data in circular segments with varying radii. Effective for equal-category comparisons, such as application usage across endpoint groups.
Radar	Uses a radial grid to plot multiple metrics. Best suited for visualizing performance across several criteria, such as device compliance score metrics.
World Geography	Plots data across global regions. Useful for global endpoint location visualization or country-wise license usage. **NOTE:** To display the country name on the World Geo Map chart correctly, ensure that the county name must match the supported country names. Refer to the List of Countries topic.
US Geography	Similar to World Geography but focused on U.S. states. Useful for region-specific deployment or compliance tracking within the U.S. **NOTE:** The chart requires the complete US state name. For example, the name should be Texas not TX.
Score	Displays a single metric or Key Performance Indicator (KPI), such as counts of updated devices. Offers a focused view on a single value.
Progress	Shows progress toward a target, such as number of encrypted devices vs. total devices. Typically used for goal tracking.
Table	Presents structured data in rows and columns. Ideal for viewing details like device inventory, patch statuses, or alert logs.
Gauge	Visualizes data on a scale with thresholds (for example, critical to optimal). Suitable for tracking health indicators or system readiness percentages.

Important Points:

- When you change the report topic in the report wizard, the fields are updated dynamically. Review all wizard steps to ensure your chart is correctly configured.
- SQL reports require explicit permission settings to ensure secure access. Report Wizard associate permission based on the selected report topic.
- Sample dashboard reports are available for your reference to help you understand how data is visualized and structured within the system. To view these samples, go to the Reports list and set the **View By** filter to **Samples - Dashboard Reports**. This will display a collection of example dashboards you can explore.

Chart Type Details

The section below lists each supported chart type, the relevant fields and their description.

Bar Chart

This chart displays data as rectangular bars on an X and Y axis. It is useful for comparing counts or values across categories such as Tickets by Category. You should select **Bar** from the **Please select the chart type you want to use** drop-down.

Configure the fields for the Bar chart in the following sections:

1. **Label and Axis Settings** Section

Section	Fields	Description
Label and Axis Settings		This section allows you to define which report columns are used for chart elements such as axes, legends, and data point values across various chart types. Configure these settings to control how your data is organized and displayed.
	X-Axis	This field specifies the categories or groups that represents the labels for the chart's X-Axis. Select the entity from the drop-down list.
	Y-Axis	This field is used to specify the data that will be represented as data points in the chart. Each data point corresponds to a specific value or measurement that will be plotted on the chart. Select the entity from the drop-down list.
	Clustered By	This field specifies the grouping or clustering criteria for the chart's data points. Set this to the field that defines how the data should be grouped or categorized for visualization. For Example: Refer the image for Bar chart. **X-Axis**: Ticket Category(Other, Hardware, Network, Software), **Y-Axis**: Ticket Count, **Cluster By**: Status
	Label	It defines the text shown on the chart to describe data point and helps to quickly understand what the value represents. This field populates when the **Clustered By** field is set to **None**.
	+ Add More Chart Data Point	Click to add more data points to the chart. This field populates when the **Cluster By** field is set to **None**.

2. **Visualization Settings** Section

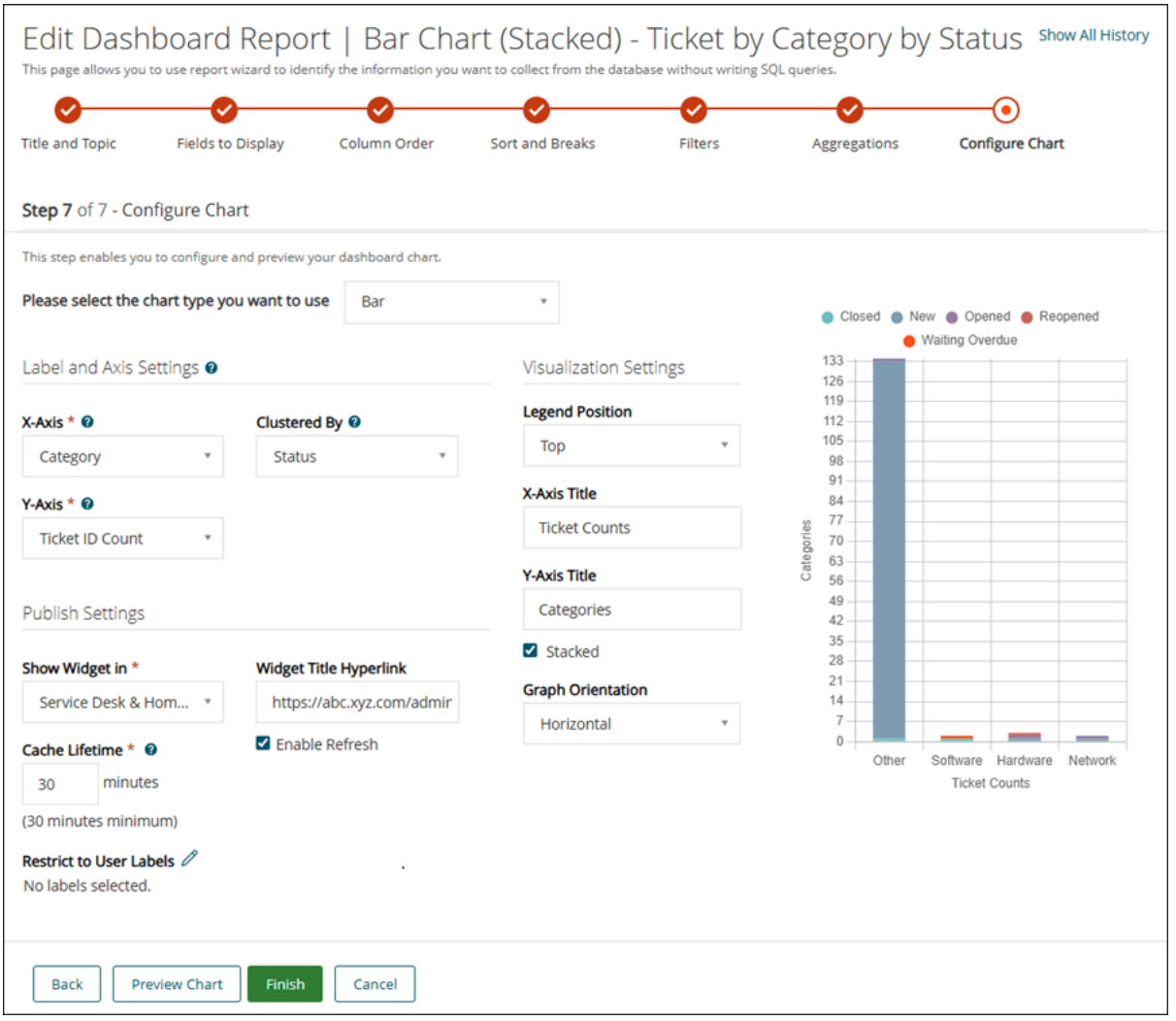
Section	Fields	Description
Visualization Settings		The settings define how the chart is visually presented. These settings help make the chart easier to read and interpret.
	Legend Position	Select the position from the drop-down. It specifies where the chart legend is displayed, such as top, bottom, left, or right of the chart. Select **None** to hide the legend.
	X-Axis Title	Enter the title to display on X-Axis.
	Y-Axis Title	Enter the title to display on Y-Axis.
	Stacked	Select this to displays multiple data series on top of each other in a single bar or column, showing the combined total for each category instead of separate segments.

Section	Fields	Description
	Graph Orientation	Select an option from the drop-down to set the direction of the chart's base axis- horizontal or vertical. This changes how the chart layout is displayed.

3. **Publish Settings** Section

Section	Fields	Description
Publish Settings		Defines where and how the widget is displayed on dashboards.
	Show Widget in	Select the dashboard category where you wish to make the widget available. All the widgets are available on the **Home** dashboard **NOTE:** This is not a permission control; it is simply linking widget to dashboard. This makes the widget available for selection in a particular dashboard.
	Widget Title Hyperlink	Add a clickable link to the widget title. When users click the title, it opens the specified URL in a new tab.
	Cache Lifetime	Set the duration the data will be cached for. The minimum duration is 30 minutes
	Restrict to User Labels	Select the Labels to show the widget only to the users assigned to the selected label.
	Enable Refresh	It allows the widget to automatically update its data at regular intervals or when manually refreshed. When enabled, a refresh icon appears on the widget, letting you to reload the latest data.
	Admin Console Permission Reference	This field is available only to a non-wizard type of report. It specifies the permission category required to view the widget. This field ensures that only users with the appropriate access rights (defined in their role permissions) can view or interact with the widget on the dashboard. **NOTE:** This field enforces permission control. If a user does not have access to the selected permission category (for example, Tickets, Devices), the widget will not appear in the **Add Widget** list. If the widget was previously added to a dashboard and the user's permission is later revoked, the widget will display an error message indicating that the user does not have permission to view it.
Preview Chart		Click it to view how the chart will appear using the selected configuration.
Finish		Click it after you finish the configuration.

The example below shows how to configure a dashboard report using a bar chart. In this chart, ticket counts are displayed by category, with bars stacked by status to show the breakdown within each category.



Pie Chart

Pie charts displays data as slices of a circle with each slice showing a proportion of the total. It is useful for showing part-to-whole relationships.

You should select **Pie** from the **Please select the chart type you want to use** drop-down. Configure the fields for the **Pie** chart in the following sections:

1. **Label and Axis Settings** Section

Section	Fields	Description
Label and Axis Settings		This section allows you to define which report columns are used for chart elements such as axes, legends, and data point values across various chart types. Configure these settings to control how your data is organized and displayed.
	Legend	Select a category or group from the drop-down list to represent each slice of the pie chart.
	Value	It specifies the data that determines the size of each slice in the pie chart. Each value represents a measurable quantity that is visually proportioned to reflect its share of the total.

Section	Fields	Description
		For example, refer the image for Pie Chart - it is a Pie chart for **Patches per Severity**. **Legend**: Severity (Critcal, Important, Low, Moderate, Recommended) Value: Severity Count
	Label	Type the text shown on the chart to describe data point and helps to quickly understand what the value represents.
	+ Add More Chart Data Point	Click to add more data points on X-Axis. This field populates when the **Cluster By** field is set to **None**.

2. **Visualization Settings** Section

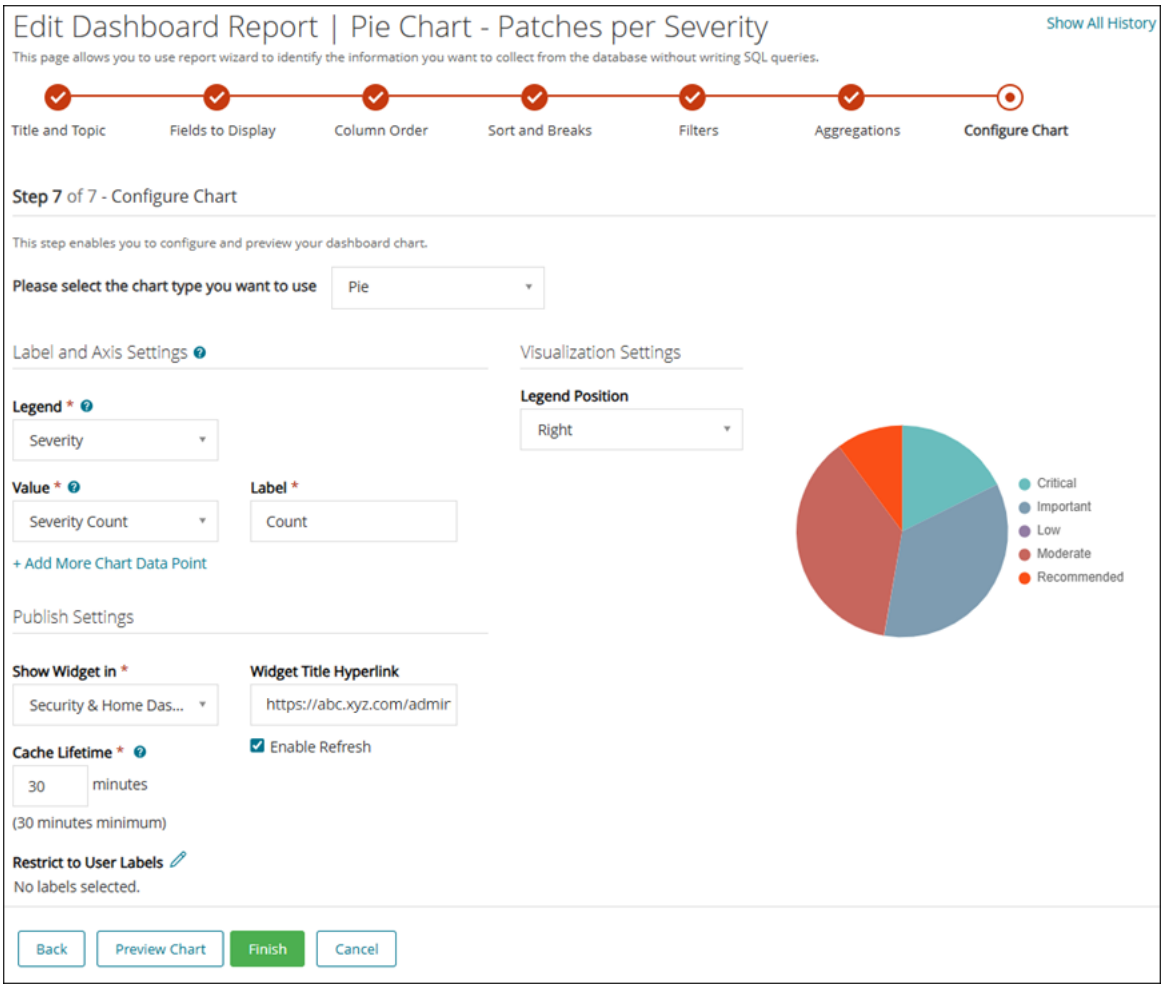
Section	Fields	Description
Visualization Settings		The settings define how the chart is visually presented. These settings help make the chart easier to read and interpret.
	Legend Position	Specifies where the chart legend is displayed, such as top, bottom, left, or right of the chart. Select None to hide the legend

3. **Publish Settings** Section

Section	Fields	Description
Publish Settings		Defines where and how the widget is displayed on dashboards.
	Show Widget in	Select the dashboard category where you wish to make the widget available. All the widgets are available on the **Home** dashboard **NOTE:** This is not a permission control; it is simply linking widget to dashboard. This makes the widget available for selection in a particular dashboard.
	Widget Title Hyperlink	Add a clickable link to the widget title. When users click the title, it opens the specified URL in a new tab.
	Cache Lifetime	Set the duration the data will be cached for. The minimum duration is 30 minutes
	Restrict to User Labels	Select the Labels to show the widget only to the users assigned to the selected label.
	Enable Refresh	It allows the widget to automatically update its data at regular intervals or when manually refreshed. When enabled, a refresh icon appears on the widget, letting you to reload the latest data.
	Admin Console Permission Reference	This field is available only to a non-wizard type of report. It specifies the permission category required to view the widget. This field ensures that only users with the appropriate access rights (defined in their role permissions) can view or interact with the widget on the dashboard.

Section	Fields	Description
		NOTE: This field enforces permission control. If a user does not have access to the selected permission category (for example, Tickets, Devices), the widget will not appear in the **Add Widget** list. If the widget was previously added to a dashboard and the user's permission is later revoked, the widget will display an error message indicating that the user does not have permission to view it.
Preview Chart		Click it to view how the chart will appear using the selected configuration.
Finish		Click it after you finish the configuration.

The example below shows how to configure a dashboard report using a pie chart. This chart illustrates the number of patches categorized by severity level.



Radar Chart

The chart uses a radial grid to plot multiple metrics. This chart is best suited for visualizing performance across several criteria, such as device compliance score metrics. The Radar chart works best if we are evaluating multiple data points (three or more) on a two-dimensional plane.

You should select **Radar** from the **Please select the chart type you want to use** drop-down. Configure the fields for the **Radar** chart in the following sections:

1. **Label and Axis Settings** Section

Section	Fields	Description
Label and Axis Settings		This section allows you to define which report columns are used for chart elements such as axes, legends, and data point values across various chart types. Configure these settings to control how your data is organized and displayed.
	Axis	Select a category or group from the drop-down list to represent segment of the chart. This field specifies the categories that will be displayed along the radial axes of the chart.
	Value	It specifies the data that will be represented as data points in the chart. Each data point corresponds to a specific value or measurement that will be plotted on the chart.
	Clustered By	This field specifies the grouping or clustering criteria for the chart's data points. Set this to the field that defines how the data should be grouped or categorized for visualization. For Example: Refer the image for Radar chart. **Axis**: Category, **Value**: Ticket ID Count, **Cluster By**: Status If you select None from the drop-down list the **Label** field populates.
	Label	Type the text shown on the chart to describe data point and helps to quickly understand what the value represents.
	+ Add More Chart Data Point	Click to add more data points. This field populates when the **Cluster By** field is set to **None**.

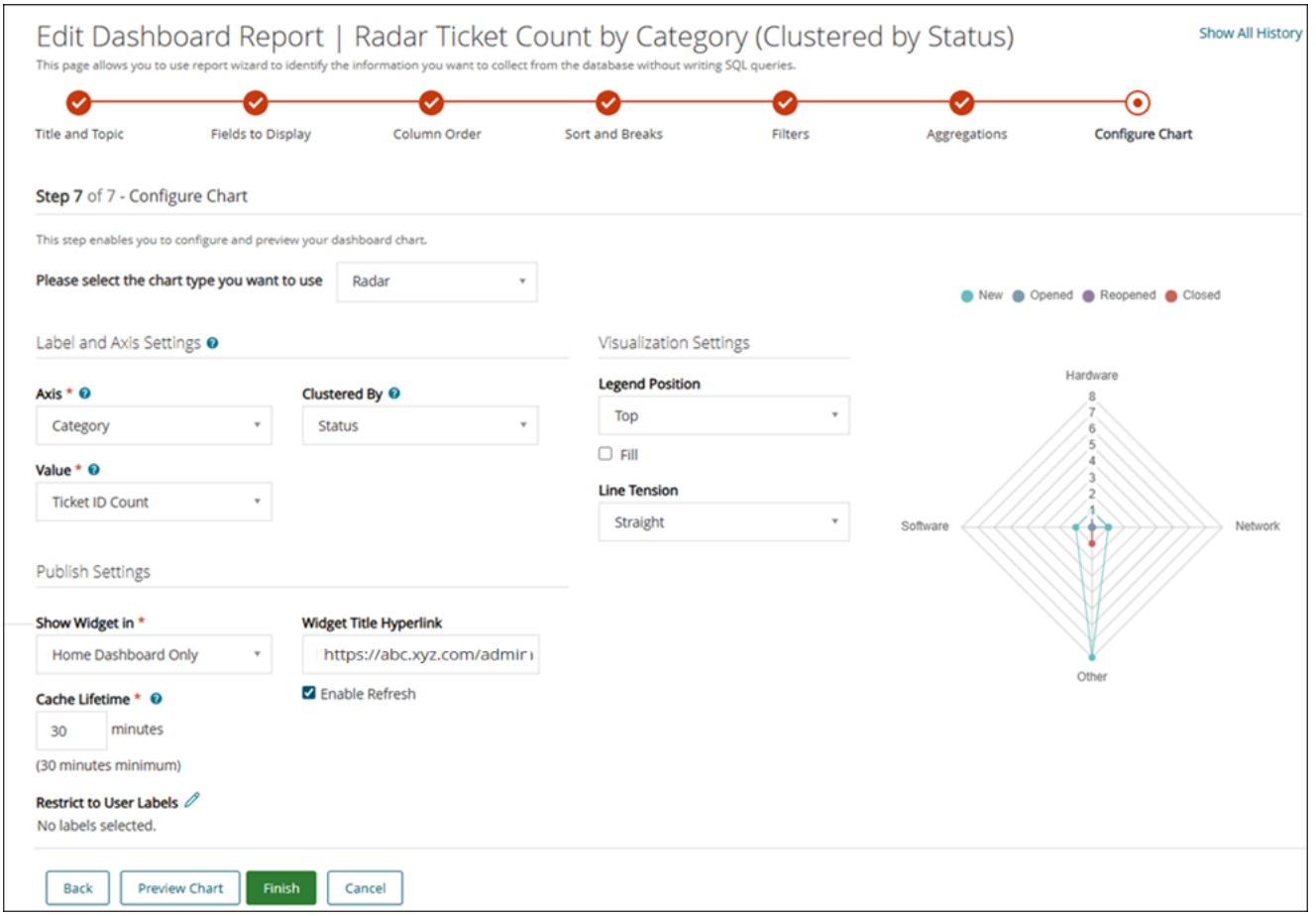
2. Visualization Settings Section

Section	Fields	Description
Visualization Settings		The settings define how the chart is visually presented. These settings help make the chart easier to read and interpret.
	Legend Position	Select an option to **specify where the chart legend should displayed, such as top, bottom, left, or right of the chart.** Select **None** to hide the legend.
	Fill	Select the field to fill the area under the line or within the radar shape with color.
	Line Tension	Select the option from the drop-down to define the curvature of the lines connecting data points in a radar chart.

3. **Publish Settings** Section

Section	Fields	Description
Publish Settings		Defines where and how the widget is displayed on dashboards.
	Show Widget in	Select the dashboard category where you wish to make the widget available. All the widgets are available on the **Home** dashboard **NOTE:** This is not a permission control; it is simply linking widget to dashboard. This makes the widget available for selection in a particular dashboard.
	Widget Title Hyperlink	Add a clickable link to the widget title. When users click the title, it opens the specified URL in a new tab.
	Cache Lifetime	Set the duration the data will be cached for. The minimum duration is 30 minutes
	Restrict to User Labels	Select the Labels to show the widget only to the users assigned to the selected label.
	Enable Refresh	It allows the widget to automatically update its data at regular intervals or when manually refreshed. When enabled, a refresh icon appears on the widget, letting you to reload the latest data.
	Admin Console Permission Reference	This field is available only to a non-wizard type of report. It specifies the permission category required to view the widget. This field ensures that only users with the appropriate access rights (defined in their role permissions) can view or interact with the widget on the dashboard. **NOTE:** This field enforces permission control. If a user does not have access to the selected permission category (for example, Tickets, Devices), the widget will not appear in the **Add Widget** list. If the widget was previously added to a dashboard and the user's permission is later revoked, the widget will display an error message indicating that the user does not have permission to view it.
Preview Chart		Click it to view how the chart will appear using the selected configuration.
Finish		Click it after you finish the configuration.

The example below shows how to configure a dashboard report using a Radar chart. This chart illustrates the Ticket Count by Category.



Polar Area Chart

This chart displays data in circular segments with varying radii. This chart is effective for equal-category comparisons, such as application usage across endpoint groups.

You should select **Polar Area** from the **Please select the chart type you want to use** drop-down. Configure the fields for the **Polar Area** chart in the following sections:

1. **Label and Axis Settings** Section

Section	Fields	Description
Label and Axis Settings		This section allows you to define which report columns are used for chart elements such as axes, legends, and data point values across various chart types. Configure these settings to control how your data is organized and displayed.
	Legend	Select a category or group from the drop-down list to represent segment of the chart.
	Value	It specifies the data that will be represented as data points in the chart. Each data point corresponds to a specific value or measurement that will be plotted on the chart.
	Clustered By	This field specifies the grouping or clustering criteria for the chart's data points. Set this to the field that defines how the data should be grouped or categorized for visualization.

Section	Fields	Description
		If you select **None** from the drop-down list the **Label** field populates.
	Label	Type the text shown on the chart to describe data point and helps to quickly understand what the value represents.
	+ Add More Chart Data Point	Click to add more data points. This field populates when the **Cluster By** field is set to **None**.

2. **Visualization Settings** Section

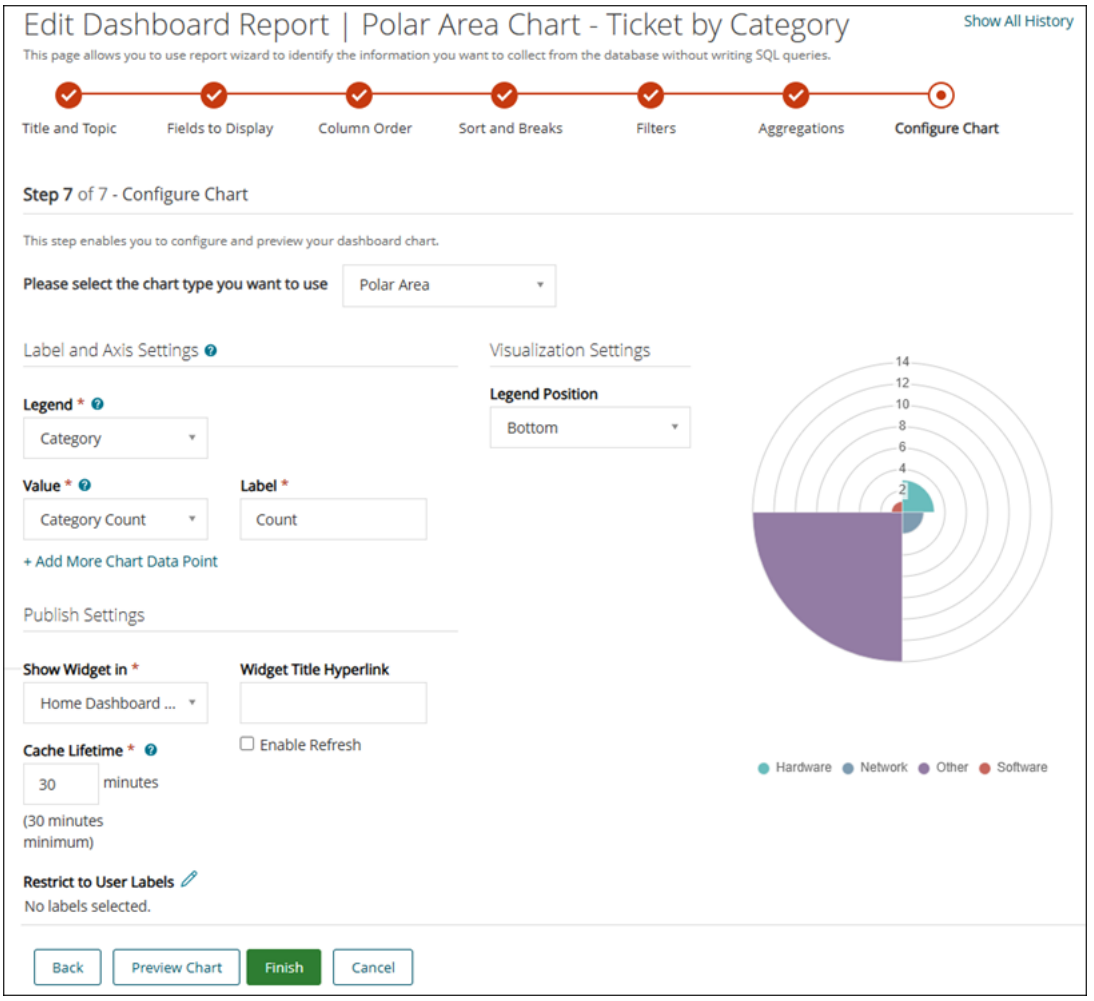
Section	Fields	Description
Visualization Settings		The settings define how the chart is visually presented. These settings help make the chart easier to read and interpret.
	Legend Position	Select an option to specify where the chart legend should displayed, such as top, bottom, left, or right of the chart. Select **None** to hide the legend.

3. **Publish Settings** Section

Section	Fields	Description
Publish Settings		Defines where and how the widget is displayed on dashboards.
	Show Widget in	Select the dashboard category where you wish to make the widget available. All the widgets are available on the **Home** dashboard **NOTE:** This is not a permission control; it is simply linking widget to dashboard. This makes the widget available for selection in a particular dashboard.
	Widget Title Hyperlink	Add a clickable link to the widget title. When users click the title, it opens the specified URL in a new tab.
	Cache Lifetime	Set the duration the data will be cached for. The minimum duration is 30 minutes
	Restrict to User Labels	Select the Labels to show the widget only to the users assigned to the selected label.
	Enable Refresh	It allows the widget to automatically update its data at regular intervals or when manually refreshed. When enabled, a refresh icon appears on the widget, letting you to reload the latest data.
	Admin Console Permission Reference	This field is available only to a non-wizard type of report. It specifies the permission category required to view the widget. This field ensures that only users with the appropriate access rights (defined in their role permissions) can view or interact with the widget on the dashboard.

Section	Fields	Description
		NOTE: This field enforces permission control. If a user does not have access to the selected permission category (for example, Tickets, Devices), the widget will not appear in the **Add Widget** list. If the widget was previously added to a dashboard and the user's permission is later revoked, the widget will display an error message indicating that the user does not have permission to view it.
Preview Chart		Click it to view how the chart will appear using the selected configuration.
Finish		Click it after you finish the configuration.

The example below shows how to configure a dashboard report using a Polar Area chart. This chart illustrates the Ticket Count by Category.



World Geography Chart

This chart type plots data across global regions. This chart is useful for global endpoint location visualization or country-wise license usage.

NOTE: To display the country name on the World Geography chart correctly, ensure that the county name must match the supported country names. For list of countries, see the List of Countries topic.

You should select **World Geography** from the **Please select the chart type you want to use** drop-down. Configure the fields for the **World Geography** chart in the following sections:

1. **Label and Axis Settings** Section

Section	Fields	Description
Label and Axis Settings		This section allows you to define which report columns are used for chart elements such as axes, legends, and data point values across various chart types. Configure these settings to control how your data is organized and displayed.
	Country	This field specifies the countries that will be represented on the chart. Set this to the field containing country names to map the data accurately.
	Value	It specifies the data that will be represented as data points in the chart. Each data point corresponds to a specific value or measurement that will be plotted on the chart.

2. **Visualization Settings** Section

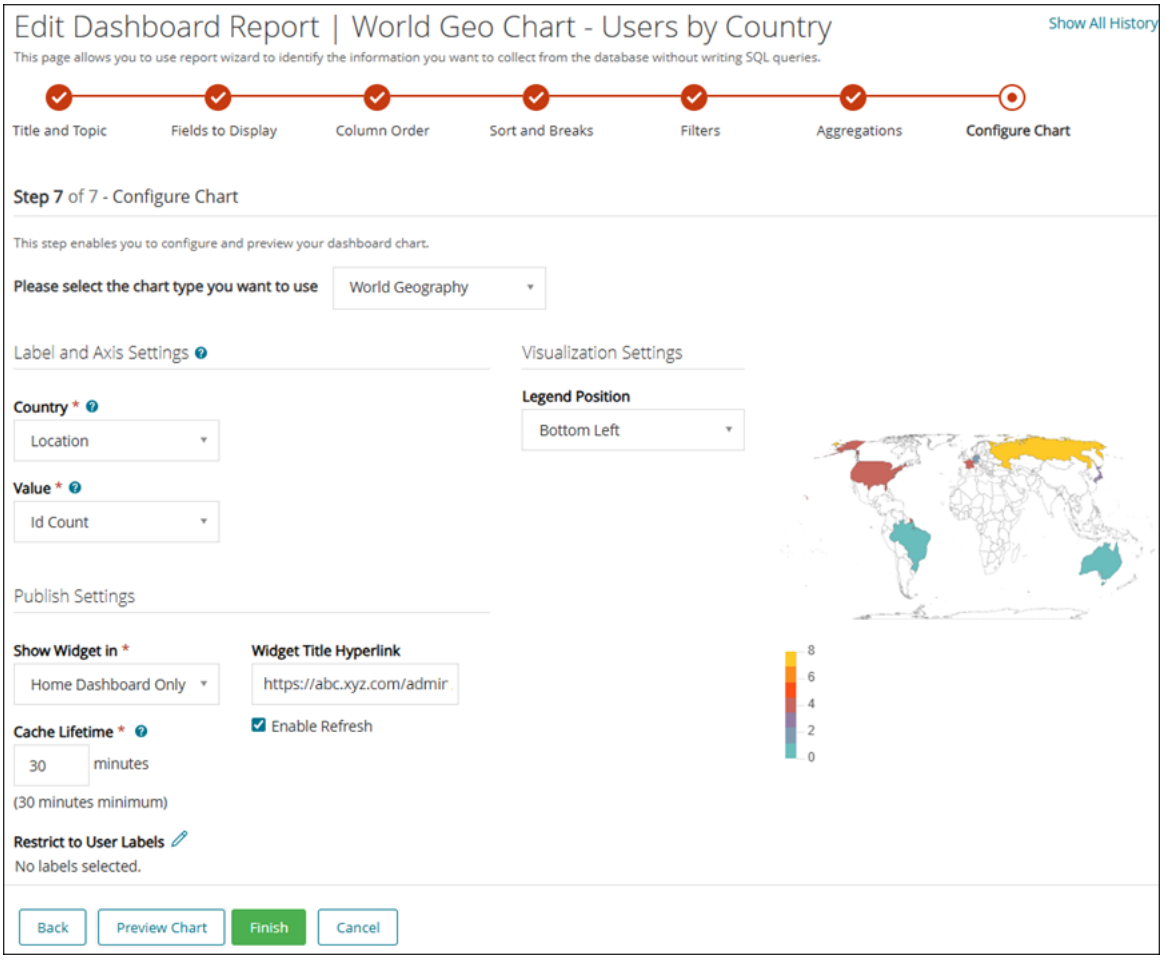
Section	Fields	Description
Visualization Settings		The settings define how the chart is visually presented. These settings help make the chart easier to read and interpret.
	Legend Position	Select an option to specify where the chart legend should displayed, such as top, bottom, left, or right of the chart.

3. **Publish Settings** Section

Section	Fields	Description
Publish Settings		Defines where and how the widget is displayed on dashboards.
	Show Widget in	Select the dashboard category where you wish to make the widget available. All the widgets are available on the **Home** dashboard **NOTE:** This is not a permission control; it is simply linking widget to dashboard. This makes the widget available for selection in a particular dashboard.
	Widget Title Hyperlink	Add a clickable link to the widget title. When users click the title, it opens the specified URL in a new tab.
	Cache Lifetime	Set the duration the data will be cached for. The minimum duration is 30 minutes
	Restrict to User Labels	Select the Labels to show the widget only to the users assigned to the selected label.

Section	Fields	Description
	Enable Refresh	It allows the widget to automatically update its data at regular intervals or when manually refreshed. When enabled, a refresh icon appears on the widget, letting you to reload the latest data.
	Admin Console Permission Reference	This field is available only to a non-wizard type of report. It specifies the permission category required to view the widget. This field ensures that only users with the appropriate access rights (defined in their role permissions) can view or interact with the widget on the dashboard. **NOTE:** This field enforces permission control. If a user does not have access to the selected permission category (for example, Tickets, Devices), the widget will not appear in the **Add Widget** list. If the widget was previously added to a dashboard and the user's permission is later revoked, the widget will display an error message indicating that the user does not have permission to view it.
Preview Chart		Click it to view how the chart will appear using the selected configuration.
Finish		Click it after you finish the configuration.

The following is an image for World Geography chart for Users by Country.



US Geography Chart

Similar to World Geography but focused on U.S. states. Useful for region-specific deployment or compliance tracking within the U.S.

NOTE: The chart requires the complete US state name. For example, the name should be Texas not TX.

You should select **US Geography** from the **Please select the chart type you want to use** drop-down. Configure the fields for the **US Geography** chart in the following sections:

1. **Label and Axis Settings** Section

Section	Fields	Description
Label and Axis Settings		This section allows you to define which report columns are used for chart elements such as axes, legends, and data point values across various chart types. Configure these settings to control how your data is organized and displayed.
	State	This field specifies the US states that will be represented on the chart. Set this to the field containing US state names to map the data accurately.

Section	Fields	Description
	Value	It specifies the data that will be represented as data points in the chart. Each data point corresponds to a specific value or measurement that will be plotted on the chart.

2. **Visualization Settings** Section

Section	Fields	Description
Visualization Settings		The settings define how the chart is visually presented. These settings help make the chart easier to read and interpret.
	Legend Position	Select the option to specify where the chart legend should be displayed, such as bottom right, top right, bottom left, or top left of the chart.

3. **Publish Settings** Section

Section	Fields	Description
Publish Settings		Defines where and how the widget is displayed on dashboards.
	Show Widget in	Select the dashboard category where you wish to make the widget available. All the widgets are available on the **Home** dashboard **NOTE:** This is not a permission control; it is simply linking widget to dashboard. This makes the widget available for selection in a particular dashboard.
	Widget Title Hyperlink	Add a clickable link to the widget title. When users click the title, it opens the specified URL in a new tab.
	Cache Lifetime	Set the duration the data will be cached for. The minimum duration is 30 minutes
	Restrict to User Labels	Select the Labels to show the widget only to the users assigned to the selected label.
	Enable Refresh	It allows the widget to automatically update its data at regular intervals or when manually refreshed. When enabled, a refresh icon appears on the widget, letting you to reload the latest data.
	Admin Console Permission Reference	This field is available only to a non-wizard type of report. It specifies the permission category required to view the widget. This field ensures that only users with the appropriate access rights (defined in their role permissions) can view or interact with the widget on the dashboard. **NOTE:** This field enforces permission control. If a user does not have access to the selected permission category (for example, Tickets, Devices), the widget will not appear in the **Add Widget** list. If the widget was previously added to a dashboard and the user's permission is later revoked, the widget will display an error message indicating that the user does not have permission to view it.

Section	Fields	Description
Preview Chart		Click it to view how the chart will appear using the selected configuration.
Finish		Click it after you finish the configuration.

The following is an image for US Geography chart for US users per State.

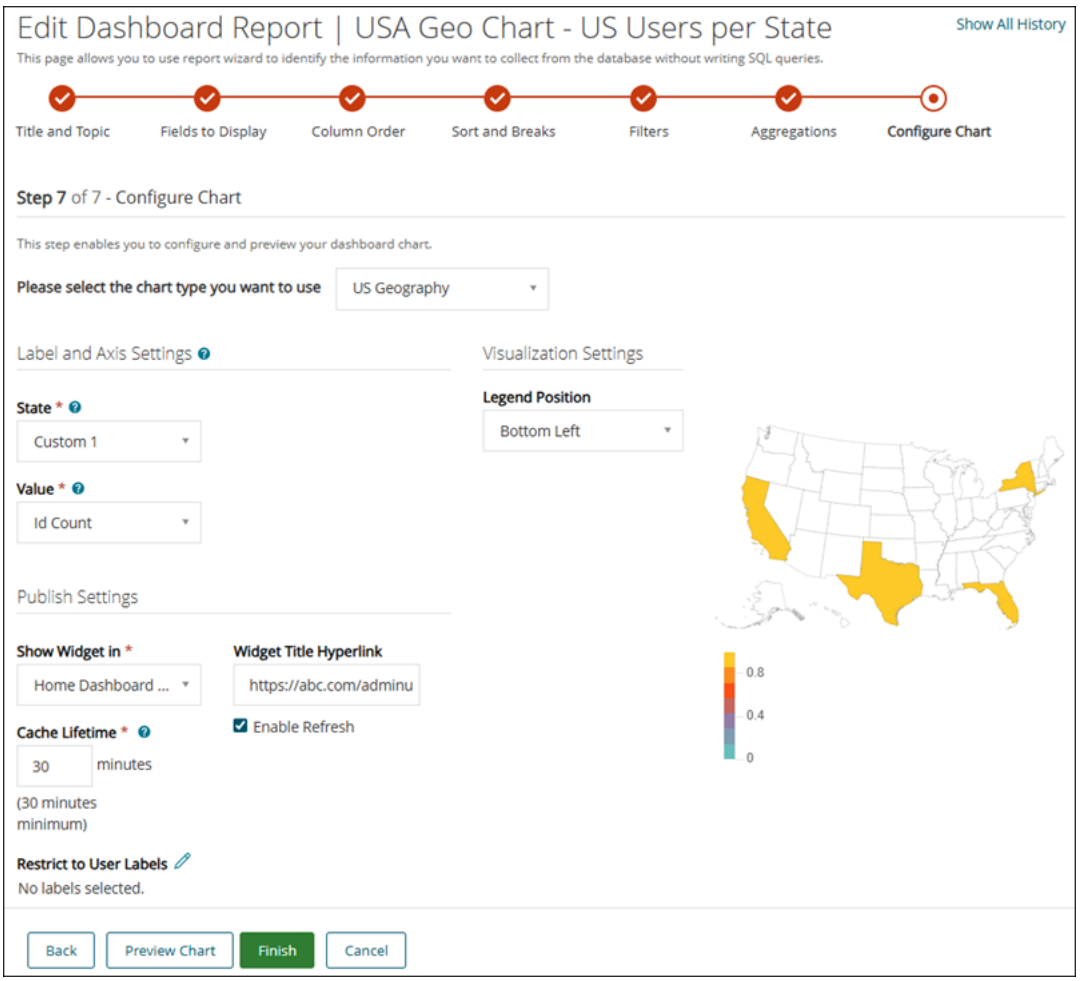


Table Chart

This chart presents structured data in rows and columns. Ideal for viewing details like device inventory, patch statuses, or alert logs.

You should select **Table** from the **Please select the chart type you want to use** drop-down. Configure the fields for the **Table** chart in the following sections:

1. **Label and Axis Settings** Section

Section	Fields	Description
Label and Axis Settings		This section allows you to define which report columns are used for chart elements such as axes, legends, and data point values across various chart types. Configure these settings to control how your data is organized and displayed.

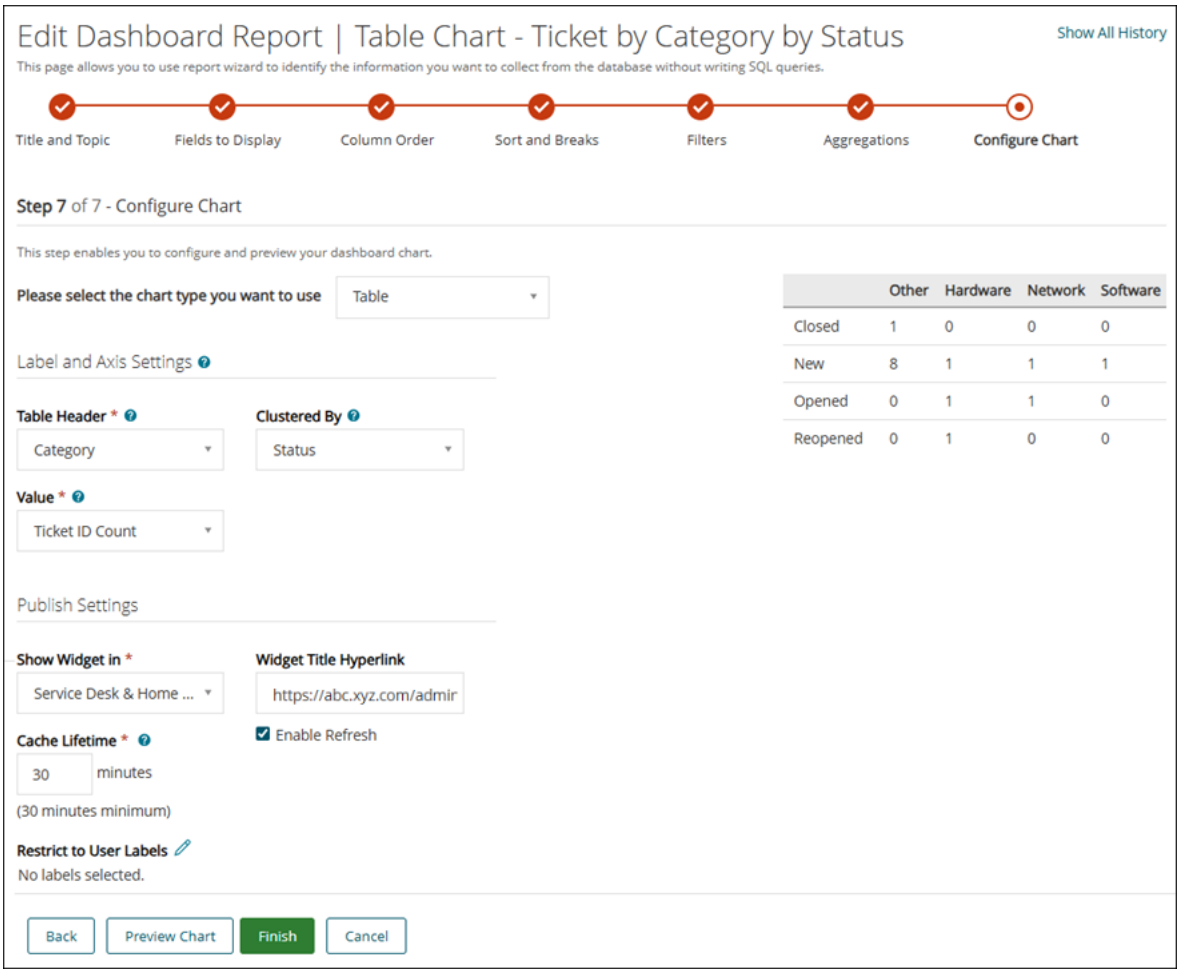
Section	Fields	Description
	Table Header	This field specifies the column headers of the table. Select the column name from the drop-down list.
	Value	It specifies the data that will be represented as data points in the chart. Each data point corresponds to a specific value or measurement that will be plotted on the chart.
	Clustered By	This field specifies the grouping or clustering criteria for the chart's data points. Set this to the field that defines how the data should be grouped or categorized for visualization. If you select **None** from the drop-down list the **Label** field populates.
	+ Add More Chart Data Point	Click to add more data points. This field populates when the **Cluster By** field is set to **None**.

2. **Publish Settings** Section

Section	Fields	Description
Publish Settings		Defines where and how the widget is displayed on dashboards.
	Show Widget in	Select the dashboard category where you wish to make the widget available. All the widgets are available on the **Home** dashboard **NOTE:** This is not a permission control; it is simply linking widget to dashboard. This makes the widget available for selection in a particular dashboard.
	Widget Title Hyperlink	Add a clickable link to the widget title. When users click the title, it opens the specified URL in a new tab.
	Cache Lifetime	Set the duration the data will be cached for. The minimum duration is 30 minutes
	Restrict to User Labels	Select the Labels to show the widget only to the users assigned to the selected label.
	Enable Refresh	It allows the widget to automatically update its data at regular intervals or when manually refreshed. When enabled, a refresh icon appears on the widget, letting you to reload the latest data.
	Admin Console Permission Reference	This field is available only to a non-wizard type of report. It specifies the permission category required to view the widget. This field ensures that only users with the appropriate access rights (defined in their role permissions) can view or interact with the widget on the dashboard.

Section	Fields	Description
		NOTE: This field enforces permission control. If a user does not have access to the selected permission category (for example, Tickets, Devices), the widget will not appear in the **Add Widget** list. If the widget was previously added to a dashboard and the user's permission is later revoked, the widget will display an error message indicating that the user does not have permission to view it.
Preview Chart		Click it to view how the chart will appear using the selected configuration.
Finish		Click it after you finish the configuration.

The example below shows how to configure a dashboard report using a table chart. In this chart, ticket counts are organized by category across the columns (header) and by status down the rows.



Progress Chart

This chart shows progress toward a target, such as number of encrypted devices vs total devices. This is typically used for goal tracking.

Below is a sample for creating a dashboard report using SQL queries.

Once you add the details for creating report with SQL (for more information, refer Create dashboard report using SQL queries), you should select **Would you like to use this report for Dashboard**. Configure the fields for the **Progress** chart in the following sections:

1. Select appropriate option.

Fields	Description
Would you like to use this report for Dashboard?	Select the option if you want to display the report on the dashboard. Once you select this option, the following fields are displayed.
Please select the chart type you want to use	You should select **Progress** from the drop-down.

2. **Label and Axis Settings** Section

Section	Fields	Description
Label and Axis Settings		This section allows you to define which report columns are used for chart elements such as axes, legends, and data point values across various chart types. Configure these settings to control how your data is organized and displayed.
	Value	**It defines the current progress or achieved amount to be visualized on the chart.** This is the actual value being measured (for example, number of resolved tickets, completed tasks, or percentage of target met). It determines how much of the progress bar is filled.
	Max Value	It specifies the target or maximum possible value for the progress indicator. This value sets the full scale of the progress chart. The percentage of progress is calculated as: (Value ÷ Max Value) × 100

3. **Visualization Settings** Section

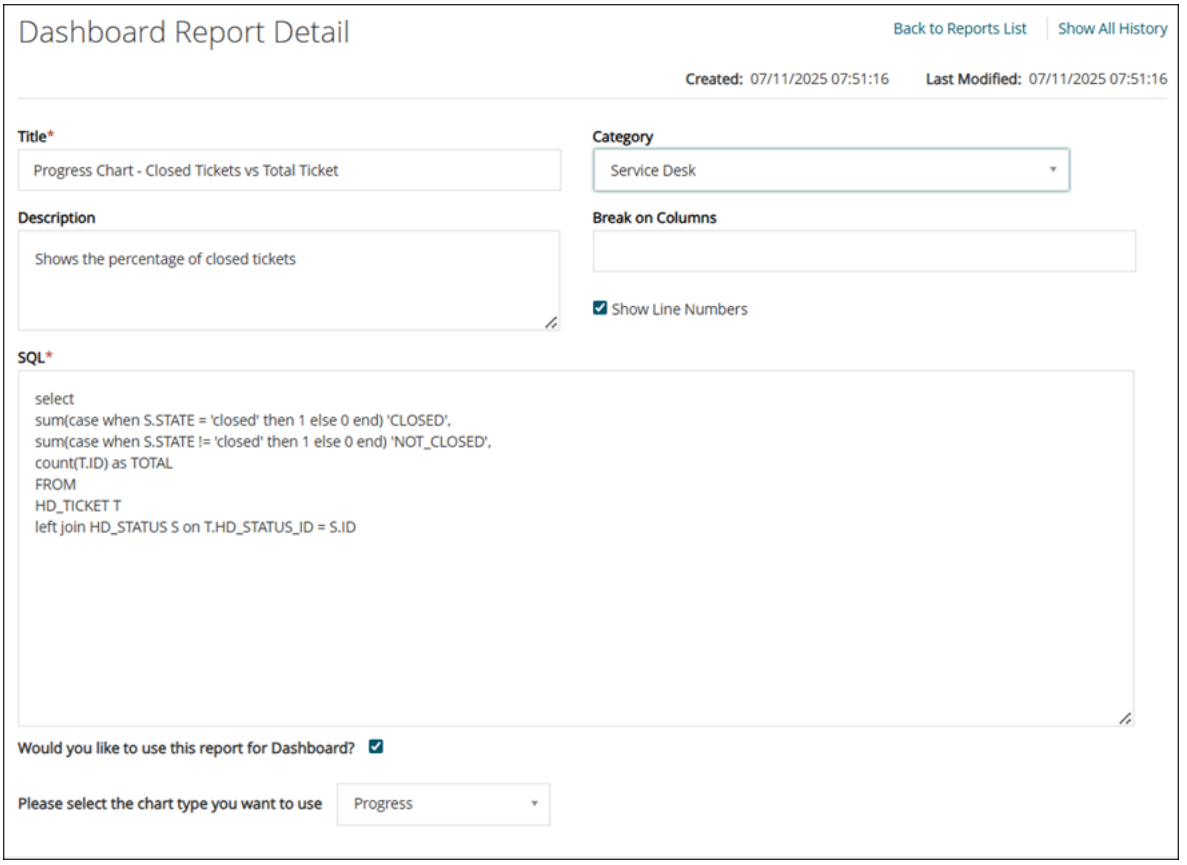
Section	Fields	Description
Visualization Settings		The settings define how the chart is visually presented. These settings help make the chart easier to read and interpret.
	Subtitle	Add the text that appears below the chart.

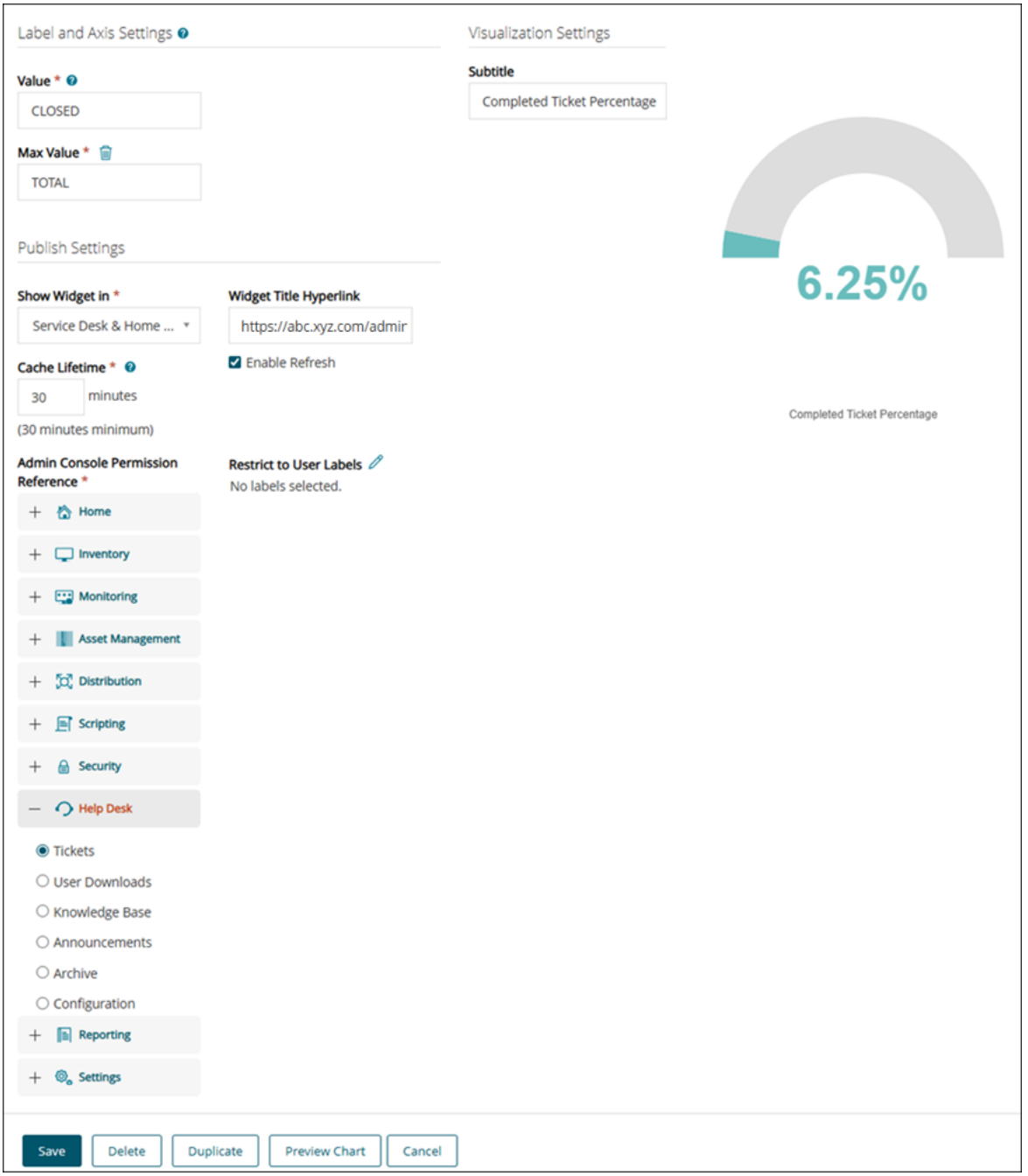
4. **Publish Settings** Section

Section	Fields	Description
Publish Settings		Defines where and how the widget is displayed on dashboards.
	Show Widget in	Select the dashboard category where you wish to make the widget available. All the widgets are available on the **Home** dashboard **NOTE:** This is not a permission control; it is simply linking widget to dashboard. This makes the widget available for selection in a particular dashboard.

Section	Fields	Description
	Widget Title Hyperlink	Add a clickable link to the widget title. When users click the title, it opens the specified URL in a new tab.
	Cache Lifetime	Set the duration the data will be cached for. The minimum duration is 30 minutes
	Restrict to User Labels	Select the Labels to show the widget only to the users assigned to the selected label.
	Enable Refresh	It allows the widget to automatically update its data at regular intervals or when manually refreshed. When enabled, a refresh icon appears on the widget, letting you to reload the latest data.
	Admin Console Permission Reference	This field is available only to a non-wizard type of report. It specifies the permission category required to view the widget. This field ensures that only users with the appropriate access rights (defined in their role permissions) can view or interact with the widget on the dashboard. **NOTE:** This field enforces permission control. If a user does not have access to the selected permission category (for example, Tickets, Devices), the widget will not appear in the **Add Widget** list. If the widget was previously added to a dashboard and the user's permission is later revoked, the widget will display an error message indicating that the user does not have permission to view it.
Preview Chart		Click it to view how the chart will appear using the selected configuration.
Finish		Click it after you finish the configuration.

The example below demonstrates how to configure a dashboard report using a progress chart. This chart displays the percentage of completed work by showing the number of closed tickets relative to the total number of tickets.


Dashboard Report Detail
Back to Reports List
Show All History
Created: 07/11/2025 07:51:16
Last Modified: 07/11/2025 07:51:16
Title*
Progress Chart - Closed Tickets vs Total Ticket
Category
Service Desk
Description
Shows the percentage of closed tickets
Break on Columns
Show Line Numbers
SQL*
select
sum(case when S.STATE = 'closed' then 1 else 0 end) 'CLOSED',
sum(case when S.STATE != 'closed' then 1 else 0 end) 'NOT_CLOSED',
count(T.ID) as TOTAL
FROM
HD_TICKET T
left join HD_STATUS S on T.HD_STATUS_ID = S.ID
Would you like to use this report for Dashboard?
Please select the chart type you want to use
Progress



Gauge Chart

This chart visualizes data on a scale with thresholds (for example, critical to optimal). This is suitable for tracking health indicators or system readiness percentages.

Once you add the details for creating report with SQL (for more information, refer Create dashboard report using SQL queries), you should select **Would you like to use this report for Dashboard**. Configure the fields for the **Gauge** chart for the following sections:

1. Select appropriate option.

Fields	Description
Would you like to use this report for Dashboard?	Select the option if you want to display the report on the dashboard. Once you select this option, the following fields are displayed.
Please select the chart type you want to use	You should select **Gauge** from the drop-down.

2. **Label and Axis Settings** Section

Section	Fields	Description
Label and Axis Settings		This section allows you to define which report columns are used for chart elements such as axes, legends, and data point values across various chart types. Configure these settings to control how your data is organized and displayed.
	Value	It represents the current metric or data point being measured on the gauge. This is the actual value displayed by the gauge needle. It reflects progress, usage, or performance (for example, CPU utilization, sales achieved, or tickets resolved).
	Max Value	It defines **the upper limit or full scale of the gauge. This sets the maximum range against which the current value is evaluated**

3. **Visualization Settings** Section

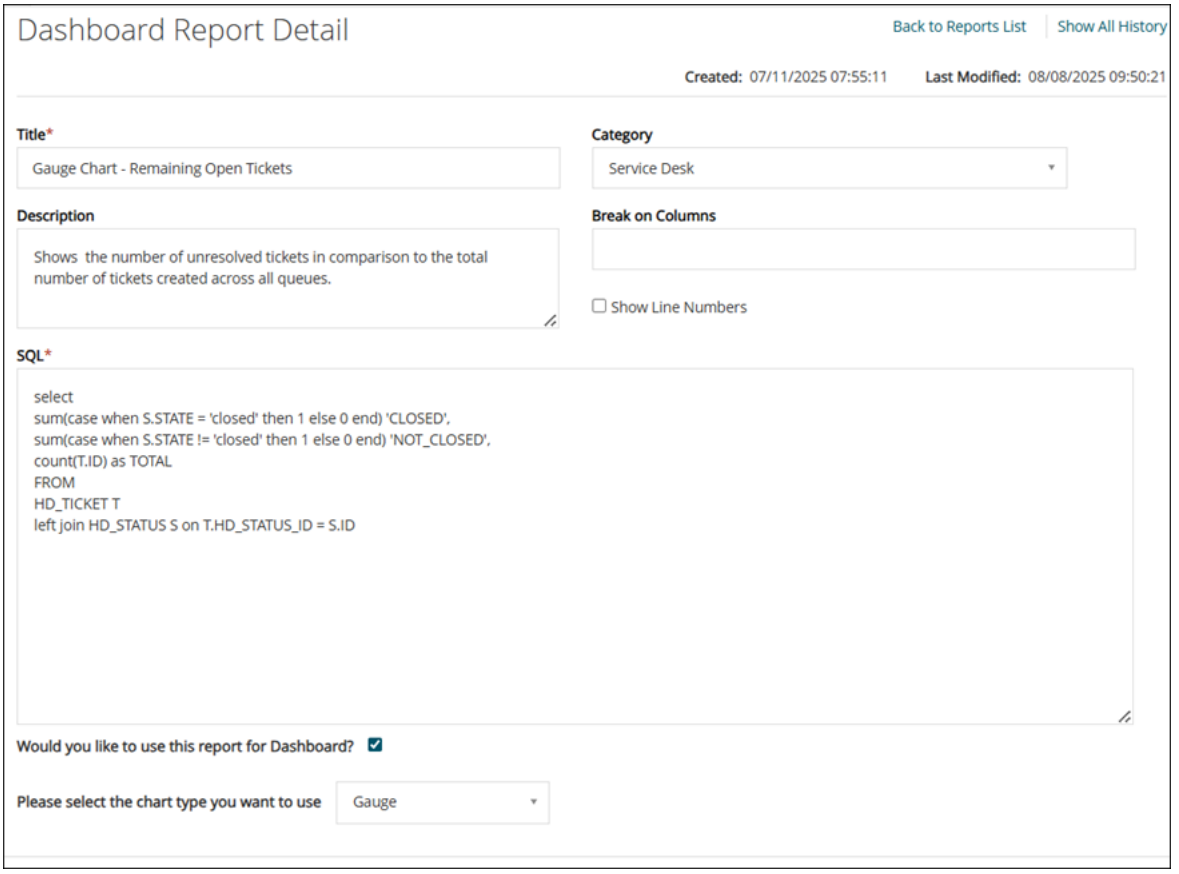
Section	Fields	Description
Visualization Settings		The settings define how the chart is visually presented. These settings help make the chart easier to read and interpret.
	Subtitle	Add the text that appears below the chart.
	Use Monochromatic Effect	Select this to apply a single base color across the gauge, using varying shades to represent intensity.
	Color Sorting	It determines how the shades are applied when using the monochromatic effect - Darkest to Lightest or Lightest to Darkest.
	Show Gauge Numbers	Select this to display the numerical value and range directly on the gauge for quick reference.

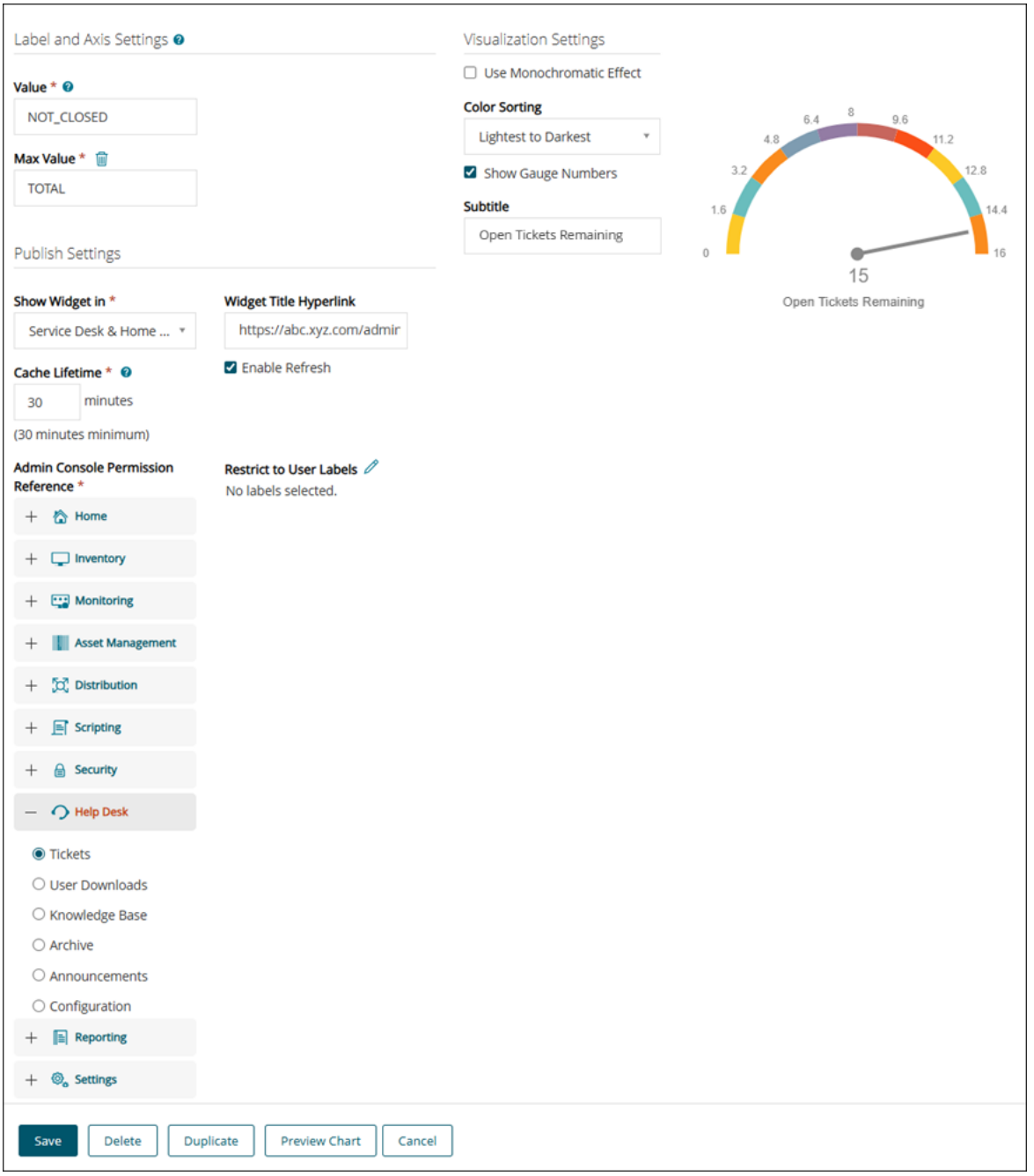
4. **Publish Settings** Section

Section	Fields	Description
Publish Settings		Defines where and how the widget is displayed on dashboards.
	Show Widget in	Select the dashboard category where you wish to make the widget available. All the widgets are available on the **Home** dashboard

Section	Fields	Description
		NOTE: This is not a permission control; it is simply linking widget to dashboard. This makes the widget available for selection in a particular dashboard.
	Widget Title Hyperlink	Add a clickable link to the widget title. When users click the title, it opens the specified URL in a new tab.
	Cache Lifetime	Set the duration the data will be cached for. The minimum duration is 30 minutes
	Restrict to User Labels	Select the Labels to show the widget only to the users assigned to the selected label.
	Enable Refresh	It allows the widget to automatically update its data at regular intervals or when manually refreshed. When enabled, a refresh icon appears on the widget, letting you to reload the latest data.
	Admin Console Permission Reference	This field is available only to a non-wizard type of report. It specifies the permission category required to view the widget. This field ensures that only users with the appropriate access rights (defined in their role permissions) can view or interact with the widget on the dashboard. **NOTE:** This field enforces permission control. If a user does not have access to the selected permission category (for example, Tickets, Devices), the widget will not appear in the **Add Widget** list. If the widget was previously added to a dashboard and the user's permission is later revoked, the widget will display an error message indicating that the user does not have permission to view it.
Preview Chart		Click it to view how the chart will appear using the selected configuration.
Finish		Click it after you finish the configuration.

The example below demonstrates how to configure a dashboard report using a gauge chart. This chart highlights the amount of incomplete work by showing the number of open tickets relative to the total number of tickets.


Dashboard Report Detail
Back to Reports List
Show All History
Created: 07/11/2025 07:55:11
Last Modified: 08/08/2025 09:50:21
Title*
Gauge Chart - Remaining Open Tickets
Category
Service Desk
Description
Shows the number of unresolved tickets in comparison to the total number of tickets created across all queues.
Break on Columns
Show Line Numbers
SQL*
select
sum(case when S.STATE = 'closed' then 1 else 0 end) 'CLOSED',
sum(case when S.STATE != 'closed' then 1 else 0 end) 'NOT_CLOSED',
count(T.ID) as TOTAL
FROM
HD_TICKET T
left join HD_STATUS S on T.HD_STATUS_ID = S.ID
Would you like to use this report for Dashboard?
Please select the chart type you want to use
Gauge



Combo Chart

The Combo Chart is a versatile visualization type that allows you to display multiple data series using a mix of bar and line formats within a single chart. This chart type is especially useful when you want to compare different metrics side by side—such as volume versus trend—while maintaining clarity and context.

Each data series in a Combo chart can be individually configured to appear as either a bar or a line. You can also define multiple Y-axes, apply stacking for bar segments, and customize line behavior using fill and tension settings. These features make the Combo Chart ideal for presenting layered insights in a compact and interactive format.

Once you add the details for creating report with SQL (for more information, refer Create dashboard report using SQL queries), you should select **Would you like to use this report for Dashboard**. Configure the following fields for the Combo chart:

1. Select appropriate option.

Fields	Description
Would you like to use this report for Dashboard?	Select the option if you want to display the report on the dashboard. Once you select this option, the following fields are displayed.
Please select the chart type you want to use	You should select **Combo** from the drop-down.

2. **Label and Axis Settings** Section

Section	Fields	Description
Label and Axis Settings		This section allows you to define which report columns are used for chart elements such as axes, legends, and data point values across various chart types. Configure these settings to control how your data is organized and displayed.
	X-Axis	This field specifies the categories or groups that represents the labels for the chart's X-Axis. Select the entity from the drop-down list.
	Clustered By	This field specifies the grouping or clustering criteria for the chart's data points. Set this to the field that defines how the data should be grouped or categorized for visualization.
	Y-Axis 1	This field is used to specify the data that will be represented as data points in the chart. Each data point corresponds to a specific value or measurement that will be plotted on the chart.
	Label	It defines the text shown on the chart to describe data point and helps to quickly understand what the value represents. This field populates when the **Cluster By** field is set to **None**.
	Type	Select the type of bar you want to display on the chart - Line or a Bar.
	Y-Axis 2	This is the second field. Each data point corresponds to a specific value or measurement that will be plotted on the chart.
	Label	It defines the text shown on the chart to describe data point and helps to quickly understand what the value represents. This field populates when the **Cluster By** field is set to **None**.
	Type	Select the type of bar you want to display on the chart - Line or a Bar.
	Y-Axis 3	This field is used to specify the data that will be represented as data points in the chart. Each data point corresponds to a specific value or measurement that will be plotted on the chart.
	Label	It defines the text shown on the chart to describe data point and helps to quickly understand what the value represents.

Section	Fields	Description
		This field populates when the **Cluster By** field is set to **None**.
	Type	Select the type of bar you want to display on the chart - Line or a Bar.
	+ Add More Chart Data Point	Click to add more data points to the chart. This field populates when the **Cluster By** field is set to **None**.

3. Visualization Settings Section

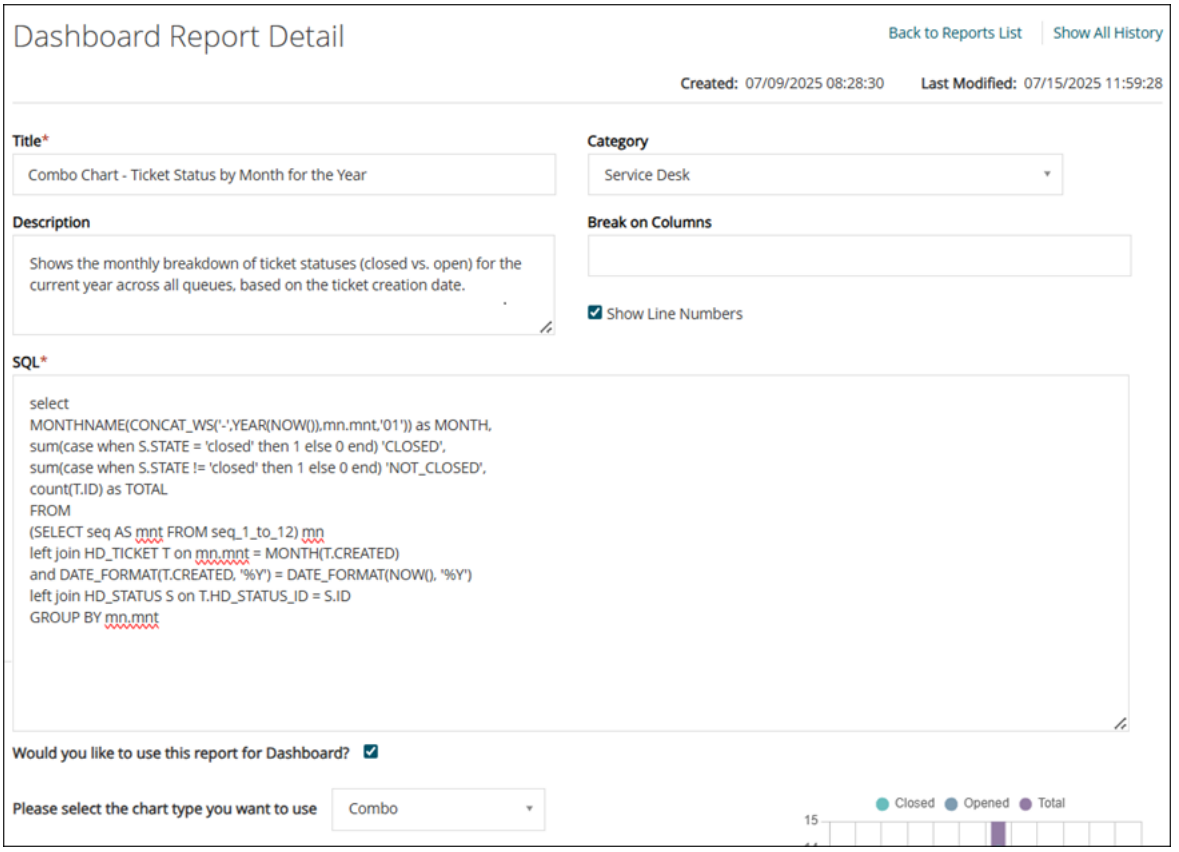
Section	Fields	Description
Visualization Settings		The settings define how the chart is visually presented. These settings help make the chart easier to read and interpret.
	Legend Position	Select the position from the drop-down. It specifies where the chart legend is displayed, such as top, bottom, left, or right of the chart. Select **None** to hide the legend.
	X-Axis Title	Enter the title to display on X-Axis.
	Y-Axis Title	Enter the title to display on Y-Axis.
	Stacked	Select this to displays multiple data series on top of each other in a single bar or column, showing the combined total for each category instead of separate segments.
	Fill	Select to apply a color fill beneath the line (in line charts).
	Line Tension	Select the option from the drop-down to define the curvature of the lines connecting data points in a radar chart.
	Graph Orientation	Select an option from the drop-down to set the direction of the chart's base axis- horizontal or vertical. This changes how the chart layout is displayed.

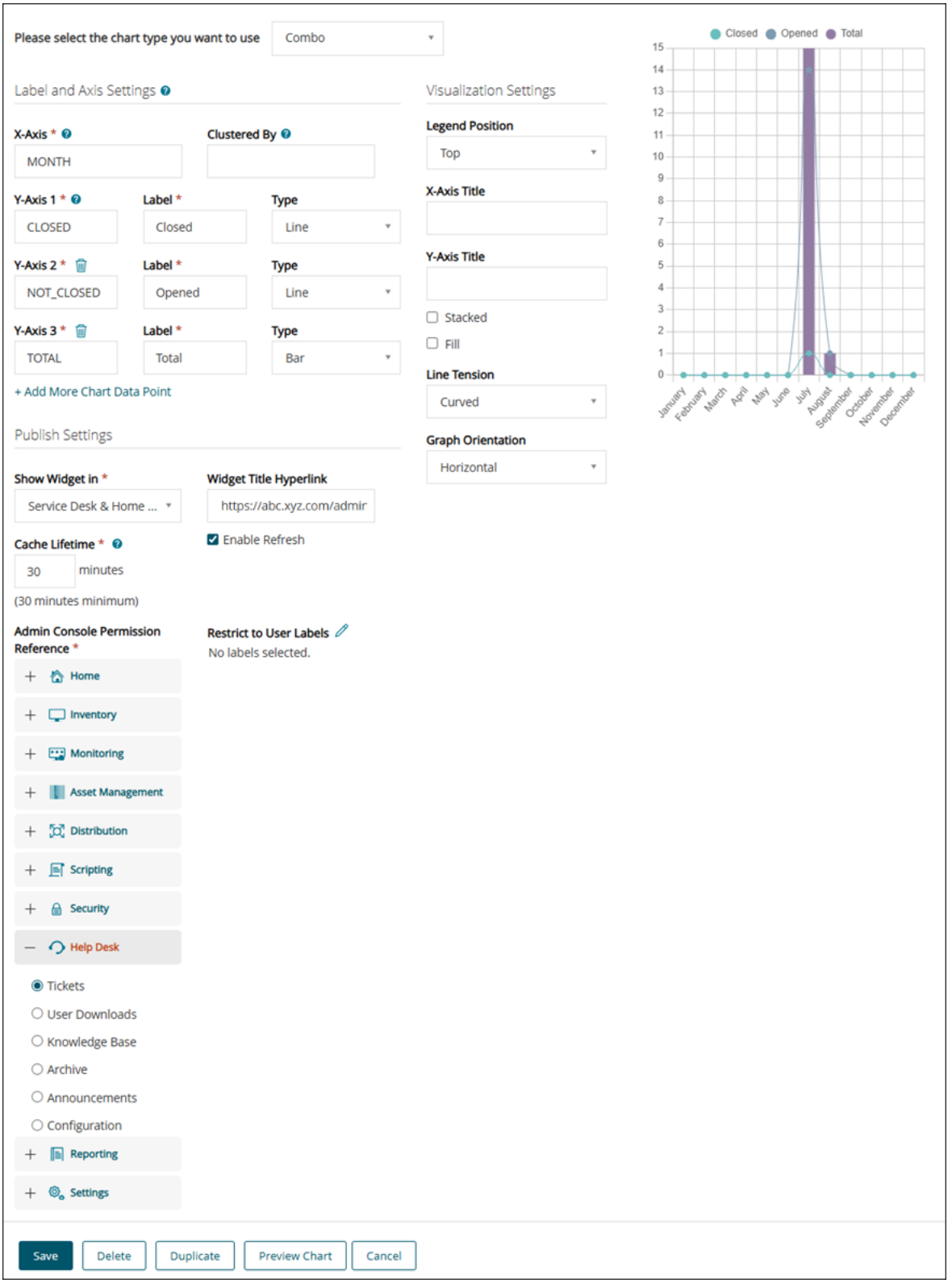
4. **Publish Settings** Section

Section	Fields	Description
Publish Settings		Defines where and how the widget is displayed on dashboards.
	Show Widget in	Select the dashboard category where you wish to make the widget available. All the widgets are available on the **Home** dashboard **NOTE:** This is not a permission control; it is simply linking widget to dashboard. This makes the widget available for selection in a particular dashboard.
	Widget Title Hyperlink	Add a clickable link to the widget title. When users click the title, it opens the specified URL in a new tab.

Section	Fields	Description
	Cache Lifetime	Set the duration the data will be cached for. The minimum duration is 30 minutes
	Restrict to User Labels	Select the Labels to show the widget only to the users assigned to the selected label.
	Enable Refresh	It allows the widget to automatically update its data at regular intervals or when manually refreshed. When enabled, a refresh icon appears on the widget, letting you to reload the latest data.
	Admin Console Permission Reference	This field is available only to a non-wizard type of report. It specifies the permission category required to view the widget. This field ensures that only users with the appropriate access rights (defined in their role permissions) can view or interact with the widget on the dashboard. **NOTE:** This field enforces permission control. If a user does not have access to the selected permission category (for example, Tickets, Devices), the widget will not appear in the **Add Widget** list. If the widget was previously added to a dashboard and the user's permission is later revoked, the widget will display an error message indicating that the user does not have permission to view it.
Preview Chart		Click it to view how the chart will appear using the selected configuration.
Finish		Click it after you finish the configuration.

The example below demonstrates how to configure a dashboard report using a combo chart. This chart compares ticket counts by status across each month of the current year. Closed and Open ticket counts are represented by lines, while the Total Ticket Count is represented by bars.


Dashboard Report Detail
Back to Reports List
Show All History
Created: 07/09/2025 08:28:30
Last Modified: 07/15/2025 11:59:28
Title*
Combo Chart - Ticket Status by Month for the Year
Category
Service Desk
Description
Shows the monthly breakdown of ticket statuses (closed vs. open) for the current year across all queues, based on the ticket creation date.
Break on Columns
Show Line Numbers
SQL*
select
MONTHNAME(CONCAT_WS('-',YEAR(NOW()),mn.mnt,'01')) as MONTH,
sum(case when S.STATE = 'closed' then 1 else 0 end) 'CLOSED',
sum(case when S.STATE != 'closed' then 1 else 0 end) 'NOT_CLOSED',
count(T.ID) as TOTAL
FROM
(SELECT seq AS mnt FROM seq_1_to_12) mn
left join HD_TICKET T on mn.mnt = MONTH(T.CREATED)
and DATE_FORMAT(T.CREATED, '%Y') = DATE_FORMAT(NOW(), '%Y')
left join HD_STATUS S on T.HD_STATUS_ID = S.ID
GROUP BY mn.mnt
Would you like to use this report for Dashboard?
Please select the chart type you want to use
Combo
Closed
Opened
Total
15


Please select the chart type you want to use
Combo
Label and Axis Settings
X-Axis *
MONTH
Clustered By
Y-Axis 1 *
CLOSED
Label *
Closed
Type
Line
Y-Axis 2 *
NOT_CLOSED
Label *
Opened
Type
Line
Y-Axis 3 *
TOTAL
Label *
Total
Type
Bar
+ Add More Chart Data Point
Publish Settings
Show Widget in *
Service Desk & Home ...
Widget Title Hyperlink
https://abc.xyz.com/admir
Enable Refresh
Cache Lifetime *
30
minutes
(30 minutes minimum)
Admin Console Permission Reference *
Restrict to User Labels
No labels selected.
Home
Inventory
Monitoring
Asset Management
Distribution
Scripting
Security
Help Desk
Tickets
User Downloads
Knowledge Base
Archive
Announcements
Configuration
Reporting
Settings
Visualization Settings
Legend Position
Top
X-Axis Title
Y-Axis Title
Stacked
Fill
Line Tension
Curved
Graph Orientation
Horizontal
Closed
Opened
Total
January
February
March
April
May
June
July
August
September
October
November
December
Save
Delete
Duplicate
Preview Chart
Cancel

Doughnut Chart

The Doughnut chart is a circular statistical graphic that is similar to Pie chart but with a hollow center. It is useful for comparing categorical data like operating systems or patch statuses and so on.

You should select **Doughnut** from the **Please select the chart type you want to use** drop-down. Configure the fields for the **Doughnut** chart in the following sections:

1. **Label and Axis Settings** Section

Section	Fields	Description
Label and Axis Settings		This section allows you to define which report columns are used for chart elements such as axes, legends, and data point values across various chart types. Configure these settings to control how your data is organized and displayed.
	Legend	Select a category or group from the drop-down list to represent each slice of the Doughnut chart.
	Value	It specifies the data that determines the size of each slice in the pie chart. Each value represents a measurable quantity that is visually proportioned to reflect its share of the total. For example, refer the image for Doughnut Chart - it is a Doughnut chart for **Device per OS**. **Legend**: OS Name Value: Device ID Count
	Label	Type the text shown on the chart to describe data point and helps to quickly understand what the value represents.
	+ Add More Chart Data Point	Click to add more data points, such as Value and Label.

2. Visualization Settings Section

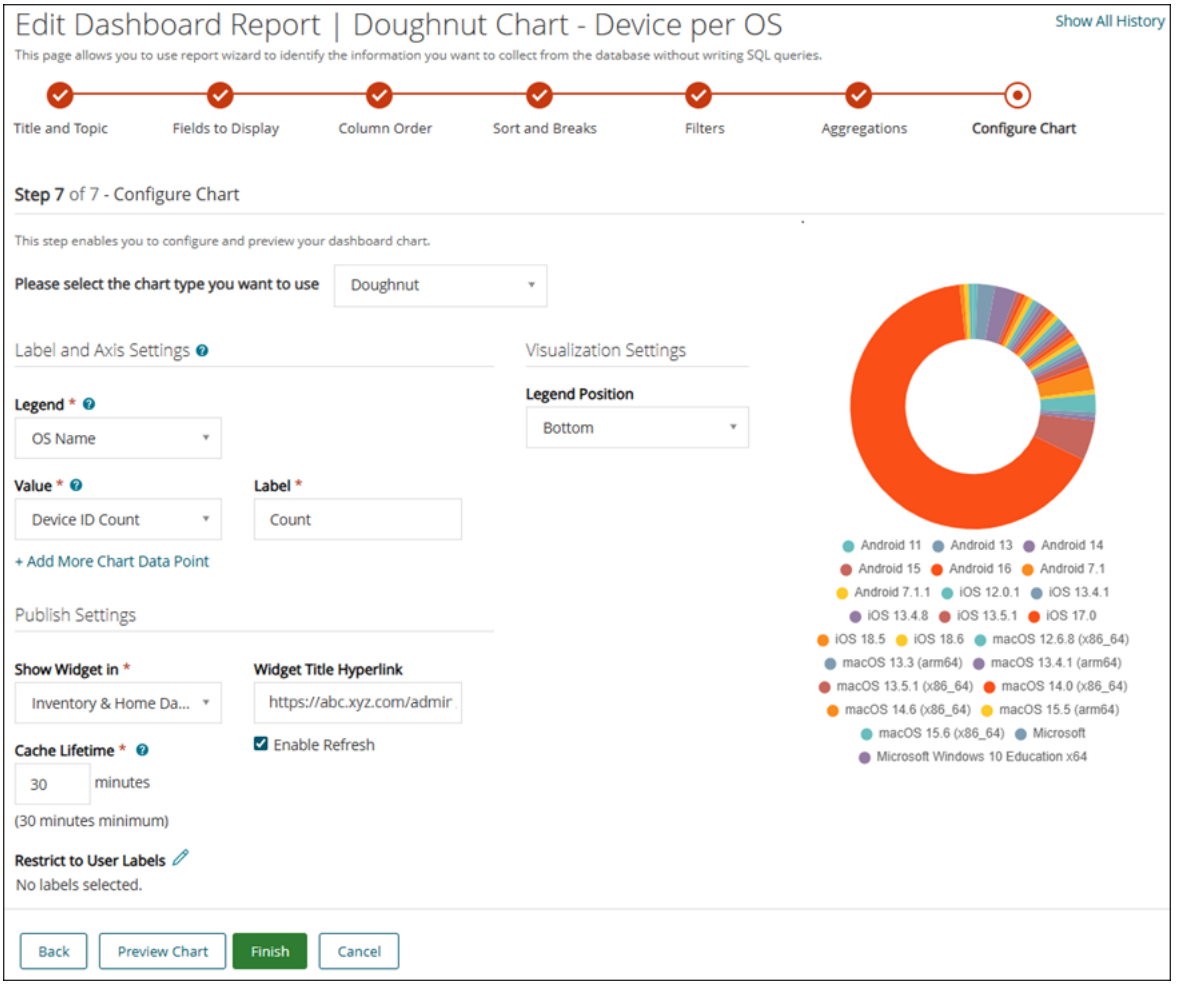
Section	Fields	Description
Visualization Settings		The settings define how the chart is visually presented. These settings help make the chart easier to read and interpret.
	Legend Position	Specifies where the chart legend is displayed, such as top, bottom, left, or right of the chart. Select None to hide the legend.

3. **Publish Settings** Section

Section	Fields	Description
Publish Settings		Defines where and how the widget is displayed on dashboards.
	Show Widget in	Select the dashboard category where you wish to make the widget available. All the widgets are available on the **Home** dashboard **NOTE:** This is not a permission control; it is simply linking widget to dashboard. This makes the widget available for selection in a particular dashboard.

Section	Fields	Description
	Widget Title Hyperlink	Add a clickable link to the widget title. When users click the title, it opens the specified URL in a new tab.
	Cache Lifetime	Set the duration the data will be cached for. The minimum duration is 30 minutes
	Restrict to User Labels	Select the Labels to show the widget only to the users assigned to the selected label.
	Enable Refresh	It allows the widget to automatically update its data at regular intervals or when manually refreshed. When enabled, a refresh icon appears on the widget, letting you to reload the latest data.
	Admin Console Permission Reference	This field is available only to a non-wizard type of report. It specifies the permission category required to view the widget. This field ensures that only users with the appropriate access rights (defined in their role permissions) can view or interact with the widget on the dashboard. **NOTE:** This field enforces permission control. If a user does not have access to the selected permission category (for example, Tickets, Devices), the widget will not appear in the **Add Widget** list. If the widget was previously added to a dashboard and the user's permission is later revoked, the widget will display an error message indicating that the user does not have permission to view it.
Preview Chart		Click it to view how the chart will appear using the selected configuration.
Finish		Click it after you finish the configuration.

The example below demonstrates how to configure a dashboard report using a doughnut chart. This chart illustrates the number of devices categorized by operating system.



Score Chart

The Score chart displays a single metric or Key Performance Indicator (KPI), such as counts of updated devices and so on. This chart offers a focused view on a single value.

You should select **Score** from the **Please select the chart type you want to use** drop-down. Configure the fields for the **Score** chart in the following sections:

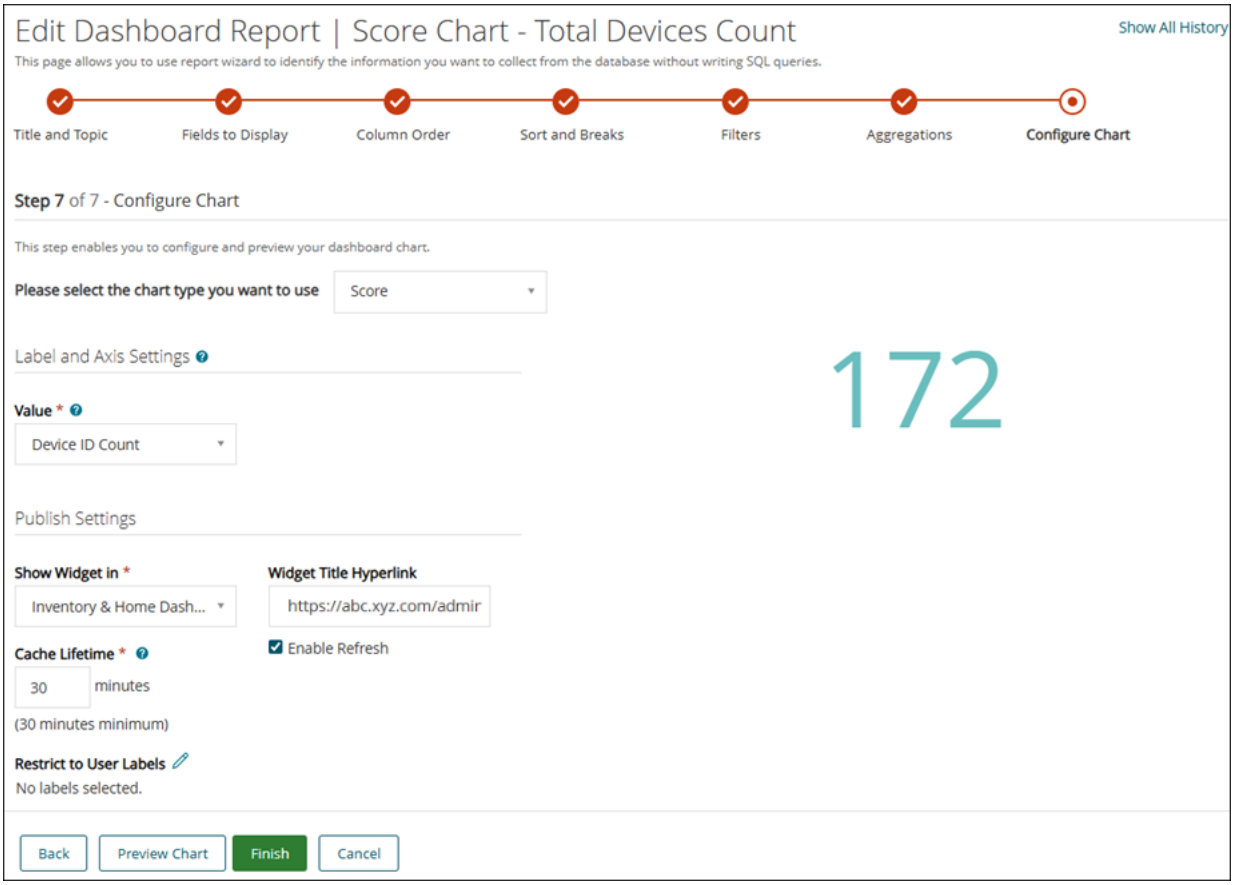
1. **Label and Axis Settings** Section

Section	Fields	Description
Label and Axis Settings		This section allows you to define which report columns are used for chart elements such as axes, legends, and data point values across various chart types. Configure these settings to control how your data is organized and displayed.
	Value	It represents the primary metric displayed on the score chart. This is the numeric value shown prominently to indicate a key performance indicator (KPI), such as total open tickets, total users, or any other measurable data point. For example, refer the image for Score **Chart** - it is a Score chart for **Total Device Count**. **Value**: Device ID Count

2. **Publish Settings** Section

Section	Fields	Description
Publish Settings		Defines where and how the widget is displayed on dashboards.
	Show Widget in	Select the dashboard category where you wish to make the widget available. All the widgets are available on the **Home** dashboard **NOTE:** This is not a permission control; it is simply linking widget to dashboard. This makes the widget available for selection in a particular dashboard.
	Widget Title Hyperlink	Add a clickable link to the widget title. When users click the title, it opens the specified URL in a new tab.
	Cache Lifetime	Set the duration the data will be cached for. The minimum duration is 30 minutes
	Restrict to User Labels	Select the Labels to show the widget only to the users assigned to the selected label.
	Enable Refresh	It allows the widget to automatically update its data at regular intervals or when manually refreshed. When enabled, a refresh icon appears on the widget, letting you to reload the latest data.
	Admin Console Permission Reference	This field is available only to a non-wizard type of report. It specifies the permission category required to view the widget. This field ensures that only users with the appropriate access rights (defined in their role permissions) can view or interact with the widget on the dashboard. **NOTE:** This field enforces permission control. If a user does not have access to the selected permission category (for example, Tickets, Devices), the widget will not appear in the **Add Widget** list. If the widget was previously added to a dashboard and the user's permission is later revoked, the widget will display an error message indicating that the user does not have permission to view it.
Preview Chart		Click it to view how the chart will appear using the selected configuration.
Finish		Click it after you finish the configuration.

The example below shows how to configure a dashboard report using a Score chart. This chart illustrates the Score chart for Total devices Count.



Line Chart

A line chart shows trends over time using points connected by lines. It is typically used to visualize time-series data, such as patch deployment trends or ticket volume and so on, making it easy to track changes and patterns across different time periods.

Once you add the details for creating report with SQL (for more information, refer Create dashboard report using SQL queries), you should select **Would you like to use this report for Dashboard**. Configure the fields for the **Line** chart in the following sections:

1. Select appropriate option.

Fields	Description
Would you like to use this report for Dashboard?	Select the option if you want to display the report on the dashboard. Once you select this option, the following fields are displayed.
Please select the chart type you want to use	You should select **Line** from the drop-down.

2. **Label and Axis Settings** Section

Section	Fields	Description
Label and Axis Settings		This section allows you to define which report columns are used for chart elements such as axes, legends, and data point values across various chart types. Configure these settings to control how your data is organized and displayed.

Section	Fields	Description
	X-Axis	It specifies the categories or groups that represents the labels for the chart's X-Axis (or Y-Axis if chart's orientation is set to vertical).
	Y-Axis	It specifies the data that will be represented as data points in the chart. Each data point corresponds to a specific value or measurement that will be plotted on the chart.
	Clustered By	The field specifies the grouping or clustering criteria for the chart's data points. Set this to the field that defines how the data should be grouped or categorized for visualization.
	Label	It defines the text shown on the chart to describe data point and helps to quickly understand what the value represents.
	+ Add More Chart Data Point	Click to add more data points on Y-Axis and add a Label to it.

3. **Visualization Settings** Section

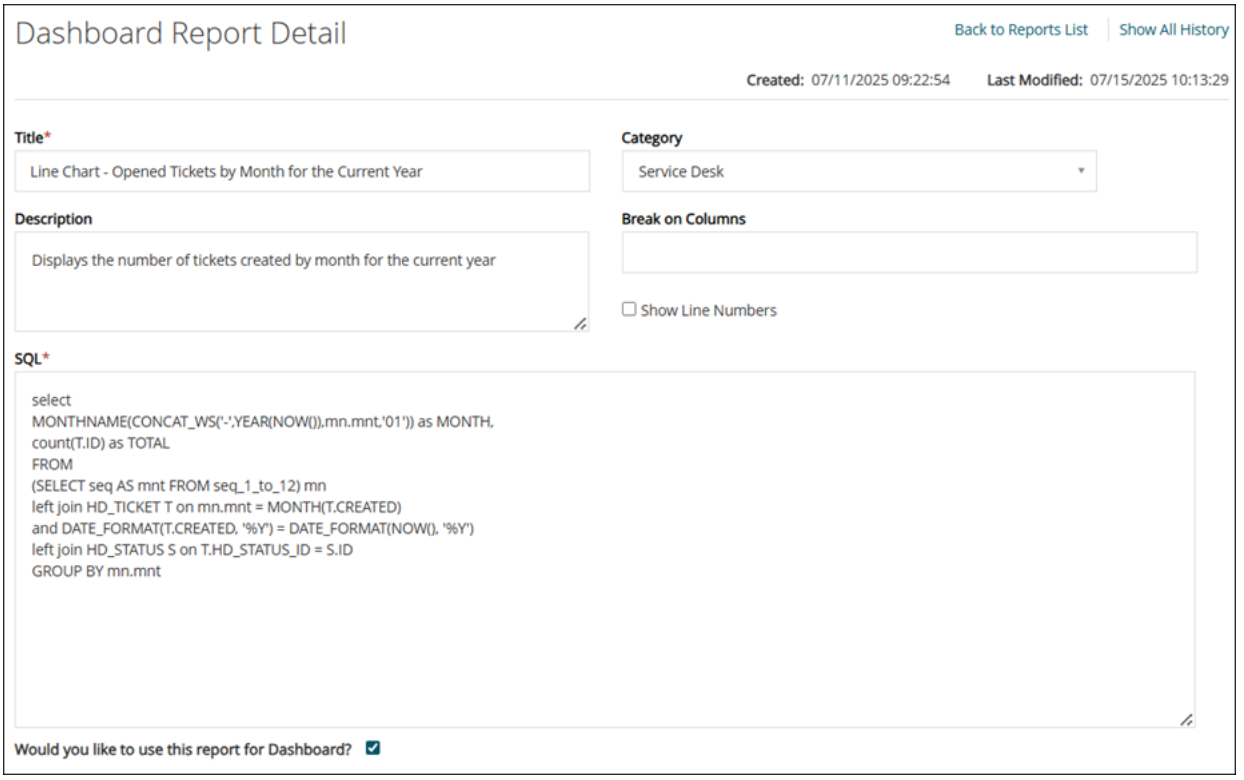
Section	Fields	Description
Visualization Settings		This section allows you to define which report columns are used for chart elements such as axes, legends, and data point values across various chart types. Configure these settings to control how your data is organized and displayed.
	Legend Position	Select the position from the drop-down. It specifies where the chart legend is displayed, such as top, bottom, left, or right of the chart. Select **None** to hide the legend.
	X-Axis Title	Enter the title to display on X-Axis.
	Y-Axis Title	Enter the title to display on Y-Axis.
	Stacked	Select this to displays multiple data series on top of each other in a single bar or column, showing the combined total for each category instead of separate segments.
	Fill	Select to apply a color fill beneath the line (in line charts).
	Line Tension	Select the option from the drop-down to define the curvature of the lines connecting data points in a radar chart.
	Graph Orientation	Select an option from the drop-down to set the direction of the chart's base axis- horizontal or vertical. This changes how the chart layout is displayed.

4. **Publish Settings** Section

Section	Fields	Description
Publish Settings		Defines where and how the widget is displayed on dashboards.

Section	Fields	Description
	Show Widget in	Select the dashboard category where you wish to make the widget available. All the widgets are available on the **Home** dashboard **NOTE:** This is not a permission control; it is simply linking widget to dashboard. This makes the widget available for selection in a particular dashboard.
	Widget Title Hyperlink	Add a clickable link to the widget title. When users click the title, it opens the specified URL in a new tab.
	Cache Lifetime	Set the duration the data will be cached for. The minimum duration is 30 minutes
	Restrict to User Labels	Select the Labels to show the widget only to the users assigned to the selected label.
	Enable Refresh	It allows the widget to automatically update its data at regular intervals or when manually refreshed. When enabled, a refresh icon appears on the widget, letting you to reload the latest data.
	Admin Console Permission Reference	This field is available only to a non-wizard type of report. It specifies the permission category required to view the widget. This field ensures that only users with the appropriate access rights (defined in their role permissions) can view or interact with the widget on the dashboard. **NOTE:** This field enforces permission control. If a user does not have access to the selected permission category (for example, Tickets, Devices), the widget will not appear in the **Add Widget** list. If the widget was previously added to a dashboard and the user's permission is later revoked, the widget will display an error message indicating that the user does not have permission to view it.
Preview Chart		Click it to view how the chart will appear using the selected configuration.
Finish		Click it after you finish the configuration.

The example below demonstrates how to configure a dashboard report using a line chart. This chart compares the number of tickets created each month throughout the current year.


Dashboard Report Detail
Back to Reports List
Show All History
Created: 07/11/2025 09:22:54
Last Modified: 07/15/2025 10:13:29
Title*
Line Chart - Opened Tickets by Month for the Current Year
Category
Service Desk
Description
Displays the number of tickets created by month for the current year
Break on Columns
Show Line Numbers
SQL*
select
MONTHNAME(CONCAT_WS('-',YEAR(NOW()),mn.mnt,'01')) as MONTH,
count(T.ID) as TOTAL
FROM
(SELECT seq AS mnt FROM seq_1_to_12) mn
left join HD_TICKET T on mn.mnt = MONTH(T.CREATED)
and DATE_FORMAT(T.CREATED, '%Y') = DATE_FORMAT(NOW(), '%Y')
left join HD_STATUS S on T.HD_STATUS_ID = S.ID
GROUP BY mn.mnt
Would you like to use this report for Dashboard?

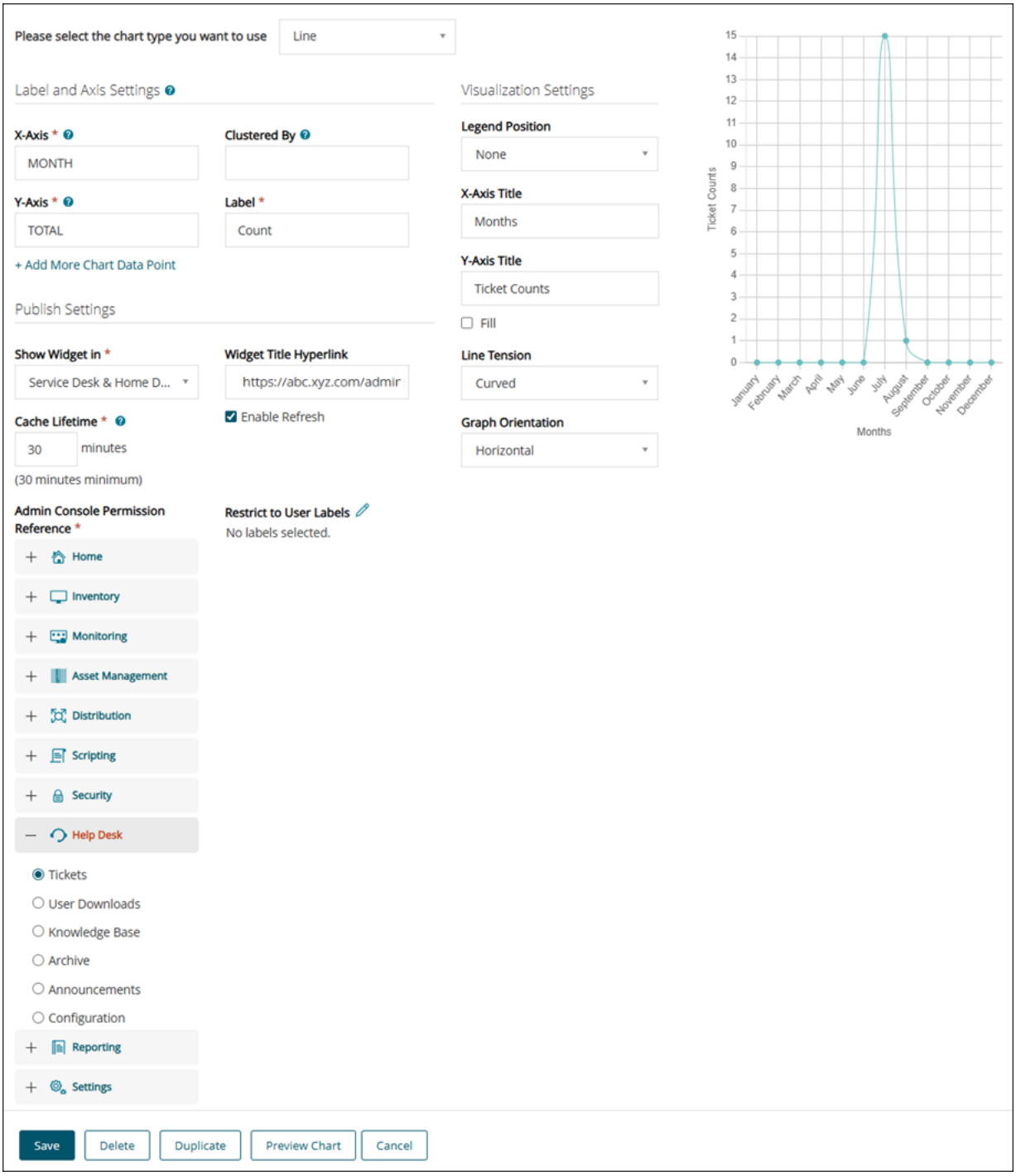


Chart Types in Widgets

Each widget can be customized to display various types of charts, based on the data and the preferred visual representation.

In many cases, after creating a widget, you may want to change the chart type based on the visualization needs or user preference. While editing a widget, some chart types can be converted to others, making it easy to change it without creating from scratch.

The table below lists each supported chart type, its description, and the other chart types it can be converted into when editing.

Chart Type	Convertible to other Chart Types
Pie	Doughnut, Line, Bar, Polar Area, Radar, Table
Doughnut	Pie, Line, Bar, Polar Area, Radar, Table
Line	Pie, Doughnut, Bar, Polar Area, Radar, Table
Bar	Pie, Doughnut, Line, Polar Area, Radar, Table
Combo	Pie, Doughnut, Line, Bar, Polar Area, Radar, Table
Polar Area	Pie, Doughnut, Line, Bar, Radar, Table
Radar	Pie, Doughnut, Line, Bar, Polar Area, Table
World Geography	Pie, Doughnut, Line, Bar, Polar Area
US Geography	Pie, Doughnut, Line, Bar, Polar Area
Score	Score
Progress	Gauge
Table	Pie, Doughnut, Line, Bar, Polar Area, Radar
Gauge	Progress

Chart Usage Guidelines

Here are some guidelines when using the following chart types:

- **Use Line or Bar charts** to analyze time-based trends such as patch deployments or script execution history.
- **Pie and Doughnut charts** are ideal for showing categorical distribution, such as OS breakdown or ticket categories.
- **Table view** is best when precise data and filtering are needed, such as listing vulnerable devices or script results.
- **Score, Gauge, and Progress** charts are used to highlight a single metric or indicate how close the system is to a defined goal.
- **Radar and Polar Area** charts can compare metrics like compliance ratings across multiple policies or departments.
- **World and US Geography** charts help visualize endpoint distribution geographically for global and regional tracking.

NOTE: When you create a chart, always preview the converted chart to ensure data readability and correct formatting.

Dashboard Widgets with Multi-Instance Support

The widgets, once added to a dashboard, are removed from the **Add Widget** list to prevent duplication. However, some widgets can be added multiple times to a dashboard. If the widget is added to dashboard, you can still view it in the Add Widget list. You can add them again with different parameters (for example, grouping by different fields such as owner or priority).

The following is the list of widgets that can be added repeatedly:

Widgets	Description
Active Tickets	Shows the current active service desk tickets by owner, category, priority, queue, or range.
Overdue Tickets	Shows the overdue service desk tickets by owner, category, priority, queue, or range.
Overdue Tickets Today	Shows today's overdue service desk tickets by owner, category, priority, or queue.
Closed Tickets	Shows closed service desk tickets by owner, category, priority, queue, or range.
Tickets Due Today	Shows the service desk tickets due today by owner, category, priority, or queue.
Reopened Tickets	Shows reopened tickets by owner, category, priority, queue, or range.
Average Ticket Resolution Time	Shows average resolution time by owner, category, priority, queue, or month.
Compliance By Machine	Shows patch compliance by machine.
Patch Failed	Shows patches failed.
Compliance By Patch	Shows patch compliance by patch.
Patches Deployed	Shows patches deployed.
Patches Released	Shows patches released.

Duplicate reports

You can duplicate any report, including standard reports that are shipped with the appliance. If you are creating a report that is similar to an existing report, duplicating the existing report can be faster than creating a report from scratch.

1. Go to the *Reports* list by doing one of the following:

   - **If your appliance has the Organization component enabled, and you want to access a System-level report:**

     Log in to the appliance System Administration Console, `https://`**appliance_hostname**`/system`, or select **System** from the drop-down list in the top-right corner of the page. Then click **Reporting**.
     System-level reports include consolidated reports that aggregate information from all organizations, as well as standard reports for various appliance components.

   - **If your appliance does not have the Organization component enabled, or if you want to access an organization-level report, log in to the appliance Administrator Console, `https://appliance_hostname/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information. Then click Reporting.**

     Organization-level reports include standard reports for various appliance components. If the Organization component is enabled on your appliance, these reports provide information specific to the selected organization.

   The *Reports* list appears.
2. Click the title of a report.

Depending on the type of report, either the *Report Detail* page or the first page in the report wizard appears.

3. At the bottom of the page, click **Duplicate**.

   Depending on the type of report, either the *Report Detail* page or the first page in the report wizard appears.

4. Modify the report details as necessary, then click **Save**.

Edit SQL statements on reports created with the report wizard

You can edit the SQL statements on single-topic reports created with the report wizard.

This editing is useful when you want to change the SQL statement, or when you want to copy the SQL statement to a new report. The edit option is not available on multi-topic reports.

1. Go to the *Reports* list by doing one of the following:

   - **If your appliance has the Organization component enabled, and you want to access a System-level report:**

     Log in to the appliance System Administration Console, `https://`**appliance_hostname**`/system`, or select **System** from the drop-down list in the top-right corner of the page. Then click **Reporting**.
     System-level reports include consolidated reports that aggregate information from all organizations, as well as standard reports for various appliance components.

   - **If your appliance does not have the Organization component enabled, or if you want to access an organization-level report, log in to the appliance Administrator Console, `https://`appliance_hostname`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information. Then click Reporting.**

     Organization-level reports include standard reports for various appliance components. If the Organization component is enabled on your appliance, these reports provide information specific to the selected organization.

   The *Reports* list appears.

2. Click the title of a single-topic report created with the report wizard.

   The report wizard appears.

3. At the bottom of the form, click **Edit SQL** to display the *Report Detail* page.
4. Edit or copy text in the *SQL* field as needed, then click **Save**.

> **NOTE:** When copying SQL statements from one type of report to another, you might have to modify the SQL statement before you can use it. For example, if you copy the SQL statement from an application compliance report, and paste it into a report that has the *Aggregate Results* option for organizations selected, the appliance reports errors in the SQL statement. You cannot save the report until the errors are resolved.

Modifying reports

You can modify or delete reports as needed.

Edit reports

You can edit any custom report, but you cannot edit the standard reports that are shipped with the appliance.

To edit a standard report, first duplicate it, then edit the duplicated report. See Duplicate reports.

1. Do one of the following:
   - **To edit organization-level reports, select an organization in the drop-down list in the top-right corner of the page (if applicable), then click Reporting.**
   - **To edit System-level reports, log in to the System Administration Console, `http://appliance_hostname/system`, or select System in the drop-down list in the top-right corner of the page. Then click Reporting (for appliances with the Organization component enabled only).**

   The *Reports* page appears.
2. Click the title of a report to display the *Report Detail* page.

Delete reports

You can delete any custom report, but you cannot delete standard reports shipped with the appliance.

1. Do one of the following:
   - **To delete organization-level reports, select an organization in the drop-down list in the top-right corner of the page (if applicable), then click Reporting.**
   - **To delete System-level reports, log in to the System Administration Console, `http://appliance_hostname/system`, or select System in the drop-down list in the top-right corner of the page. Then click Reporting (for appliances with the Organization component enabled only).**

   The *Reports* page appears.
2. Select the check box next to one or more reports.
3. Select **Choose Action** > **Delete**, then click **Yes** to confirm.

Customizing logos used for reports

Reports use the Quest logo by default, but you can replace it with your own logo.

To upload your own logo, see the *Logo Overrides* sections in:

- Configure appliance General Settings with the Organization component enabled
- Configure appliance General Settings without the Organization component

Scheduling reports and notifications

You can schedule reports and notifications to monitor the activity on your appliance.

Running single-organization and consolidated reports

If the Organization component is enabled on your appliance, and if you have multiple organizations on your appliance, you can run single-organization reports for each organization separately.

In addition, you can run consolidated reports that provide information for all organizations in a single report.

Run single-organization reports

Single-organization reports show information specific to a single organization.

If the Organization component is not enabled on your appliance, or if you have only a single organization, these reports provide information about the Default organization.

1. Go to the *Reports* list:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Reporting**, then click **Reports**.
2. In the *Generate Report* column, click a format type for the report.

    HTML reports are displayed in a new window. For other formats, you can open the file or save it to your device.

    NOTE: Charts and graphs cannot be created from within the appliance reporting tool. To create charts or graphs, generate a report in **XLS** (Microsoft Excel) or **CSV** (comma-separated value) format, then import the data into a tool that has chart or graph capabilities, such as Microsoft Excel.

    NOTE: Be aware that multibyte characters, such as those used to support Japanese and Chinese character sets, might display as "garbage characters" when CSV files are imported to Excel. For more information, contact **Quest Support** at https://support.quest.com/contact-support.

Run consolidated organization reports

If the Organization component is enabled on your appliance, you can run reports that consolidate the information from all organizations into a single report.

1. Go to the *Reports* list:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Reporting**, then click **Reports**.
2. In the *Generate Report* column, click a format type for the report.

    HTML reports are displayed in a new window. For other formats, you can open the file or save it to your device.

    NOTE: Charts and graphs cannot be created from within the appliance reporting tool. To create charts or graphs, generate a report in **XLS** (Microsoft Excel) or **CSV** (comma-separated value) format, then import the data into a tool that has chart or graph capabilities, such as Microsoft Excel.

    NOTE: Be aware that multibyte characters, such as those used to support Japanese and Chinese character sets, might display as "garbage characters" when CSV files are imported to Excel. For more information, contact **Quest Support** at https://support.quest.com/contact-support.

Scheduling reports

To monitor your environment, you can schedule the appliance to run reports and send them to administrators at specified times and intervals. This is useful for tracking software, devices, and system health.

Add report schedules

You can add report schedules to enable the appliance to run reports automatically at specified times. This is useful for reports that you need to run periodically, such as software License Compliance reports.

1. Do one of the following:
   - **To schedule organization-level reports, select an organization in the drop-down list in the top-right corner of the page (if applicable), then click Reporting.**
   - **To schedule System-level reports, log in to the System Administration Console, `http://appliance_hostname/system`, or select System in the drop-down list in the top-right corner of the page. Then click Reporting (for appliances with the Organization component enabled only).**

   The *Reports* page appears.
2. Do one of the following:
   - **Click the Schedule button next to a report:** .
   - **Click Report Schedules on the left navigation bar, then select Choose Action > New to display the *Report Schedule Detail* page.**
3. Specify the following settings in the *Configure* tab.

Option	Description
Name	The display name for the schedule. Make this name as descriptive as possible, so you can distinguish this schedule from others.
Report	The name of the report you are scheduling. This name is provided automatically if you click the **Schedule** button next to a report on the *Reports* page.
Formats	The format of the report.
Description	A description of the schedule. This description appears on the *Schedule Reports* page.

4. In the *Notify* tab, specify the following settings:

Option	Description
Subject	The subject line of the email message that contains the report.
Recipients	The email addresses where the report is to be sent. Separate multiple addresses with a comma.
Don't send empty reports	Whether the appliance should send the report every time, or only when results are found. Select this option to prevent the appliance from sending the report if it is empty.
Message	Any information you want to provide in the body of the email message.
Attachment Options	The format for the report. Choose **Attachment** to attach the file to the email message, or choose **Zipped Attachment** to attach the file as a ZIP archive.

5. In the *Schedule* tab, specify the following settings:

Option	Description
None	Run in combination with an event rather than on a specific date or at a specific time.
Every n hours	Run at a specified interval.
Every day/specific day at HH:MM	Run daily at a specified time, or run on a designated day of the week at a specified time.
Run on the nth of every month/ specific month at HH:MM	Run on the same day every month, or a specific month, at the specified time.
Run on the nth weekday of every month/specific month at HH:MM	Run on the specific weekday of every month, or a specific month, at the specified time.

Custom	Run according to a custom schedule.
	Use standard 5-field cron format (extended cron format is not supported):
	`* * * * *`
	`| | | | +————————day of week (0-6)(Sun=0)`
	`| | | +————————month (1-12)`
	`| | +————————day of month (1-31)`
	`| +————————hour (0-23)`
	`+————————minute (0-59)`
	Use the following when specifying values:
	• **Spaces ( )**: Separate each field with a space.
	• **Asterisks (*)**: Include the entire range of values in a field with an asterisk. For example, an asterisk in the hour field indicates every hour.
	• **Commas (,)**: Separate multiple values in a field with a comma. For example, `0,6` in the day of the week field indicates Sunday and Saturday.
	• **Hyphens (-)**: Indicate a range of values in a field with a hyphen. For example, `1-5` in the day of the week field is equivalent to `1,2,3,4,5`, which indicates Monday through Friday.
	• **Slashes (/)**: Specify the intervals at which to repeat an action with a slash. For example, `*/3` in the hour field is equivalent to `0,3,6,9,12,15,18,21`. The asterisk (`*`) specifies every hour, but `/3` restricts this to hours divisible by 3.
	Examples:
	• `15 * * * * Run 15 minutes after every hour every day`
	• `0 22 * * * Run at 22:00 every day`
	• `0 0 1 1,6 * Run at 00:00 on January 1 and June 1`
	• `30 8,12 * * 1-5 Run weekdays at 08:30 and 12:30`
	• `0 2 */2 * * Run every other day at 02:00`

Option	Description
View Task Schedule	Click to view the task schedule. The *Task Schedule* dialog box displays a list of scheduled tasks. Click a task to review the task details. For more information, see View task schedules.

6. Click **Save**.

Delete report schedules

Report schedules enable the appliance to run reports at specified times and intervals. When you delete report schedules, both the report criteria and the schedule settings are removed from the appliance.

Report schedules can be deleted any time as needed.

1. Do one of the following:
   - **To delete organization-level report schedules, select an organization in the drop-down list in the top-right corner of the page (if applicable), then click Reporting.**
   - **To delete System-level report schedules, log in to the System Administration Console, `http://appliance_hostname/system`, or select System in the drop-down list in the top-right corner of the page. Then click Reporting (for appliances with the Organization component enabled only).**

   The *Reports* page appears.
2. On the left navigation bar, click **Report Schedules** to display the *Report Schedules* page.
3. Select the check box next to one or more report schedules.
4. Select **Choose Action** > **Delete**, then click **Yes** to confirm.

Scheduling notifications

To maintain a watch on your environment, you can schedule the appliance to notify administrators through email when specified criteria are met. This activity is useful for watching system health and device properties.

You can add, edit, and delete notification schedules.

Add notification schedules from the Reporting section

You can add notification schedules for devices, discovery scans, and assets from the *Reporting* section.

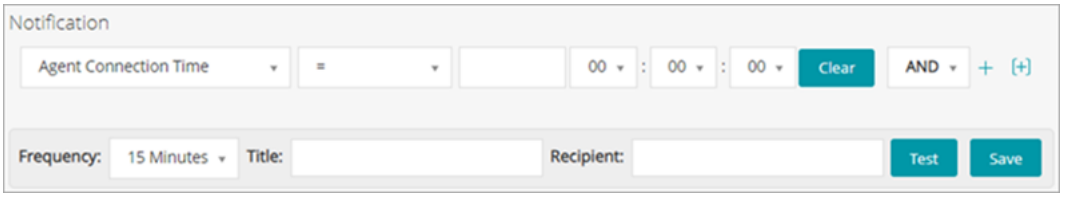
1. Go to the *Notification Schedules* list page:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.

b. On the left navigation bar, click **Reporting**, then click **Notifications**.

2. Select **Choose Action** and select one of the following:

   - **New** > **Antivirus Notification**
   - **New** > **Device Notification**
   - **New** > **Discovery Notification**
   - **New** > **Asset Notification**
   - **New** > **Contract Notification**
   - **New** > **License Notification**
   - **New** > **Purchase Notification**
   - **New** > **Monitoring Alerts Notification**
   - **New** > **Quarantine Notification**

   The *Notification* panel appears.



3. Select notification criteria. For example, to send a notification when Windows 7 devices have not connected to the appliance within 24 hours, specify the following:

   a. Specify the criteria required to find devices that have the Windows 7 operating system:

      ```
      Operating System: Name | contains | Windows 7
      ```

   b. With **AND** selected in the operator drop-down list, click + to add a line.

   c. Specify the criteria required to find devices that have not connected to the appliance in the last 24 hours:

      ```
      Device Identity Information: Last Sync Time | > | 24 hours
      ```

4. Provide the following information below the notification criteria:

Field	Description
Title	The information that you want to appear in the *Subject* line of the email. This also appears as the name of the notification on the *Notification Schedules* page.
Recipient	The email address or addresses of intended recipients. Email addresses must be fully qualified email addresses. To send email to multiple addresses, use commas to separate each address, or use email distribution lists.
Frequency	The interval at which the appliance runs the query to compare the selected criteria with items in inventory. If criteria are met, the notification is sent.

5. **Optional**: To verify the criteria, click **Test**.

   The list is refreshed to show items that match the specified criteria. Notifications are not sent during the test.

6. Click **Save**.

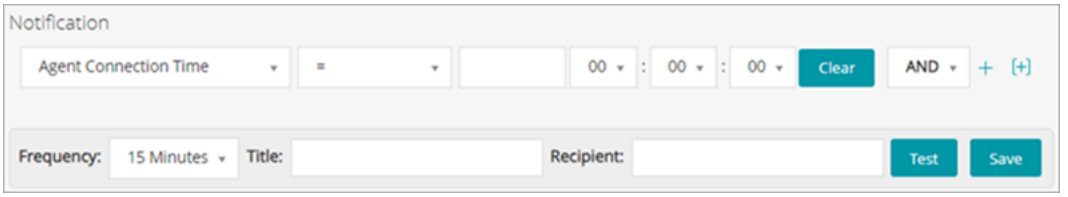
The notification is created and it appears on the *Notification Schedule* page. For information about scheduling the frequency of the notification, see Edit notification schedules.

Add notification schedules from list pages

You can add notification schedules from list pages, such as the *Devices*, *Software*, *Software Catalog*, *Discovery*, or *Assets* page.

1. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
2. Go to a list page, such as the *Devices* list, and click the **Notification** tab above the list on the right.

   The *Notification* panel appears.



3. Select the criteria to use for the notification schedule.

   See Example: Search for managed devices using Filter criteria.

4. Provide the following information below the notification criteria:

Field	Description
Title	The information that you want to appear in the *Subject* line of the email. This title also appears as the name of the notification on the *Notification Schedules* page.
Recipient	The email address or addresses of intended recipients. Email addresses must be fully qualified email addresses. To send email to multiple addresses, use commas to separate each address, or use email distribution lists.
Frequency	The interval at which the appliance runs the query to compare the selected criteria with items in inventory. If criteria are met, the notification is sent.

5. **Optional**: To verify the criteria, click **Test**.

   The list is refreshed to show items that match the specified criteria. Notifications are not sent during the test.

6. Click **Save**.

The notification is created and it appears on the *Notification Schedules* page. Notifications are enabled by default. To disable or add a description to the notification, see Edit notification schedules.

Edit notification schedules

You can enable, disable, change the frequency of, or modify notification schedules as needed.

1. Go to the *Notification Schedules* list page:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Reporting**, then click **Notifications**.
   c. Click the name of a notification.
2. Modify the properties as needed:

Field	Description
Enabled	Whether the notification is active or inactive. Select **Enabled** to permit the appliance to run the query and send the appropriate notifications at the selected frequency. Select **Disabled** to prevent the appliance from running the query and sending notifications.
Name	The information that you want to appear in the *Subject* line of the email. When you create notifications on the *Notification* panel, you enter this information in the *Title* field.
Recipients	The email address or addresses of intended recipients. Email addresses must be fully qualified email addresses. To send email to multiple addresses, use commas to separate each address, or use email distribution lists.
Description	Any additional information you want to provide.
Frequency	The interval at which the appliance runs the query to compare the selected criteria with items in inventory. If criteria are met, the notification is sent.

3. **Optional**: To edit the report using the wizard, select the edit icon next to *To edit the Notification using the original editor* above the **Save** button.
4. **Optional**: To change the SQL criteria that triggers the alert, click the edit icon next to the check box labeled *To edit the Notification using this editor* above the **Save** button.

   If you edit the SQL query, make sure to use the following `as` statements:

   ```
   MACHINE.NAME AS SYSTEM_NAME
   ```

   ```
   MACHINE.ID as TOPIC_ID
   ```

   For example:

   ```
   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. Click **Save**.

Delete notification schedules

When you delete notification schedules, both the notification criteria and the schedule settings are removed from the appliance.

Notification schedules can be deleted any time as needed.

1. Go to the *Notification Schedules* list page:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Reporting**, then click **Notifications**.
2. Select the check box next to one or more notification schedules.
3. Select **Choose Action** > **Delete**, then click **Yes** to confirm.

Monitoring devices

The appliance offers you a module with which you can perform basic performance monitoring for your servers in inventory.

About server monitoring

The appliance monitoring feature targets supported operating systems, and provides default monitoring profiles that define criteria for performance alerts for each operating system. You can define additional, custom profiles that point to alternative event logs or OS level logs, with similar or different criteria.

For details on OS versions supported for server monitoring, see the **Technical Specifications** guides.

NOTE: For Agent-based monitoring to work on an RHEL device running Security-Enhanced Linux (SELinux), SELinux must be either turned off or switched to "permissive mode." You can change the SELinux mode by modifying the file `/etc/selinux/config` and rebooting the device. For further information about enabling or disabling SELinux on Red Hat Enterprise Linux, go to 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.

Table 31. Monitoring interface components under the Monitoring tab in the appliance navigation bar

Section	Description
Devices	For each monitored device, displays most critical alert, alert count, bound profile count, bound Maintenance Window count, and link to detail page to edit configuration settings for the device. This section can also display time alert created and modified, IP address of the monitored device, and whether Configuration Change Alert is enabled.
Alerts	Displays alert level, alert summary, link to detail of alert, date and time of alert creation, most recent repeat time, repeat count, IP address, and status.
Profiles	Displays profile name, list of default profiles and added profiles, count of devices to which the profile is bound, and if the profile is automatically added to a device with a particular operating system type. A profile is where the criteria for triggering an alert is configured. In the profile, the log path and file are defined, along with the search text to look for in the log, and what severity is assigned to the alert. You can bind multiple profiles to a device if there are multiple logs you want to monitor.
Maintenance Windows	Displays Maintenance Window name, count of devices to which the Maintenance Window is bound, whether the Maintenance Window is automatically added to all devices, and link to detail page to edit schedule and OS default settings. This section can also display Maintenance Window description and time Maintenance Window created and modified.
Log Enablement Packages	Displays a base set of Windows Reliability and Performance Monitor (PerfMon) templates and non-Windows open-source Perl scripts, so that you can extend your monitoring capability, and identify system and application performance issues.

Monitoring profiles

With the default monitoring profiles and with profiles you can set up, your appliance can provide:

- Windows event log monitoring
- Non-Windows file system log monitoring
- Configuration change monitoring

In addition, you can use Log Enablement Packages (LEPs) to provide:

- Threshold monitoring
- Application monitoring

You can download your profiles for others to use, and can upload custom profiles that are developed and made available by others.

Free or licensed server monitoring

The appliance comes with monitoring available for 200 servers with your standard license, and you can obtain a license to expand that number. To see how many servers your system is licensed to manage, click on the icon at the top-right corner of the page and then click the icon. The line for *Management Capacity Usage* displays *Monitored Computers*, with the number of devices that currently have monitoring enabled compared to the total number of devices that could be monitored under the existing license.

Working with the alerts

Alerts appear in the **Administrator Console**, where you can review and dismiss them after they have been dealt with. The appliance provides additional capabilities. Among other things, you can:

- Have certain alerts trigger email notifications.
- Create a Service Ticket directly from an alert.
- Have alert notifications sent to a mobile device that uses the KACE GO app.

The appliance has a number of functions that make working with alerts more efficient:

- **Alert consolidation (repeat counts)**: To prevent notification spam, the appliance analyzes the alerts for uniqueness, and uses repeat count for identical alerts to indicate the number of times the alert has been generated.
- **Alert storm mitigation**: To prevent too much repeated data from streaming in, the appliance limits the collection for any one device to 50 alerts in a single collection. The appliance then composes a generic alert indicating that there is abnormal activity that needs attention.
- **Grooming**: A user can dismiss (hide from view, but keep in the database) alerts, or delete alerts manually or automatically after a set number of days. However, the appliance automatically limits a device to storing 2000 alerts before the appliance begins deleting alerts from the database.

Getting started with monitoring

The appliance comes with monitoring available for maximum 200 devices. If an agent-supported device is in inventory, you can enable monitoring for that device. The device can start reporting alerts after the next inventory.

NOTE: Your product license agreement entitles you to manage a specified number of devices that are classified as Managed Computers, Non-Computer Devices, and Monitored Devices. If you enable monitoring on a device, the device is counted once as a Managed Computer and once as a Monitored Device.

Enable monitoring for a device

You can enable monitoring on any eligible device in your inventory, up to 200 devices, as prescribed by your appliance license.

Only Agent-supported operating systems are supported for Monitoring.

The appliance provides two methods for enabling monitoring.

- Enable monitoring for one or more devices from the Devices inventory list
- Enable monitoring for a server from its Device Detail page

When a server is enabled, an icon in the *Status* column on the *Device* page in the *Inventory* section indicates the enabled status, and whether monitoring is active or paused:

- : Device monitoring is enabled and active on this Agent-managed device.
- : Device monitoring is paused on this Agent-managed device.
- : Device monitoring is enabled and active on this Agentless-managed device.
- : Device monitoring is paused on this Agentless-managed device.

Related topics

Disable monitoring for one or more devices

Pause monitoring for a device

Enable monitoring for one or more devices from the Devices inventory list

You can enable monitoring on a server, or on several servers, from the *Devices* inventory list.

1. Go to the *Devices* inventory page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Inventory**, then click **Devices**.
2. Select the check box for each device on which you want to enable monitoring.
3. Select **Choose Action** > **Monitoring** > **Enable**.

    Information about the success or failure of the action appear at the top of the list, and the *Status* for the device changes to display a monitoring icon.

    Potential causes for failure to have monitoring enabled include the device's OS is not supported, or the type of device is not supported, or the monitoring license count has been exceeded.
4. **Optional**: On the left navigation bar, select **Monitoring** > **Devices**, then click the name of a device to make any changes to the monitoring setup for this device on its *Monitoring Detail* page.
    - **Pause or reactivate monitoring. See Pause monitoring for a device.**
    - **Enable monitoring of configuration changes. See Receive alerts when device configurations change.**
    - **Add a monitoring profile or change the profile. See Working with monitoring profiles.**
    - **Add any Maintenance Windows. See Schedule a Maintenance Window during which time alerts are not collected from a device.**

If you have enabled multiple devices, repeat as necessary.

Related topics

Enable monitoring for a server from its Device Detail page

Enable monitoring for a server from its Device Detail page

You can enable monitoring on eligible devices in the inventory, up to a total of 200 devices, as prescribed by your appliance license.

1. Go to the *Device Detail* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Inventory**, then click **Devices**.
    a. Click the name of a device.
2. On the Device Details page, under *Activities* tab, click **Monitoring** to expand the section.

    If a device is not eligible for monitoring because it does not have a supported operating system, the *Monitoring* section appears with the message, **Operating system is currently not supported by Monitoring**.
3. Click **Enable Monitoring** to start monitoring and also display details of the default monitoring setup for the device.

    With monitoring enabled, the *Monitoring* section displays the name of the monitoring profile bound to the device by default. If a Maintenance Window has been defined as a default, its name appears as well. It also displays up to 10 recent alerts, in any.
4. **Optional**: Click **Edit Monitoring Details** to make any changes to the monitoring setup for this device on its *Monitoring Detail* page.
    - **Pause or reactivate monitoring. See Pause monitoring for a device.**
    - **Enable monitoring of configuration changes. See Receive alerts when device configurations change.**
    - **Add a monitoring profile or change the profile. See Working with monitoring profiles.**
    - **Add any Maintenance Windows. See Schedule a Maintenance Window during which time alerts are not collected from a device.**

Related topics

Enable monitoring for a device

Obtaining a new license key to increase server monitoring capacity

To take advantage of expanded monitoring capabilities for up to 200 devices, you must obtain a new license key. You contact the Quest Sales team to obtain the key.

1. Write an email to **license@quest.com** with the current license information (License ID, Key, or Account number). You also mention that you are a current appliance user and want to gain access to the monitoring functionality.

Update the license key information in your appliance once the License Team provides a new key.

Apply a new license key to increase server monitoring capacity

You can increase server monitoring capacity by applying a new license key.

You have obtained your new license key.

1. Go to the appliance *Settings*:
   - **If the Organization component is not enabled on the appliance, log in to the appliance Administrator Console, `https://appliance_hostname/admin`, then select Settings > Control Panel.**
   - **If the Organization component is enabled on the appliance, log in to the appliance System Administration Console, `https://appliance_hostname/system`, or select System in the drop-down list in the top-right corner of the page, then select Settings > Control Panel.**
2. Click **Appliance Updates** to display the *Appliance Updates* page.
3. In the *License Information* section, enter your new license key, then click **Update**.
4. Click **Yes** in the *Confirm* dialog to reboot your system.

The full features are available to you after you sign back in to the appliance following the reboot.

Working with monitoring profiles

Monitoring profiles describe the criteria for creating an alert, by identifying text to search for in the device's log and associating that text with a defined alert level.

The appliance provides a set of default profiles for log monitoring of devices with supported operating systems, and also for SNMP trap devices. Beyond that, you can modify existing monitoring profiles, create your own profiles, and upload profiles created by other users. In addition, you have access to standard Log Enablement Packages (LEPs) to enable application and threshold monitoring.

The available monitoring profiles are listed on the Monitoring *Profiles* page

TIP: To display only the log monitoring profiles, in the top-right corner, click **View By** > **Type** > **Log**. To display the monitoring profiles for SNMP trap devices, click **View By** > **Type** > **SNMP Trap**.

As an example, the default profile for creating alerts for Mac OS X devices indicates that `/var/log/system.log` is the log that the monitoring function scans, looking for text that would trigger an alert. The following table describes the default search text in the *Include Text* field and the associated alert levels.

Text searched for in log	Alert level
`critical`	**Critical**
`error`	**Error**
`fatal`	**Error**
`fail`	**Error**
`appliance monitor alert`	**Error**

Text searched for in log	Alert level
warn	**Warning**
unavailable	**Warning**

You can add other alerts customized to your operational needs.

The default profiles cover the following supported operating systems:

- CentOS
- Debian
- FreeBSD
- macOS
- Oracle Enterprise Linux
- Red Hat Enterprise Linux
- Solaris
- SUSE Linux
- Ubuntu
- Windows
- Raspberry Pi OS

For devices with Linux operating systems, there are several different log paths for MySQL and Apache logs, depending on the version of the OS. See Profile log paths for MySQL and Apache.

For Agentless devices that are monitored using the SNMP trap mechanism, you need to provide trap message formats and expressions to capture the specific trap elements. See Configure SNMP trap messages and alerting criteria.

In the *Log Enablement Packages* list page, Quest publishes a base set of Windows Reliability and Performance Monitor (PerfMon) templates and non-Windows open-source Perl scripts, so that users can extend their monitoring capability and identify system and application performance issues. These templates and scripts are available so that users do not have to create them from scratch. Monitoring on the appliance works without these additional templates and scripts, but the profiles that are created from the templates and scripts are helpful if you want to do performance threshold monitoring.

Edit a profile

You can change, add, or remove alert criteria and log paths for any existing profile.

If you want to use an existing profile as a starting point for creating a profile, see Create a new profile using a default profile as a template.

To identify events that you want raised as alerts, use strings or regular expressions in *Include Text* to specify the appropriate message content. For instance, if you enter the string, Physical memory, an alert is raised for every message with that exact string.

To cover multiple possibilities, you can use a regular expression. For example, if you want alerts for any drive mount point that has drive errors, in the form, “Drive /dev/[any drive mount point] has drive errors”, you can use Drive /dev/[a-z]{1,} has drive errors in *Include Text*. Alerts are raised for any messages that contain "Drive /dev/" followed by any word of any length containing the characters a-z, followed by "has drive errors".

You can exclude specific events from being raised as alerts if you find them unnecessary or distracting. To filter the alerts you do not want to receive, you use *Exclude Text* to indicate the content that identifies an unwanted alert. You can use

Exclude Text to filter whole categories of alerts, or use *Exclude Text* in conjunction with *Include Text* to refine a subset of an alert category. See Examples of Include Text and Exclude Text for monitoring profiles.

1. Go to the *Profiles* list page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Monitoring**, then click **Profiles**.
2. Select the check box for the existing profile that you want to edit, and select **Choose Action** > **Edit** to display the *Profile Detail* page.
3. **Optional**: Change or modify the *Name* and *Description* of the profile to indicate the edits.

    NOTE: If you are editing one of the default profiles, you cannot make any change to the *Add Automatically To* field.

4. Make changes to the *Criteria* settings, according to your needs.
    - **Change *Include Filter* (SNMP traps only) or *Include Text* (all other monitoring profiles).**
        1. On the line with the include search text (or filter for SNMP traps) you want to change, click the **Edit** button: .
        2. Type the new search text or filter.
    - **Optional. Change *Exclude Filter* (SNMP traps only) or *Exclude Text* (all other monitoring profiles).**
        1. On the line with the text (or filter for SNMP traps) you want to change in order to exclude certain alerts, click the **Edit** button: .
        2. Type the new exclude text or filter.
    - **If the provided search text is case sensitive, select Yes in the *Case-sensitive* drop-down list.**
    - **SNMP traps only. Create a Service Desk ticket automatically each time the appliance receives a specific SNMP alert.**
        # On the line containing an SNMP include and exclude filter (as configured), in the *Create Ticket* column, click **Select Queue**, and select a ticket queue that you want to use to create a Service Desk ticket. The appliance will create a Service Desk ticket in the specified ticket queue when it receives an alert resulting from the specific include filter. The device associated with the alert will appear selected in the Service Desk ticket. The name and summary of the event that triggered the SNMP alert will appear in the ticket details. For more information about Service Desk tickets, see Managing Service Desk tickets, processes, and reports.
    - **Change the alert *Level*.**
        1. On the line with the alert level you want to change, click the **Edit** button: .
        2. In the *Level* drop-down list, select the level from among the five choices: **Critical**, **Error**, **Warning**, **Info**, and **Recovered**.
    - **Add an alert Criteria.**
        1. On the *Criteria* category header, click the **Add** button: .
        2. Set the level, include text, exclude text (optional), and case sensitivity.
5. Click **Save** at the bottom of the page.

NOTE: You can return a default profile to factory settings for its operating system by using the **Reset to Factory Settings** button at the bottom of the page.

Related topics

Filter alerts using the Include Text and Exclude Text capability from the Profile Details page

Examples of Include Text and Exclude Text for monitoring profiles

Configure SNMP trap messages and alerting criteria

You can configure SNMP trap messages and the alerting criteria using the Profiles page.

- Enable SNMP trap monitoring on the appliance. For more information, see Configure security settings for the appliance
- Enable monitoring on your SNMP devices. For more information, see Enable monitoring for one or more devices

SNMP (Simple Network Management Protocol) is a protocol for monitoring managed devices on a network. This protocol is supported by Dell Open Manage and many third-party products. When you enable this feature on the appliance, and the related devices are also enabled for monitoring, the appliance can receive SNMP traps from the monitored Agentless devices using SNMP connections, such as printers, projectors, and routers.

SNMP traps are messages initiated by network devices and sent to the trap receiver on the appliance. For example, a router can send a message when its power supply fails. Or, a printer initiates a message when it runs out of paper. The appliance receives these traps and generates alerts when certain pre-defined thresholds are reached.

You can configure SNMP trap messages and the alerting criteria using the *Profile Detail* page.

You can include or exclude certain events from being detected, as needed.

1. Go to the *Profiles* list page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Monitoring**, then click **Profiles**.
2. Complete one of the following steps.
    # To create a new SNMP trap profile, select **Choose Action > New> SNMP Trap Profile**.
    # To edit an existing SNMP trap profile, select it in the list, and **Choose Action** > **Edit**.
    # To duplicate an existing SNMP trap profile, select it in the list, and **Choose Action** > **Duplicate and Edit**.

    The *Profile Detail* page appears.
3. **Optional**: Change or modify the *Name* and *Description* of the profile to indicate the edits.

    NOTE: If you are editing one of the default profiles, you cannot make any change to the *Add Automatically To* field.
4. Make changes to the *Trap Message Formats* settings, according to your needs.

    For example: `%Td (%Tn => %To) %Vz`

    You can use the following elements in your SNMP trap message:

Element	Description
`%Aa`	The agent address.
`%Ah`	The agent host name.
`%d`	Local day.
`%m`	Local month.
`%y`	Local year.

Element	Description
%h	Local hour.
%i	Local minute.
%s	Local second.
%u	Unix timestamp.
%Td	Trap description.
%Tm	Trap MIB (management information base).
%Tn	Trap name.
%To	Trap OID (object ID).
%Tt	Trap type (0-5 Generic; 6 - Enterprise).
%Tv	Trap version (Inform, Trap v1, v2, or v3).
%Vd**#**	Variable binding description (where '#' is a number representing the element's position in the sequence).
%Vn**#**	Variable binding name (where '#' is a number representing the element's position in the sequence).
%Vo**#**	Variable binding OID (where '#' is a number representing the element's position in the sequence).
%Vt**#**	Variable binding type (where '#' is a number representing the element's position in the sequence).
%Vv**#**	Variable binding value (where '#' is a number representing the element's position in the sequence).
%Vz	Shows all variable bindings (`Name: Value`, `Name: Value`, `Name: Value`). If a Name is missing (due to a missing MIB file), the OID is displayed instead.

5. Specify one or more alert levels, as needed.

   The following alert levels are available: Critical, Error, Warning, Info, and Recovered.

   - To add an alert level, under *Criteria*, click ✚ to add a new alert level.
   - To edit an existing alert level, in the row containing the alart level, click ✎.

6. For each level, specify its Include and/or Exclude expressions, and also indicate if the expressions are case-sensitive. These expressions allow you to include or exclude certain events from being detected.

   The syntax for Include and Exclude expressions is as follows:

   <Field_Type> {TRAP_OID|TRAP_NAME|TRAP_DESCRIPTION|TRAP_TYPE|TRAP_MIB|VARBIND} {=|!=|>|<|>=|<=} <Field_Value> [<AND|OR> <Condition_A>] [<AND|OR> <Condition_B>] . . .

For example:

- `TRAP_OID = ".1.3.6.1.4.1.8072.2.3.2.1"`: An alert is generated when the trap OID contains ".1.3.6.1.4.1.8072.2.3.2.1".
- `TRAP_NAME = "acctngFileFull" AND VARBIND = "acctngFileName|ABC"`: An alert is generated when the trap name contains "acctngFileFull" and if one of the trap's variable bindings is "acctngFileName" with a value of "ABC".

7. Click **Save** at the bottom of the page.

NOTE: You can return a default profile to factory settings for its operating system by using the **Reset to Factory Settings** button at the bottom of the page.

Create a new profile using a default profile as a template

You can copy a default or existing monitoring profile and edit the copy to create a new profile.

You are not limited to one profile for each device. You can create additional profiles that generate different alerts and bind the profiles to devices that already have one or more profiles associated with them.

1. Go to the *Profiles* list page:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Monitoring**, then click **Profiles**.
2. Select the check box for the existing profile that you want to start with as a template, and select **Choose Action** > **Duplicate and Edit** to display the *Profile Detail* page.
3. Rename the profile and modify its description.
4. **Optional**: Change or modify the *Name* and *Description* of the profile to indicate the edits.

   NOTE: If you are editing one of the default profiles, you cannot make any change to the *Add Automatically To* field.
5. For the log path, use the path appropriate for the operating system or application.

   The path can be the basic one for the operating system, as shown in the table.

Operating system	Log path
CentOS	`/var/log/messages`
Debian	`/var/log/syslog`
Fedora	`/var/log/messages`
FreeBSD	`/var/log/messages`
macOS	`/var/log/system.log`
openSUSE	`/var/log/messages`
Oracle Enterprise Linux	`/var/log/messages`

Operating system	Log path
Red Hat Enterprise Linux	`/var/log/messages`
Solaris	`/var/adm/messages`
SUSE Enterprise Linux	`/var/log/messages`
Ubuntu	`/var/log/syslog`
Windows	`application` for Windows Application **NOTE:** You must use the *Full Name* of the event log, as it appears in the properties for that log. To ensure you have the correct Full Name, open the *Event Viewer*. Expand *Windows Logs*, right-click the event log and select **Properties**. Use the version of the Full Name that appears in the field in the *Log Properties* dialog. `Microsoft-Windows-TaskScheduler/Operational` for Windows Task Scheduler Operational
Raspberry Pi OS	`/var/log/syslog`

Alternatively, you can enter a path that defines a log that contains data beyond the basic event logs. For instance, if you had an application on SUSE that sends its data to a specific log such as `/var/log/`**<myapplog>**, you can use that path in a new profile, and define the search text and alert level as described in this procedure.

For devices with Linux operating systems, there are a number of different log paths for MySQL and Apache logs, depending on the version of the OS. See Profile log paths for MySQL and Apache.

NOTE: Only one log path can be defined in a profile. You must create multiple profiles for multiple logs.

6. Make changes to the *Criteria* settings, according to your needs.

- **Change *Include Text*.**
  1. On the line with the include search text you want to change, click the **Edit** button: .
  2. Type the new search text, and, if necessary, select **Yes** in the *Case-sensitive* drop-down list.
  3. Click **Save** at the right of the row.
- **Optional: Change *Exclude Text*.**
  1. On the line with the text you want to change in order to exclude certain alerts, click the **Edit** button: .
  2. Type the new exclude text, and, if necessary, select **Yes** in the *Case-sensitive* drop-down list.
  3. Click **Save** at the right of the row.
- **Change alert *Level*.**
  1. On the line with the alert level you want to change, click the **Edit** button: .
  2. In the *Level* drop-down list, select the level from among the five choices: **Critical**, **Error**, **Warning**, **Info**, and **Recovered**.
  3. Click **Save** at the right of the row.
- **Add an alert.**

1. On the *Criteria* category header, click the **Add** button: +.
2. Set the level, search text, and case sensitivity, and click **Save** at the right of the row
3. Repeat for as many alerts as you want to add.
4. **Optional**: Reorder the new alert criteria using the **Drag** button: ☰.

7. Click **Save** at the bottom of the page.

The profile is available to be assigned to a device on that device's *Monitoring Detail* page.

Profile log paths for MySQL and Apache

For devices with Linux operating systems, there are a number of different log paths for MySQL and Apache logs, depending on the version of the OS.

NOTE: Only one log path can be defined in a profile. You must create multiple profiles for multiple logs.

Upload a profile that was created by another user

If another user has made a custom profile available for use by others, you can upload it into your appliance.

You have access to an XML profile file created by another user.

1. Go to the *Profiles* list page:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Monitoring**, then click **Profiles**.
2. Select **Choose Action** > **Upload Profiles** to display the *Upload Profiles* dialog.
3. Click **Choose File** to navigate to the profile you want to upload, choose it, then click **Upload**.

   You can select more than one profile.

The profile or profiles appear at the bottom of the *Profiles* list.

You can edit the new profile, if needed. See Edit a profile.

Download a profile so that it can be used by others

You can download a custom profile to make it available for use by other users.

1. Go to the *Profiles* list page:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Monitoring**, then click **Profiles**.
2. Select the check box for the profile or profiles that you want to download, and select **Choose Action** > **Download Profiles** to send the profile or profiles to your *Downloads* folder.

   The profile XML file name is derived from the profile name, as seen on the Profile Detail page, with a UNIX timestamp appended.

Distribute the profile.

Bind an additional profile to a device

When you enable monitoring on a device, the appliance assigns, or binds, to the device the default profile and the default log path that is appropriate for the device's operating system. You can add other profiles as needed, from custom profiles you create.

1. Go to the *Monitoring Detail* page:
    a. On the left navigation bar, click **Monitoring**, then click **Devices**.
    b. Click the name of a device to display the *Monitoring Detail* page.
2. Click in the *Profiles* field to see a drop-down list of defined profiles, and select the one you want to apply.
3. Click **Save**.

Define nonstandard log date format

For any given operating system, the appliance knows and uses the standard format for log date and time when scanning the log file. However, if you use an uncommon format in your logs, you must define that format so that monitoring can properly parse the log.

NOTE: In most cases, this field should be left blank.

NOTE: Log Date Format is not pertinent to Windows event logs.

1. Go to the *Profiles* list page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Monitoring**, then click **Profiles**.
2. Select the check box for the existing profile that you want to edit, and select **Choose Action** > **Edit** to display the *Profile Detail* page.
3. Type the nonstandard log date format in to *Log Date Format*.

    The supported format characters, and examples, can be viewed if you click ⓘ next to *Log Date Format*.
4. Click **Save** at the bottom of the page.

Configuring application and threshold monitoring with Log Enablement Packages

Performance threshold monitoring and monitoring for applications such as Exchange, Internet Information Services (IIS), and so on, require packages, called Log Enablement Packages (LEPs), that you can access from the *Log Enablement Packages* list page.

In the *Log Enablement Packages* list page, Quest publishes a base set of Windows Reliability and Performance Monitor (PerfMon) templates and non-Windows open-source Perl scripts, so that users can extend their monitoring capability and identify system and application performance issues. These templates and scripts are available so that users do not have to create them from scratch. Monitoring on the appliance works without these additional templates and scripts, but the profiles that are created from the templates and scripts are helpful if you want to do performance threshold monitoring.

Windows PerfMon template

In the appliance, a default Windows OS and Application LEP Profile has been predefined in the appliance that contains the specific event log and generic criteria that Microsoft uses for PerfMon triggered events. The base PerfMon templates

available for Microsoft Server 2008 through LEPs on the Log Enablement Packages list page are for system (CPU, memory, disk), Exchange, SQL, IIS, Active Directory, and Hyper-V.

Non-Windows Perl scripts

Each package is an open-source Perl script that runs periodically using the built-in operating system scheduler: cron, fcron, and so on. When the Perl script is executed, the script runs a series of commands to determine the use of CPU, memory, and local volumes. An alert is written to the system log (syslog) file if the utilization exceeds the threshold defined in the package. Because the scripts are configured to log to syslog and contain a prefix message for each event, the appliance has predefined the criteria in the syslog defaults for all non-Windows profiles for ease of configuration.

Install one or more LEPs on monitored devices

You can install Log Enablement Packages on Windows devices and non-Windows devices directly from the appliance.

1. Go to the *Log Enablement Packages* list page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Monitoring**, then click **Log Enablement Packages**.
2. Select the check box for the package or packages that you want to install on devices, and select **Choose Action** > **Add to Devices** to display the *Log Enablement Packages Install* page.

    If you are choosing multiple packages, you can choose both Windows and non-Windows packages to install. In this case, the *Log Enablement Packages Install* page displays a separate section for Windows packages and a separate section for non-Windows packages. If all the packages you select are for one type, then only the section for that particular type appears.

3. Select the devices to which to add the package or packages.
    a. Click in the *Devices* text box to display a list of devices within inventory that are compatible with the packages listed in *Selected Packages* to the right.
    b. Select the device or devices you want from the list.
4. **Optional**: For Windows packages, clear the check box for *Add Windows OS and Application LEP Profile* if that profile is already bound to the device or devices and you do not want to reinstall it.
5. Determine how you want the installation to go if one of the packages is already installed on a device.
    - **Leave *Replace it* selected if you want the current package reinstalled over an existing version.**
    - **Select *Skip it* if you want to retain the package that might be currently installed on the device. For instance, you might have made edits to the package earlier and do not want to lose those changes.**
6. Click **Install**.
7. **Optional**: View the progress of the installation.
    a. Click **Devices** in the **Monitoring** section of the left navigation bar, and select the name of the monitored device to display its *Monitoring Detail* page.

        The LEP Installation Log section appears at the bottom of the page, displaying a summary of the installation process for this particular device.

    b. **Optional**: Click **See all LEP Installation Logs for this device** to see more detail.

Edit the monitoring Log Enablement Package (LEP) for a Windows Server 2008 or higher device

You can add, remove, and configure performance counters in a monitoring LEP installed on a server.

The Log Enablement Package has been installed on the device. See Install one or more LEPs on monitored devices.

1. On the device you want to monitor, start the Performance Monitor, expand the **Data Collector Set** folder, then expand the **User Defined** folder.
2. Select the LEP-defined Data Collector Set.
3. **Optional**: If the package is running, right-click the set name and select **Stop**.
4. In the right pane, right-click the DataCollector and select **Properties** to display the *Properties* dialog.
5. Use the tabs on the *Properties* dialog to edit the package:

Option	Description
Alerts	The **Alerts** tab enables you to edit the threshold attribute and interval attribute of a performance counter. You can also add and remove counters using this tab. To configure the performance counter: 1. Select the counter in *Performance counters*. 2. Edit the alert trigger using the *Alert when* drop-down list and the *Limit* field. 3. Edit the collection interval using the *Sample interval* and *Units* drop-down menus. 4. Click **OK** to save the changes. To add a performance counter to this LEP: 1. Click **Add** to display the add counters dialog. Performance counters for applications installed locally appear in *Available counters*. You can also select objects and counters from a remote system if you use the list in *Select counters from computer* or use **Browse**. 2. In *Available counters*, select the counter or counters you want to add, and click **Add >>**. 3. Click **OK** to return to the *Properties* dialog. To remove a performance counter from this LEP: 1. Select the counter in *Performance counters*. 2. Click **Remove**. 3. Click **OK** to save the changes.
Alert Action	The objective of the package is to have events logged in the event log so that the monitoring capability of the appliance can pick up an alert, so the check box for *Log an entry in the application event log* should remain selected.
Alert Task	If you want to set a task to run when the alert is triggered, you define that task on this tab.

6. Click **OK** at the bottom of the *Properties* dialog to return to Performance Monitor.
7. In the **User Defined** folder, right-click the package and select **Start** to start the monitoring.

Managing monitoring for devices

After a device has monitoring enabled, you can configure how and when monitoring takes place, and manage monitoring on a per-device basis.

Pause monitoring for a device

You can pause monitoring if you want to prevent the monitoring function from producing alerts while you work on, or make changes to, a device.

NOTE: If you want to pause monitoring on a set schedule to accommodate regular maintenance tasks, you can set Maintenance Window schedules. See Schedule a Maintenance Window during which time alerts are not collected from a device.

If you want to pause or resume multiple devices at the same time, see Pause or resume monitoring for multiple devices.

1. Go to the *Monitoring Detail* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Monitoring**, then click **Devices**.
    c. Click the device in the *Device* column to display its *Monitoring Detail* page.
2. Select the option button for *Paused* and click **Save**.

An icon in the *Status* column on the *Device* page in the *Inventory* section indicates the paused status:

- : Device monitoring is paused on this Agent-managed device.
- : Device monitoring is paused on this Agentless-managed device.

Pause or resume monitoring for multiple devices

You can pause monitoring for multiple devices at the same time. You can resume monitoring for multiple devices as well.

1. Go to the *Monitored Devices* list page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Monitoring**, then click **Devices**.
2. Select the check boxes for all the devices you want to pause or resume.
3. Select **Choose Action** > **Pause Monitoring** or **Resume Monitoring**.

    The entry in the *Monitoring* column for the devices changes to indicate the new state, *Paused* or *Active*.

Set the polling interval and any automatic dismissal or deletion of alerts

You can configure some general monitoring settings for how often the appliance polls the logs for alerts. In addition, you can configure the appliance to dismiss alerts automatically after a number of days you set, and delete alerts too.

Dismissing an alert removes it from view on the *Alerts* list page and the dashboard widgets. Deleting an alert removes it from the database. You can recover dismissed alerts, but not deleted alerts.

1. Go to the *Monitoring Settings* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Settings**, then click **Monitoring Settings**.
2. Set the polling interval in minutes.

    The minimum interval is 10 minutes.
3. **Optional**: Set the appliance to dismiss alerts after a prescribed number of days.
    a. Select *Dismiss alerts automatically*.
    b. Type the value for the number of days.
4. **Optional**: Set the appliance to delete alerts after a prescribed number of days.
    a. Select *Delete alerts automatically*.
    b. Type the value for the number of days.
5. Click **Save**.

Related topics

Dismiss an alert

Delete alerts

Retrieve and review alerts that have been dismissed from the alerts list

Disable ping probe

Ping probes are enabled by default when you enable monitoring for any device. However, in certain instances ping probes can engender an alert storm, so the appliance makes it possible to disable ping probes.

Ping sends Internet Control Message Protocol (ICMP) echo request packets to its target. Some firewalls block ICMP packets, so it is possible, because of the frequency of the ping probes, to have an enormous number of alerts generated from the probes being rejected. In these cases, disabling ping probes unclutters the monitoring results.

1. Go to the *Monitoring Settings* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Settings**, then click **Monitoring Settings** on the *Control Panel*.
2. Clear *Enable ping probe*.
3. Click **Save**.

Receive alerts when device configurations change

You can set monitoring to create an alert when the configuration of a monitored device is changed.

When you enable this feature, each time a device configuration change is detected, an alert is generated. You can specify which types of changes you want to detect for the device assets, by selecting them in the *Device* dialog box, accessible from the *Asset History Configuration* page.

Examples of configuration change include the addition of a disk, a new logical drive, an increase or decrease of memory, a partition change, and so on. For complete information about the *Asset History Configuration* page, and how to select configuration changes, see Configure asset history subscriptions.

1. Go to the *Monitoring Detail* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Monitoring**, then click **Devices**.
    c. Click the name of a device.
2. Select the *Enable Configuration Change Alert* check box.
3. Click **Save**.

Schedule a Maintenance Window during which time alerts are not collected from a device

Using maintenance windows enables you to set aside certain time slots for performing server maintenance tasks without the monitoring function producing excessive alerts that might flood the system.

You are not limited to using one Maintenance Window for each monitored device. You can create a library of Maintenance Windows, and apply combinations of them to monitored devices depending on your needs.

1. Go to the *Maintenance Window Detail* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Monitoring**, then click **Maintenance Windows**.
    c. Select **Choose Action** > **New**.
2. Provide the following information:

Option	Description
Name	A name that identifies the Maintenance Window. The name appears on the *Maintenance Windows* list.

Option	Description
Description	Information that further identifies the purpose and subjects of the window.
Add Automatically To	• **None**: This Maintenance Window is not automatically added to a device when monitor is enabled on that device. • **All**: This Maintenance Window is automatically added to a device when monitor is enabled on that device.

3. In the *Schedule* section, specify the schedule settings:

Option	Description
Every day/specific day from HH:MM to HH:MM	Start the window daily at a specified time and for a specific duration, or start on a designated day of the week at a specified time.
Run on the nth of every month/specific month from HH:MM to HH:MM	Run on the same day every month, or a specific month, at the specified time and duration.

NOTE: The schedule uses the 24-hour clock.

4. Click **Save**.
5. Apply the Maintenance Window to a monitored device on its *Monitoring Detail* page:
   a. On the left navigation bar, click **Monitoring**, then click **Devices**.
   b. Click the name of a device to display the *Monitoring Detail* page.
   c. Click in the *Maintenance Windows* field to view a drop-down list of defined Maintenance Windows, and select the one you want to apply.
6. Click **Save**.

Create and assign monitoring-specific roles

You can create user roles that regulate the ability to work with alerts and profiles.

For instance, you can create a role for a staff member who can react to alerts, and create Service Desk tickets from them, but who cannot add profiles to devices or set Maintenance Windows.

If the Organization component is enabled on your appliance, the permissions available to User Roles depends on the Organization Role assigned to the organization. See Managing Organization Roles and User Roles.

NOTE: You cannot edit the predefined Roles: Administrator, No Access, Read Only Administrator, and User.

1. Go to the *Role Detail* page:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Settings**, then click **Roles**.
   c. Select **Choose Action** > **New** to display the *Role Detail* page.
2. In the *Name* field, provide a name, such as Monitoring Alert Attendant.
3. In the *Description* field, provide a brief description of the role, such as Used for support staff with responsibility for responding to alerts.

This description appears on the *Roles* list along with the name.

4. Click the **Monitoring** link below Administrator Console *Permissions* to display the permissions settings for server monitoring.
5. Set permissions according to the level of access you want to assign to the role:
   - **All Write**
   - **All Read**
   - **All Hide**
   - **Custom:**

You can combine WRITE, READ, or HIDE permission for the following monitoring pages

Category	Page (include Detail page)	Permissions affect these actions
Monitoring	**Devices**	• Acknowledge (Dismiss) alerts • Enable monitoring of configuration changes • Pause or resume monitoring • Add or remove profiles • Add or remove Maintenance Windows • Disable monitoring • Export alerts
	Alerts	• Acknowledge (Dismiss) alerts • Create Service Desk ticket • Set notifications • Retrieve alerts • Delete alerts • Export alerts
	Profiles	• Create profiles • Edit profiles • Delete profiles • Remove profiles from all devices • Upload and download profiles
	Maintenance Windows	• Create Maintenance Windows • Edit Maintenance Windows • Delete Maintenance Windows • Remove Maintenance Windows from all devices • Export Maintenance Windows
	Monitoring LEP	• Add to devices • Export LEPs

6. If applicable, assign the role the ability to enable monitoring on a device.

   A user enables monitoring on the device's *Device Detail* page, so permission has to be set in the *Inventory* section.

   a. Click the **Inventory** link below Administrator Console *Permissions* to display the permissions settings for inventory.
   b. Set *Devices* to **WRITE**.
7. Click **Save**.
8. Assign the role to a user.

a. On the left navigation bar, click **Settings**, then click **Users**.
b. Select the check box for the user to whom you want to assign the role.
c. Select **Choose Action** > **Apply Role** > **Name of role.**

Disable monitoring for one or more devices

When you no longer want to monitor a device, you can disable the capability, after which the device no longer counts against your license limit.

You can disable monitoring for a device in three locations. Two of the locations you use for individual devices and one location you use for a group of devices.

- Disable monitoring from a device's *Device Detail* page:
    1. On the left navigation bar, click **Inventory**, then click **Devices**.
    2. Click the name of a device.
    3. Click the *Activities* tab to expand the **Monitoring** section.
    4. Click **Disable Monitoring**.
    5. Confirm the action on the confirmation dialog.
- Disable monitoring from a device's *Monitoring Detail* page:
    1. On the left navigation bar, click **Monitoring**, then click **Devices**.
    2. Click the name of a device.
    3. On the **Monitoring Detail** page, click **Disable**.
    4. Confirm the action on the confirmation dialog.
- Disable monitoring for multiple devices from the *Devices* list.
    1. On the left navigation bar, click **Monitoring**, then click **Devices**.
    2. Select the check boxes preceding all the devices on which you want to disable monitoring.
    3. Select **Choose Action** > **Disable Monitoring**.
    4. Confirm the action on the confirmation dialog.

Disabling monitoring does not delete the device's alerts. On the *Monitoring Alerts* list page, for an alert relating to a disabled device, the *Device* column entry contains **Device deleted or no longer monitored**. If you re-enable monitoring for this device, however, the appliance treats the device as a newly monitored device. In this case, the earlier alerts from the device still appear as **Device deleted or no longer monitored**.

For information on deleting alerts, see Delete alerts.

Enable monitoring for one or more devices

When you want to monitor a device, you can start monitoring it. Any devices that are enabled for monitoring count against your license limit.

IMPORTANT: Enabling monitoring on SNMP-managed devices does not count against the license limit.

You can enable monitoring for a device in three locations. Two of the locations you use for individual devices and one location you use for a group of devices.

- Enable monitoring from a device's *Device Detail* page:
    1. On the left navigation bar, click **Inventory**, then click **Device**s.
    2. Click the name of a device.
    3. Click the *Activities* tab to expand the **Monitoring** section.

4. Click **Enable Monitoring**.
5. Confirm the action on the confirmation dialog.

- Enable monitoring for multiple devices from the *Devices* list.
  1. On the left navigation bar, click **Inventory**, then click **Device**s.
  2. Select the check boxes preceding all the devices on which you want to enable monitoring.
  3. Select **Choose Action** > **Enable Monitoring**.
  4. Confirm the action on the confirmation dialog.

Enabling monitoring for a device allows the device to generate alerts when certain thresholds are met. If you re-enable monitoring for this device, the appliance treats the device as a newly monitored device. In this case, the previous device alerts appear as **Device deleted or no longer monitored**. For information on deleting alerts, see Delete alerts.

Working with alerts

When server monitoring produces an alert, you have various responses available to you.

You can use the alert as a basis for a Service Desk ticket or an automated email notification. After dealing with the alert according to your procedures, you can dismiss it, or delete it entirely.

If you have added the monitoring widgets to your Dashboard, you can see at a glance the current top alerts, with links to the *Monitoring Alerts* list page and the *Monitored Devices* list page.

The following icons indicate alert level:

- : **Stopped**
- : **Error**
- : **Warning**
- : **Information**
- : **Done**

Related topic

About Dashboard widgets

Add notification schedules from the Monitoring Alerts list page

You can add monitoring alert notification schedules for devices, alert levels, messages, and other alert information. These schedules enable the appliance to notify administrators through email or push notification to a KACE GO mobile device when specified criteria are met.

You have configured your email notification settings.

1. Go to the *Monitoring Alerts* list page in one of the following ways:
   - **If you have the *Monitoring Alerts* widget installed on your open *Dashboard*, click Monitoring Alerts.**
   - **In the left navigation bar, select Monitoring > Alerts.**
2. Select the check box for the row that contains the alert message, then click **Notification**, to the right above the alerts list, to display the *Notification* panel.
3. Select notification criteria. For example, to send a notification when information alerts are generated, specify the following:

```
Level | is | Information
```

4. Provide the following information below the notification criteria:

Field	Description
Title	The information that you want to appear in the *Subject* line of the email.
Email Recipient	The email address or addresses of intended recipients. Email addresses must be fully qualified email addresses. To send email to multiple addresses, use commas to separate each address, or use email distribution lists.
Frequency	The interval at which the appliance runs the query to compare the selected criteria with items in inventory. If criteria are met, the notification is sent.

5. **Optional**: Select the check box for *Send to KACE GO* if you want the alert to be pushed to a mobile device that has the KACE GO app.

   Mobile device access must be enabled for this option to be available. See Configuring Mobile Device Access.

6. **Optional**: To verify the criteria, click **Test**.

   The list is refreshed to show items that match the specified criteria. Notifications are not sent during the test.

7. Click **Save**.

The notification is created and it appears on the *Notification Schedule* page. For information about scheduling the frequency of the notification, see Edit notification schedules.

Related topics

About notifications

Scheduling notifications

Create a Service Desk ticket from an alert

You can create a Service Desk ticket from a server monitoring alert, with information from the alert automatically populating fields in the ticket form.

1. Go to the *Monitoring Alerts* list in one of the following ways:
   - **If you have the *Monitoring Alerts* widget installed on your open *Dashboard*, click Monitoring Alerts.**
   - **In the left navigation bar, select Monitoring > Alerts.**
2. Select the check box for the row that contains the alert message, then select **Choose Action > New Ticket**.
   # If you want to create a ticket based on a queue, if there are multiple ticket queues in the organization, select a queue from the **Ticket** drop-down list.
   # If you want to create a ticket based on a process template, select the process from the **Process** drop-down list.

   The *Title*, *Summary*, *Submitter*, and *Device* fields contain information from the alert.
3. **Optional**: Change the *Title* and *Summary* to conform to your corporate procedures.
4. Provide the rest of the information needed to complete the form, then click **Save** to save the ticket and leave the *Ticket Detail* page, or **Apply Changes** to save the ticket and continue editing it.

Option	Description
Title	(Required) A brief description of the issue. You can replace the monitoring-provided title with one of your choosing.

Option	Description
Summary	A more detailed description of the issue. This field includes a full range of text editing options for formatting your content, such as buttons for bold text, hyperlinks, lists, or text color. For example: • To apply bold text to a text string, select it in the editor, and click B. • To add images, click , and provide the URL to the image file. # Any images you include this way will not be added as file attachments to the ticket. # Deleting an image from the text field will permanently remove it as the image in this field is not stored as an attachment. • To add external links, click . • To embed externally hosted videos, click .
Submitter	The login name of the user submitting the ticket. The submitter can be changed by selecting a different login name in the drop-down list. Click to view the submitter contact information.
Asset	The asset that the information in the ticket is about. Select an asset in the drop-down list. Click to view the asset details.
Filter on submitter assigned assets	Filter the asset list based on the assets that are assigned to the submitter.
Device	The device that the information in the ticket is about. Monitoring provides this information. Click to view the device details.
Filter on submitter assigned devices	Filter the asset list based on the devices that are assigned to the submitter.
Impact	The number of people that are inconvenienced or cannot work.
Category	A classification of the issue.
Status	The current state of the ticket. This field does not appear if you are creating or editing a ticket from a process template.
Priority	The importance of priority of the ticket.
Owner	The user responsible for managing the ticket through its lifecycle.
Due	Date and time the ticket is scheduled to be completed. If Service Level Agreements are not enabled, the due date is set to None, by default. If Service Level Agreements are enabled, the due date is automatically calculated according to the SLA settings. The due date is calculated based on the priority set when the ticket is submitted. If the priority is changed after the ticket is initially submitted, the due date will be recalculated according to the new priority, but based on the original submitted date and time. If the SLA resolution time configuration

Option	Description
	is changed, it is only applicable on new tickets. Old tickets are not affected. See Configuring Service Level Agreements. Select **Manual Date** to manually set the due date and time. In this case, if Service Level Agreements are enabled, the due date and time is calculated and displayed as an option, but not selected.
CC List	A list of users who receive a notification email when a ticket event occurs. The CC List is emailed based on the ticket event and **Ticket CC** being configured for the queue **Email on Events** configuration.
Resolution	The resolution of the issue associated with the ticket. This field includes a full range of text editing options for formatting your content, such as buttons for bold text, hyperlinks, lists, or text color. For example: • To apply bold text to a text string, select it in the editor, and click B. • To add images, click, and provide the URL to the image file. # Any images you include this way will not be added as file attachments to the ticket. # Deleting an image from the text field will permanently remove it as the image in this field is not stored as an attachment. • To add external links, click. • To embed externally hosted videos, click.
Related Ticket Information	This section does not appear if you are creating a ticket from a process template.
Add Ticket	Click to add an additional ticket to this ticket's related information.
Referrers	The **Referrer** is a read-only field that holds a ticket reference to any ticket that references this ticket by way of the **See also** section.
Merged Tickets	This section allows you to edit the list of tickets merged with this ticket, as applicable. Any tickets that you want to merge must belong to the same queue. When you merge tickets using the *Ticket Detail* page, the open ticket becomes the primary ticket. All other merged tickets are archived when you merge them. For more details, see Merging tickets. To add a merged ticket, click **Add Tickets to Merge/Edit Merged Tickets**, and select a ticket from the list that appears.
Process Information	This section only appears if you are creating a ticket from a process template. All of the settings appearing in this section are read-only. For complete information about creating and configuring process templates, see Add, edit, and enable process templates
Process	The name of the process template associated with this ticket.
Process Type	The type of the process.

Option	Description
Process Status	The status of the workflow associated with this process template. For example, *Pending Approval*.
Parent	The name of the parent ticket, as defined in the process template associated with this ticket.
Process Approvals	A list of users that are assigned as approvers for this ticket, if applicable. The approvers are listed in stages, as defined in the process template. Each stage can have one or more approvers, as needed. The settings related to each approver and stage are also listed in this section, such as approval timeouts and notifications. When you create a process ticket, the timeout period starts for the first approver. When that user approves the ticket, the timeout starts for the next one, and so on.
Process Activities	A list of process activities, each representing a child ticket, and listed in stages, as defined in the process template. Multiple tickets can be assigned to the same stage, if needed. For example, if the first stage is to obtain equipment and supplies for a new-hire, you can have several separate child tickets for ordering devices, office equipment, and supplies, all assigned to stage 1. When you create a process ticket, all child tickets assigned to stage 1 are created automatically. Stage 2 tickets are created when all stage 1 tickets are closed, stage 3 tickets are created when all stage 2 tickets are closed, and so on.
Add Ticket	Click to add an additional ticket to this ticket's related information.
Referrers	The **Referrer** is a read-only field that holds a ticket reference to any ticket that references this ticket by way of the **See also** section.
Comments	Comments that you want to add to the ticket. You can also add file attachments, screenshots, provide automatic responses or Knowledge Base article contents as ticket comments. For more information see: • Add comments to tickets • Add or delete screen shots and attachments from Service Desk tickets If you want to add an automatic response as a resolution to this ticket, click **Predefined Response** and select a response template. The selected response template appears in the **Resolution** field. You can add multiple response templates as resolution entries. They appear in the order you selected them. **TIP:** To create or edit a response template, save your changes and click **Manage**. This will take you to the *Response Templates* page. For more information about response templates, see View and edit response templates.
Knowledge Base Article	Look up a Knowledge Base article and append its contents to the ticket comments. For more information about Knowledge Base articles, see Managing Knowledge Base articles.

Related topics

Managing Service Desk tickets, processes, and reports

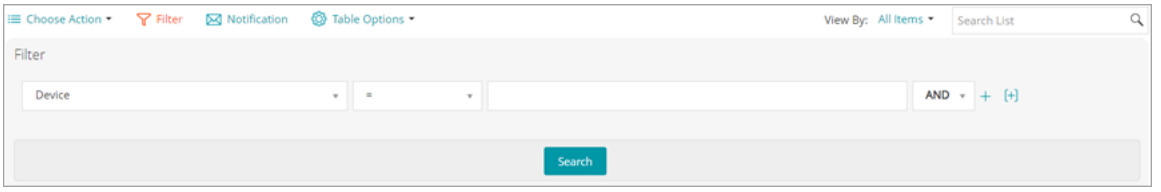
Search for alerts using Filter criteria

Advanced Page-level Search enables you to search for information on the current page using various combinations of criteria.

This example shows how to use Filter to find critical alerts related to a connection issue.

1. Go to the *Monitoring Alerts* list page in one of the following ways:
   - **If you have the *Monitoring Alerts* widget installed on your open *Dashboard*, click Monitoring Alerts.**
   - **In the left navigation bar, select Monitoring > Alerts.**
2. Click **Filter** on the right, above the *Monitoring Alerts* list.

   The *Filter* panel appears.



3. Specify the criteria required to find alert level:

   `Montoring Alert Information: Level | is | Critical`
4. With **AND** selected in the operator drop-down list, click + to add a new line, then specify the criteria required to find alerts that contain **Unable to connect** in the message:

   `Montoring Alert Information: Message | contains | unable to connect`
5. Click **Search**.

The list is refreshed to show devices that match the specified criteria.

Filtering alerts using the Include Text and Exclude Text capability

If you are receiving too many alerts of a certain type, or if you want to track a particular alert, you can filter alerts based on the message text and severity level.

You can exclude specific events from being raised as alerts if you find them unnecessary or distracting. To filter the alerts you do not want to receive, you use *Exclude Text* to indicate the content that identifies an unwanted alert. Use *Exclude Text* in conjunction with *Include Text* to refine a subset of an alert category.

There are two methods for filtering alerts from being reported by the monitoring feature. One entails working in the *Profile Details* page and the other entails using the **Choose Action** drop-down menu from the *Monitoring Alerts* list page.

Filter alerts using the Include Text and Exclude Text capability from the Profile Details page

You can filter the alerts you receive based on the message text and severity level.

Use *Exclude Text* in conjunction with *Include Text* to refine a subset of an alert category.

NOTE: The criteria match text, for example, error, is matched in Windows event logs against both the severity level and the message itself.

1. Go to the *Profiles* list page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Monitoring**, then click **Profiles**.
2. Select the check box for the existing profile that you want to edit, and select **Choose Action** > **Edit** to display the *Profile Detail* page.
3. Make changes to the include and exclude *Criteria* settings, as needed.
    - **Change *Include Text*.**
        1. On the line with the include search text you want to change, click the **Edit** button: .
        2. Type the new search text.
    - **Change *Exclude Text*.**
        1. On the line with the text you want to change in order to exclude certain alerts, click the **Edit** button: .
        2. Type the new exclude text.
    - **If necessary, select Yes in the *Case-sensitive* drop-down list.**
    - **Add an alert Criteria.**
        1. On the *Criteria* category header, click the **Add** button: .
        2. Set the level, include text, exclude text, and case sensitivity.
4. Click **Save** at the bottom of the page.

Related topics

Examples of Include Text and Exclude Text for monitoring profiles

Edit a profile

Filter alerts using the Exclude Text capability from the Monitoring Alerts list page

If you are receiving too many alerts of a certain type, you can filter them based on the message text.

You can use full messages, parts of messages, and basic regular expressions in the *Exclude Text* field to define criteria for filtering the alerts you receive.

1. Go to the *Monitoring Alerts* list:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. Access the alerts list from either the Dashboard or the navigation bar.
    - **If you have the *Monitoring Alerts* widget installed on your open *Dashboard*, click Monitoring Alerts.**
    - **In the left navigation bar, select Monitoring > Alerts.**
2. Select the check box next to an alert.
3. Select **Choose Action** > **Filter Alerts Like This**.

The *Filter Alerts Like This* dialog appears, with the content of the alert message populating the *Exclude Text* field.

4. Edit text in the *Exclude Text* field to refine the filter.

   Example: To raise alerts for disk errors except for those errors for a fragmented disk, you could enter the following:

Include Text entry	Exclude Text entry
Error code.*Disk /dev/sd[a-z]	is fragmented

5. Click **Save**.

   The profile that generated the alert is modified with this exclude information.

Related topics

Examples of Include Text and Exclude Text for monitoring profiles

Filter alerts using the Include Text and Exclude Text capability from the Profile Details page

Examples of Include Text and Exclude Text for monitoring profiles

Full messages, parts of messages, and basic regular expressions can be used in the *Include Text* and *Exclude Text* fields for defining criteria.

Examples of field entries to match string formats

String Format (what to match)	Example Data	Include Text	Comments
[any text]`Error 32768 Physical memory running low`[any text]	`Error 32768 Physical memory running low`	`Error 32768 Physical memory running low`	Matches: "`Error 32768 Physical memory running low`"
`Drive /dev/`[any drive mount point] `has drive errors`	`Drive /dev/sdi has drive errors`	`Drive /dev/[a-z]{1,} has drive errors`	Matches: "`Drive /dev/`" followed by any word of any length containing the characters a-z followed by "`has drive errors`"
`Error` nnnn`: Disk is` [any text]	`2014-06-28: Error 4567: Disk is full`	`Error [0-9]{4}: Disk is`	Matches: "`Error`" followed by any four-digit number followed by "`: Disk is`"
`Error` nnnnnn [some error message]	`Error 4096 Drive has errors`	`Error [0-9]{1,8}`	Matches: "`Error`"

String Format (what to match)	Example Data	Include Text	Comments
			followed by any 1- to 8-digit number
`[FATAL]` [some error message]	`[FATAL] General exception occurred`	`[FATAL].*`	Matches: "`[FATAL]`" followed by any message
`error reading` [text] `on` [some volume]:	`error reading swap label on /dev/VolGroup00: [Errno 21] Is a directory`	`error reading.* on /dev/[a-zA-Z0-9]*:`	Matches: "`error reading`" followed by any text followed by "`on /dev/`" followed by any mount point containing the characters a-z, A-Z, 0-9 of any length followed by a colon

Examples of using Include Text and Exclude Text in conjunction to refine the alert output

Example A: String as exclude text

In this example, you are not interested in receiving alerts for disk errors about fragmented disks from a particular drive mount point, but you want all other errors to come through.

```
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
```

To raise alerts for the disk error and bad block but not for a fragmented disk, you could enter the following:

Include Text entry	Exclude Text entry
`Error code.*Disk /dev/sd[a-z]`	`is fragmented`

NOTE: *Include Text* does not recognize line breaks within the text box. This means that if you entered

```
code 5
code 7
```

NOTE: the search would look for matches for `code 5code 7`. In this case you should use **Add** to create a separate line for the second inclusion.

NOTE: However, *Exclude Text* does recognize line breaks within the text box. This means that if you entered

```
code 5
code 7
```

NOTE: the search would look for matches for `code 5` together with `code 7`. In this case you do not need to use **Add** to create a separate line for the second exclusion.

Example B: Basic regular expression as exclude text

In this example, you are not interested in receiving alerts for disk errors about fragmented disks or age information from a particular drive mount point, but you want all other errors to come through.

```
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
```

To raise alerts for the preferred events while ignoring the events that contain error code 5 or error code 7, you could enter the following:

Include Text entry	Exclude Text entry
`Error code.*Disk /dev/sd[a-z]`	`Error code [5|7]`

Escaping special characters in the include or exclude criteria text fields

When you type characters into the exclude or include criteria text fields you can also enter special characters such as single or double quotes. However, if you use these special characters, they must be escaped with a backslash character (****) in order for the search to work properly.

Character	Description
'	single quote
"	double quote
`	back tick
\	backslash

For example, to search for **Received 'redoubt started' message**, you would type Received \'redoubt started\' message.

Dismiss an alert

When you have dealt with an alert, you can dismiss it so that it does not appear in the lists of active alerts.

Dismissing an alert does not remove it from the database. If you want to delete the alert from the database, see Delete alerts.

1. Go to the *Monitoring Alerts* list page in one of the following ways:
   - **If you have the *Monitoring Alerts* widget installed on your open *Dashboard*, click Monitoring Alerts.**
   - **In the left navigation bar, select Monitoring > Alerts.**
2. Select the check box for the row that contains the alert message, then select **Choose Action > Dismiss**.

   The alert list no longer displays the alert.

Related topic

Retrieve and review alerts that have been dismissed from the alerts list

Retrieve and review alerts that have been dismissed from the alerts list

A dismissed alert remains in the database, and can be retrieved to the alerts list, where you can review it.

NOTE: Deleted alerts cannot be retrieved.

1. Go to the *Monitoring Alerts* list page in one of the following ways:
   - **If you have the *Monitoring Alerts* widget installed on your open *Dashboard*, click Monitoring Alerts.**
   - **In the left navigation bar, select Monitoring > Alerts.**
2. Select **Choose Action > Include Dismissed Alerts**.

   The alert list is repopulated with all dismissed alerts. These alerts are identified in the *Status* column with a status of *Dismissed*.

Delete alerts

After you have dealt satisfactorily with an alert, you can delete it from the database.

1. Go to the *Monitoring Alerts* list:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Monitoring**, then click **Devices**.
2. Select the check box next to one or more alerts.
3. Select **Choose Action > Delete**, then click **Yes** to confirm.

Using the Service Desk

Service Desk is the end-user trouble-ticket tracking system that is provided with the appliance. The Service Desk enables users to submit trouble tickets through email, through the Administrator Console, and through the User Console.

Configuring Service Desk

Configuring the Service Desk entails setting up roles, user authentication, labels, ticket and email settings, queues, and customizations.

System requirements

To use the Service Desk, you must have an appliance, an email server, and user account information.

- **Appliance requirements**: To use Service Desk, you must have an appliance set up and configured. See information on setting up the appliance server in Configuring the appliance.
- **Email server requirements**: You must have one of the following types of email servers for sending and receiving Service Desk email:
  # A POP3 email server. See About POP3 email accounts.
  # An email server, such as the Microsoft Exchange Server. For instructions on configuring this server to connect to the appliance, see Configuring SMTP email servers.
- **User account information**: User account information can be stored in an LDAP-compliant directory service such as Microsoft Active Directory. Storing user account information allows Service Desk to efficiently find and import data that it uses to authorize users and identify anything else that you want to track. You can filter groups of users or other entities by referencing their LDAP attributes, such as organizational units, domain components, and relative distinguished names. See Configuring user accounts, LDAP authentication, and SSO.

If your organization is small, you can eliminate this requirement by creating the required user account information manually, one user at a time. For more information about creating users manually, see Setting up Service Desk.

About Service Desk

Service Desk is the default name for the end-user trouble-ticket tracking system that is part of the appliance **User Console**. The Service Desk enables end users to submit trouble tickets through email or through the **User Console**.

Your help desk team manages these tickets through email, the **Administrator Console**, `http://`**appliance_hostname**`/admin`, or the KACE GO app. You can customize the categories and fields associated with tickets as needed.

NOTE: In previous versions of the appliance, **Service Desk** was referred to as **Help Desk**. If you upgraded from a previous release, you might see **Help Desk** or a custom phrase on the tab in the **Administrator Console**. You can change this label as described in Rename Service Desk titles and labels.

Overview of setup tasks

You can configure Service Desk to meet your company policies and branding requirements.

Setup tasks include:

- **Set up User Roles and labels**: Create permission-based roles to manage user access. See Setting up roles for user accounts.
- **Set up user accounts**: All Service Desk users and administrators must have authenticated user accounts. See Configuring user accounts, LDAP authentication, and SSO.
- **Customize ticket information**: Add ticket categories, status, impact, and priority properties as needed. Identify additional information to include in tickets. See Configuring ticket settings.
- **Customize email templates**: Configure the Service Desk email templates used to send notifications. See Configure email templates.
- **Set up email notifications**: Configure the events that trigger email notifications. See Configuring email settings.
- **Set up queues and processes**:
  # **Queues**: Use queues to organize tickets or to handle different types of tasks, such as hardware tasks and software tasks. See Configuring Service Desk ticket queues.
  # **Processes**: Use processes to set relationships between tickets that are parts of major or sequential tasks. You can also establish relationships by using parent-child relationships within tickets. See Using Service Desk processes.
- **Set up ticket rules**: Configure the rules that Service Desk uses to process tickets. See About Ticket Rules
- **Decide whether to offer a Satisfaction Survey to users**: See Using the Satisfaction Survey.
- **Configure company business hours and holidays**: Define your company's hours of operation and recognized holidays. These hours and holidays are used in determining ticket due dates and Service Level Agreement violations. See Configuring Service Desk business hours and holidays.
- **Configure Service Level Agreements (SLAs)**: Configure the SLAs used in calculating ticket due-dates and SLA violations. See Enable Service Level Agreements.
- **Configure User Console home page settings**: Change the logo and welcome information on the **User Console** home page. Or, show or hide quick actions and announcements as well as links to Knowledge Base articles, tickets, and other items. See:
  # Change the User Console logo and login text at the Admin-level
  # Show or hide action buttons and widgets on the User Console home page
  # Add, edit, hide, or delete User Console announcements
  # Add, edit, or delete custom links on the User Console home page
  # Show or hide links to Knowledge Base articles on the User Console home page

Import tickets from another system

You can import tickets from another system using prepared CSV (comma-separated value) files. Start by exporting your tickets to a CSV file and then use the *Import Tickets* wizard to import that content into the appliance. The wizard validates the data being imported, and certain fields must follow predefined formats, to prevent related records from being rejected.

1. Export your ticket data to a CSV file.
2. Go to the *Import Tickets* :

a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
b. On the left navigation bar, click **Service Desk**, then click **Configuration**.
c. On the **Configuration** panel, in the *Import* section, click **Import tickets**.

3. In the *Import tickets* wizard, on the *Step 1 of 3 - Select File* page, specify the CSV file and the related options, as needed.

TIP: You can review the status of the most recent ticket import by clicking the link at the bottom of the page.

a. In the *Upload file (.csv)* section, click **Choose File**, and select the CSV file containing ticket data that you want to import.
b. If your CSV file has a header row, select the **File Header Row** check box.
c. In the *Importing to* section, specify the queue and template into which you want to import your ticket data.
d. If your ticket data includes one or more users who do not exist in the appliance database, and you want to automatically create them as you import the tickets, select the **Auto Create User** check box.
e. Click **Next**.

4. In the *Import Tickets* wizard, on the *Step 2 of 3 - Map Fields* page that appears, map the ticket template fields to the ticket fields specified in the CSV file.

Use the following guidelines when mapping ticket fields:

To specify a ticket field, click the **CSV Fields** column, and select the applicable value.

A **Comment** field must use the following syntax: `"<datetime>";"<user_name>";"<comment>";"<owners_only_flag>"`. Multiple comments in a single **Comment** field must be separated with `|EOL|`. For example: `"01/01/2019 10:10";"Admin";"This is a sample comment";"Y"|EOL|"01/02/2019 11:20";"User A";"This is a sample comment 2";"Y"|EOL|"01/02/2019 12:00";"Admin";"This is a sample comment 3";"Y"|EOL|`. Alternatively, you can use the Primary Key to combine multiple column entries in the same ticket field. See Table 32 and Table 33.

A **Work Detail** field must use the following syntax: `"<user_name>";"<start_datetime>";"<end_datetime>";"[adjustment_time];[<note>]`. Multiple comments in a single **Comment** field must be separated with `|EOL|`. For example: `"Admin";"01/01/2019 08:10";"01/01/2019 10:30";"10";"Work Note"|EOL|"User B";"01/01/2019 11:20";"01/01/2019 12:30"`. Alternatively, you can use the Primary Key to combine multiple column entries in the same ticket field. See Table 32 and Table 33.

A **Category** field that contains subcategories must use a double colon "::" to separate subcategories. For example: `Hardware::Printer::Paper`. If the import detects any categories that do not already exist on the appliance, those records are automatically rejected.

Impact and **Priority** fields must contain valid contents that are predefined on the appliance.

User name fields (such as **Submitter**) accepts the user email, user name, user ID, and the display name. Multiple records with the same user name are automatically rejected.

The contents of any custom fields that expect a certain data format (such as links) are validated and rejected if the data is invalid.

Use the **PK** column to indicate if a row is a primary key for the data records. Any records that have the same value of the column marked as a primary key are combined into a single Service Desk ticket. For example, if you mark the **Title** column as a primary key for the ticket table, and all of your records in the CSV file have the exact same **Title** column (for example *My Ticket*), the import results in a single Service Desk ticket being created, with multiple entries combined in the same column. Alternatively, when importing *Comment* and *Work Detail* columns, you can use `|EOL|` to separate the entries. The following examples show you how to structure your input CSV file when you want to combine multiple entries into the same ticket field, either by using the `|EOL|` delimiters (*Comment* and *Work Detail* columns only), or the Primary Key (PK) setting (any column).

Table 32. Example: Combine multiple column entries using |EOL| delimiters (Comment and Work Detail columns only)

Title	Status	Priority	Owner	Comment
Title A	New	Medium	Admin	"6/15/2021 3:15:44 comment AAA" |EOL| "6/17/2021 5:17:25 comment BBB" |EOL| "6/19/2021 7:21:42 comment CCC" |EOL|
Title B	Closed	High	Admin	"7/21/2021 2:18:31 comment DDD" |EOL| "6/17/2021 4:56:56 comment EEE" |EOL| "6/19/2021 6:28:32 comment FFF" |EOL|

NOTE: The `|EOL|` delimiter instructs the wizard to combine these entries into a single *Comment* field. There is no need to declare the *Title* column as the primary key (*PK*). The same syntax applies to *Work Detail* contents.

Table 33. Example: Combine multiple column entries using the Primary Key setting

Title	Status	Priority	Owner	Comment
Title A	New	Medium	Admin	"6/15/2021 3:15:44 comment AAA"
Title A				"6/17/2021 5:17:25 comment BBB"
Title A				"6/19/2021 7:21:42 comment CCC"
Title B	Closed	High	Admin	"7/21/2021 2:18:31 comment DDD
Title B				"6/17/2021 4:56:56 comment EEE"
Title B				"6/19/2021 6:28:32 comment FFF"

NOTE: When you declare the *Title* column as a primary key (PK), all entries with the same *Title* (*Title A* and *Title B*) are combined into a single *Comment* field. There is no need to use `|EOL|` delimiters. The same mechanism applies to other columns, including *Work Detail* .

The **PK** setting can also be used to update an existing ticket. For example, you uploaded *Ticket A* with the data listed in Table 34, you can easily replace by uploading an updated CSV file outlined in Table 35, but you must set the *Title* column as the Primary Key (**PK**) in the settings:

Table 34. Example: Initial CSV data

Title	Status	Priority	Owner
Title A	New	High	User A

Table 35. Example: Updated CSV data

Title	Priority	Owner
Title A	Low	User B

When done, click **Preview**.

5. Confirm that the data you are about to import is valid on the *Step 3 of 3 - Review* page that appears.

a. Review the following sections:

Records for insertion: Lists all ticket records from the CSV file that are about to be created as Service Desk tickets.

Records for update: Lists all ticket records from the CSV file that are about to update existing Service Desk tickets.

Rejected records: Lists all ticket records from the CSV file that are not going to be created as Service Desk tickets due to errors. For each rejected record, the *Reason* column in this section indicates the cause of the error. The related ticket field appears highlighted in red. Review the contents of that field to better understand the problem. For example, if you have users in your CSV file who do not exists on the appliance, and did not select **Auto Create User** check box, this causes an error for each such user. You can resolve any errors by editing the import CSV file, or changing the applicable import options on the *Step 1 of 3 - Select File* page.

b. When you are ready to proceed with the import of the ticket data, click **Import**.

NOTE: Once you start with the import, the process cannot be stopped or reverted, however you can delete any tickets once the import is completed.

The *Import Tickets - Status* page appears, indicating that the ticket records are being imported. The time required to complete import depends on the amount of ticket data being imported. When done, the *Status* row tells you the outcome of the import operation. If any errors are detected during the import, this is indicated in the *Error records* row. Click Show details to find out more (when applicable).

6. If you are satisfied with the outcome of the import, and do not need to import any additional records, click **Done**. To import more tickets, click **Import More**, and repeat the import process, as applicable.

Configuring Service Desk business hours and holidays

You can configure business hours and holidays to effectively track and meet Service Level Agreements (SLAs) in your Service Desk queues. If the Organization component is enabled on your appliance, you configure business hours and holidays for each organization separately.

After you configure business hours and holidays, you need to enable the SLA settings in each Service Desk ticket queue to use those business hours and holidays.

Configure Service Desk business hours

You can configure the Service Desk to account for business hours when calculating due dates for tickets. If you have multiple organizations, you configure business hours for each organization separately.

After you configure Service Desk business hours, you need to enable ticket queues to use those hours in their Service Level Agreement (SLA) settings.

1. Go to the *Business Hours* page:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Service Desk**, then click **Configuration**.
   c. On the **Configuration** panel, in the *Business Hours and Holidays* section, click **Define business hours**.
2. For each day of the week, specify the hours of operation by providing the starting and ending time, by selecting the **Open 24 Hours** check box, or by selecting the **Closed** check box.
3. Click **Save**.

Configure queues to use business hours in SLAs. See Configure ticket queues.

Configure Service Desk holidays

You can configure the Service Desk to account for company holidays when calculating due dates for tickets. If you have multiple organizations, you configure the holiday schedule for each organization separately.

After you configure Service Desk holidays, you need to enable ticket queues to use those holidays in their Service Level Agreement (SLA) settings.

1. Go to the *Holidays* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Service Desk**, then click **Configuration**.
    c. On the **Configuration** panel, in the *Business Hours and Holidays* section, click **Define holidays**.
2. Click **Add Holiday** to add a new holiday to the list. Click the **Edit** button next to a holiday to edit it: . Click the **Delete** button next to a holiday to remove it: . Holidays in the list can be filtered by year by selecting a year in the **Filter by Year** drop-down list.
3. Click **Save**.

Configure queues to use holidays in SLAs. See Configure ticket queues.

Configuring Service Level Agreements

Service Level Agreements (SLAs) are the rules used to calculate the expected resolution time, or due dates, for Service Desk tickets based on ticket priority.

You can set the expected resolution time for each ticket priority, and you can enable SLAs to take the defined business hours and holidays into consideration when calculating due dates. For example, if tickets with a priority of **Low** are set to be resolved in two days, and a Low priority ticket is submitted the day before a holiday, the holiday is excluded from the two-day resolution time when calculating the due date.

In addition, if notifications and email events are enabled, email is sent to users specified in the SLA Violation email event when tickets are overdue. The frequency of email notifications is configured in the SLA settings, and notifications are sent according to that frequency, even if that frequency includes non-working hours or holidays.

Enable Service Level Agreements

Service Level Agreements (SLAs) define the time allowed to resolve tickets in each queue. If you have multiple Service Desk queues, you configure SLA settings for each queue separately.

SLAs are based on the priority values defined in the queue, so these values should be defined before SLAs are configured. See Customize ticket priority values. In addition, SLAs can use business hours and holidays only if those hours and holidays have been defined. See Configuring Service Desk business hours and holidays.

1. Go to the Service Desk *Queue Detail* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Service Desk**, then click **Configuration**.
    c. On the **Configuration** panel, click **Create and manage queues** in **Queue** section.

d. To display the *Queue Detail* page, do one of the following:

Click the name of a queue.

Select **Choose Action** > **New**.

2. Go to the *Service Level Agreement* tab. A row is displayed for each priority value defined for the queue. See Customize ticket priority values.
3. For each Priority, such as **High**, **Medium**, and **Low**, specify the following settings:

Option	Description
Response SLA Enabled?	Whether the SLA is enabled for the priority. Select the check box to enable the SLA, clear the check box to disable it. **NOTE:** If the Service Level Agreement is enabled for a Priority, the ticket due date is calculated automatically based on the Resolution Time defined for that priority. Any user who has Modify Permission on the DUE_DATE field is able to override this automatically calculated date.
Response Time	The time, in hours or minutes, for the enabled priority. This time period is used to automatically calculate a ticket's due date and time based on the date and time the ticket is submitted.
Use Business Hours/ Holidays(Response SLA)	Whether to use the configured business hours and holidays when calculating ticket due dates for each priority. Select the check boxes to use these settings. See Configuring Service Desk business hours and holidays.
Resolution SLA Enabled?	Whether the SLA is enabled for the priority. Select the check box to enable the SLA, clear the check box to disable it. **NOTE:** If the Service Level Agreement is enabled for a Priority, the ticket due date is calculated automatically based on the Resolution Time defined for that priority. Any user who has Modify Permission on the DUE_DATE field is able to override this automatically calculated date.
Resolution Time	The time, in hours or minutes, for the enabled priority. This time period is used to automatically calculate a ticket's due date and time based on the date and time the ticket is submitted.
Use Business Hours/ Holidays(Resolution SLA)	Whether to use the configured business hours and holidays when calculating ticket due dates for each priority. Select the check boxes to use these settings. See Configuring Service Desk business hours and holidays.
Resolution SLA Violation Notification Recurrence	The time, in hours or minutes, for email notifications to be sent. A recurring email notification is sent when a ticket has passed its due date and is not yet resolved. The email is sent to the users specified in the SLA Violation email event, if configured in the Email on Events section. See Configuring email triggers and email templates. **NOTE:** To send a single email notification with no recurrence, enter 0.

4. Click **Save**.

Configuring Service Desk ticket queues

Service Desk tickets are stored in queues on the appliance. Most organizations need only a single ticket queue. You can customize this single queue, or create and manage additional queues, as needed.

See Managing Service Desk ticket queues.

Configure ticket queues

You can modify the settings of ticket queues as needed.

1. Go to the Service Desk *Queue Detail* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Service Desk**, then click **Configuration**.
    c. On the **Configuration** panel, click **Create and manage queues** in **Queue** section.
    d. To display the *Queue Detail* page, do one of the following:
    # Click the name of a queue.
    # Select **Choose Action** > **New**.
2. Specify the following settings in the **General** tab:

Field	Description
Name	The name of the *Service Desk* queue. This name appears in the *From* field when users receive email messages from the Service Desk.
Email Address	A fully qualified email address for the server. Users typically do not reply to this address. If you want to allow users to reply to appliance email, specify an email address in the *Alternate Email Address* field.
Ticket Number Prefix	Specify a custom ticket prefix for this queue. You can use a different prefix for each queue to organize your Service Desk workflow, and to associate them with applicable categories, such as HD for Helpdesk or REQ for hardware and software requisitions.
Alternate Email Address	**Support@mydomain.com** The primary email address your users send email to. The appliance also uses this address to send email from the Service Desk. Confirm that the domain name is correct for your email service. **NOTE:** As a valid email address, this address is subject to the same spam and security vulnerabilities as any other email address.

3. **Optional**: Configure the SMTP/ POP3 server settings. Click **Configure queue email settings** and specify the SMTP/POP3 options in the **Inbound** tab on the *Service Desk Queue Email Settings* page, as required. See Configure queue-specific email settings.
4. Click **Save** to create the queue and configure additional settings.
5. Specify *Preferences* in the **Preferences** tab:

Field	Description
Allow ticket deletion	Allow ticket owners and administrators to delete tickets. This setting is useful if you do not want staff to delete tickets. You can periodically select this check box to clean out old tickets, then clear it again to prevent ticket deletion.
Allow parent ticket to close child tickets	Enable the system to automatically close child tickets when parent tickets are closed.
Allow last child ticket to close parent ticket	Enable the system to automatically close parent tickets when the last child ticket is closed.
Allow users with an Administrator role to read and edit tickets in this queue (**Administrator Console** only)	Grant read and write permissions to all users who are assigned to the **Administrator** role.
Default ticket owner comments to Owners Only visibility	Automatically select the *Owners Only* check box when comments are added to tickets.
Enable ticket conflict warning for ticket owners	Display a dialog, to administrators and ticket owners, that summarizes conflicts between the changes they are submitting and the changes submitted concurrently by other users. When administrators and ticket owners click **Save** or **Apply Changes** on the *Ticket Detail* page, the dialog appears if other users have edited and saved the ticket while it was open for editing. This enables administrators and ticket owners to choose whether to discard their changes, or overwrite the changes made by other users if there are conflicts. **NOTE:** By default, this warning is enabled on new queues and disabled on queues that were created in appliance version 6.3 or earlier. The dialog is displayed only if other users have modified the ticket, and it is displayed to administrators and ticket owners only. The dialog is not displayed to other users. **NOTE:** The dialog summarizes all changes made by other users. However, the current user's changes are summarized only if they conflict with changes made by other users.
Allow managers to view and comment on their employee's tickets	Enable manager accounts to view and edit comments in the tickets submitted by their employees. For more information, see View ticket comments.
Allow Ticket CC list to view and comment on the ticket	Allow the users on the ticket CC list to add comments to the ticket.
Add any user to Ticket CC list when they	Add any users that comment on a ticket to a CC list for that ticket, allowing them to be notified by email about further changes to the ticket.

Field	Description
comment on a ticket	
Enable aggressive HTML sanitization	Remove all malicious code on all fields that accept HTML.
Allow Knowledge Base article suggestions	Display KB article suggestions while typing the ticket title. **NOTE:** If this option is disabled and a password manager is linked to the browser, this prevents the browser from auto-completing the related Service Desk ticket fields.

6. In the *Restrictions* tab, select settings for ticket archival. Click the **Settings** link to enable ticket archival.

NOTE: If Ticket Archival is turned off, see Enable ticket archival.

Option	Description
Allow all users as submitters	Allow anyone who is a user on the appliance to submit tickets through this Service Desk queue.
Restrict Submitters by Label	Select submitters by label only. Available only when **Allow all users as submitters** is not selected.
Allow all users as approvers	Allow users on the appliance to approve tickets through this Service Desk queue.
Restrict Approvers by Label	Select approvers by label only. Available only when **Allow all users as approvers** is not selected.
Owner Label	If you want to enable all users to have the ability to approve tickets, select **Allow all users as approvers**. Identify the users who are allowed to own and manage tickets — typically, your IT staff. You must have a Ticket Owner who is responsible for managing the ticket through its life cycle. To do that, click **Manage Associated Labels**. In the *Select Labels* dialog box that appears, select one or more labels associated with the users that you want to select as Ticket Owners. Close the dialog box.
All users can edit/delete their own comments (including attachments)	Allow all users to edit or remove their own comments, including file attachments.
User Label	To allow specific users to edit or delete their own comments and attachments using labels, click **Manage Associated Labels**. In the *Select Labels* dialog box that appears, select one or more labels associated with the users that you want to select. Close the dialog box.
All technicians can edit/delete comments entered by others (including attachments)	Allow all technicians to edit or remove comments added by others, including file attachments.

Option	Description
Technician Label	To allow specific technicians to edit or delete comments and attachments added by others using labels, click **Manage Associated Labels**. In the *Select Labels* dialog box that appears, select one or more labels associated with the technicians that you want to select. Close the dialog box.
Accept email from unknown users	Allow unrecognized users to create tickets. **If this option is enabled in the queue configuration, any email sent to the Service Desk queue is allowed to set the *Submitter* field of a ticket. The sender is added to the appliance as a user with the *User Console Only* role. By default, this role has permission to create, view, and modify Service Desk tickets, and to interact with the appliance exclusively through the User Console. You can adjust the level of permissions associated with this and other roles, as applicable. For more information, see** Setting up roles for user accounts**.** If disabled, the preceding process works only when the email address of the sender is already associated with a Service Desk user account.
Ticket attachment restrictions	Indicate how you want to handle file attachment restrictions, as applicable. • **None**: Allow users to add any types of files as attachments. • **Allow images only**: Allow only image files to be added as attachments. • **Custom**: Specify file extensions that you want to allow as attachments. You can also allow all files without extensions. • **Prevent all attachments**: Disable users from adding any file attachments.

7. In the *Archive* tab, select settings for ticket archival. Click the **Settings** link to enable ticket archival.

NOTE: If Ticket Archival is turned off, see Enable ticket archival.

Option	Description
Archive closed tickets older than	The age of tickets to be archived. For example, if you select **3 months**, tickets are archived when three months have passed since the tickets were closed. To prevent tickets in the queue from being archived, select **Never**. Archived tickets can be restored to the queue if necessary. See Restore archived tickets.
Delete archived tickets older than	The age of tickets to be permanently removed from the archive. For example, if you select **6 months**, archived tickets are deleted from the archive when

Option	Description
	six months have passed since the tickets were opened. To prevent tickets in the queue from being deleted from the archive, select **Never**. Deleted tickets cannot be restored to the queue.
Archive Process	Displays the status of archive.

8. In the *Ticket Defaults* tab, select the default values for new tickets. For example:
   - **Category**: Software
   - **Status**: New
   - **Impact**: 1 person cannot work
   - **Priority**: Medium
9. In the *Email on Events* section, select the categories of users who will receive email when the specified events occur. Each column represents a type of Service Desk user (role) and each row represents a ticket event. See Configure email triggers.
10. **Optional**: Configure *Service Level Agreement Settings*. Here you can enable Service Level Agreement (SLA) settings based on the ticket priority. When enabled, the due date of the ticket automatically takes into account the resolution time, business hours, and holidays. See Configuring Service Level Agreements.
11. In the *Ticket Rules* section, enable the rules to apply to tickets in the queue. You can use any of the pre-defined rules or customize your own. See Using Ticket Rules for more information about how to use and customize ticket rules.
12. Click **Save**.

Configure queue-specific email settings

You can set up email settings for each ticket queue separately.

By default, the Service Desk is configured to use an internal SMTP server for sending ticket-related emails. You have an option to use an external SMTP server, however, you must configure it in the appliance network settings. For more information, see Change appliance network settings.

1. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
2. Go to the queue-specific *Service Desk Queue Email Settings* page:
   a. On the left navigation bar, click **Service Desk**, then click **Configuration**.
   b. On the **Configuration** panel, in the *Email Configuration* section, click **Configure Queue Email Settings**.
   c. On the *Service Desk Queue Email Settings* page that appears, select a queue from the drop down.

   Or:

   a. On the left navigation bar, click **Service Desk**, then click **Configuration**.
   b. On the **Configuration** panel, click **Create and manage queues** in **Queue** section.
   c. Click [edit] near the queue email address.

   The *Service Desk Queue Email Settings* page appears.
3. In the *General* tab, specify the following options:

Field	Description
Email Address	A fully qualified email address for the server. Users typically do not reply to this address.

Field	Description
	If you want to allow users to reply to appliance email, specify an email address in the *Alternate Email Address* field.
Alternate Email Address	**Support@mydomain.com** The primary email address your users send email to. The appliance also uses this address to send email from the Service Desk. Confirm that the domain name is correct for your email service. **NOTE:** As a valid email address, this address is subject to the same spam and security vulnerabilities as any other email address.

4. Select and configure the method of receiving inbound email using the options in the *Inbound Email Settings* tab.

   - **Use SMTP Server for inbound emails: Select this option if you want to use an internal SMTP server for incoming email. You can specify the required credentials in the *Outbound Email Setting* tab below. See 5.**
   - **Use POP3 Server for inbound emails: Select this option if you want to use a POP3 server for incoming email. Specify the following options:**

Option	Description
POP3 Server	Enter the name of the POP3 server you want to use for the queue. For example, **pop.example.com**.
Use SSL	Select this option if you want the POP3 server to use a secure connection.
POP3 Username (email address) **POP3 Password**	Enter the username and password of an account that has access to the POP3 server.

   Click **Test Connection** to test your POP3 configuration. The Connection Test POP3 dialog box appears, showing several log messages, indicating the test result. If the test is successful, these messages, for example, indicate if the user account is authenticated, the number of unread messages, and the subject line of the most recent email. If the test fails, verify your configuration, and try again.

   - **Use IMAP Server for inbound emails: Select this option if you want to use an IMAP server for incoming email. Specify the following options:**

Option	Description
IMAP Server	Enter the name of the IMAP server you want to use for the queue. For example, **imap.example.com**.
Use SSL	Select this option if you want the IMAP server to use a secure connection.
IMAP Server Username (email address) **IMAP Server Password**	Enter the username and password of an account that has access to the IMAP server.

   Click **Test Connection** to test your IMAP configuration. The Connection Test IMAP dialog box appears, showing several log messages, indicating the test result. If the test is successful, these messages, for example,

indicate if the user account is authenticated, the number of unread messages, and the subject line of the most recent email. If the test fails, verify your configuration, and try again.

- **Use Gmail for inbound emails: Select this option if you want to use Google Gmail for incoming email. Click Select Credential.**

  # To use an existing Google OAuth credential, select in the list.

  > **NOTE:** You must create a dedicated Google OAuth credential for retrieving email. You cannot, for example use the same account for accessing Chrome devices and downloading email.

  # To create a new Google OAuth credential, click **Add Credential**. The *Add Credential* dialog box appears. Specify the required options, as applicable. For more details, see Add and edit Google Workspace credentials.

- **Use Office365 for inbound emails: Select this option if you want to use Office 365 for incoming email. Specify the following options:**

Option	Description
Select Credential	• To use an existing Office 365 OAuth credential, select in the list. • To create a new Office 365 OAuth credential, click **Add Credential**. The *Add Credential* dialog box appears. Specify the required options, as applicable. For more details, see Add and edit Microsoft Office 365 OAuth credentials.
Microsoft 365 API Service	Select the applicable Microsoft 365 API Service for your environment: • For an Azure AD app located in the US, select one of the following options, as applicable: # **Microsoft 365 GCC**: You can continue to use the worldwide endpoints in Azure: https://graph.microsoft.com and https://portal.azure.com to register. # **Microsoft 365 GCC High**: Use https://portal.azure.us and https://graph.microsoft.us to register. # **Microsoft 365 DoD**: Use https://portal.azure.us and https://dod-graph.microsoft.us to register. • For an Azure AD app located in Germany, select **Microsoft 365 Germany**. • For an Azure AD app located in China, select **Microsoft 365 China**.

5. If you want to use an external SMTP server for emails associated with this queue, use the settings in the *Outbound Email Setting* tab.
   a. Select the *Specify Queue specific SMTP Settings* check box.
   b. Specify the following options:

Option	Description
SMTP Server	Specify the hostname or IP address of an external SMTP server, such as **smtp.gmail.com**. External SMTP servers must allow anonymous (non-authenticated) outbound email transport. Ensure that your network policies allow the appliance to contact the SMTP server directly. In addition, the mail server must be configured to allow the relaying of email from the appliance without authentication.
SMTP Port	Enter the port number to use for the external SMTP server. For standard SMTP, use port 25. For secure SMTP, use port 587.

Option	Description
SMTP Username	Enter the username of an account that has access to the external SMTP server, such as **your_account_name**@gmail.com.
SMTP Password	Enter the password of the specified server account.

6. Specify how you want to handle file attachments when emailing ticket details in the *Outgoing Email Attachment Setting* tab.

Option	Description
Allow embedded images	Select this option if you want to include any graphic files to ticket-related email. When this option is selected, the graphics appear as embedded images.
Combined image size limit per email (MB)	Specify the maximum file size of all images associated with a ticket that can be embedded in ticket-related email.
Allow file attachments on outgoing email	Select this option if you want to send files attached to the ticket instead of providing file links.
Combined file size limit per email (MB)	Specify the maximum file size of all file attachments that can be sent by email.

7. On the *Service Desk Queue Email Settings* page, in the *Email on Events* tab, select the options for sending email when the specified events occur. Each column represents a type of Service Desk user (role) and each row represents a ticket event.

Service Desk user (role)	Description
Owner	The person who is expected to resolve the ticket.
Submitter	The person whose issue is being resolved.
Approver	The person who can approve or reject the ticket for processing.
Ticket CC	One or more email addresses that are stored in the *CC* field of the ticket.
Category CC	One or more email addresses that are stored in the *CC List* of the *Category Value* of the ticket. See Configure CC lists for ticket categories.
Queue Owners	One or more owners of the ticket queue, as specified by the *Owner* label. This only applies to the *New Ticket Via Email* and *New Ticket via Portal* events.

When a ticket event occurs, email is sent to the selected roles or users. For example, if you select the **Any Change** box in the *Owner* column, email is sent to the ticket owner whenever the ticket is changed. For the *Comment* and *Ticket Closed* triggers, email is sent immediately. For other ticket changes, however, email is sent every few minutes to prevent email overload.

NOTE: If users have the KACE GO mobile app installed on their smart phone or tablet, the system sends push notifications for the selected Service Desk ticket events.

Option	Description
Any Change	Any information on the ticket is changed.
Owner Change	The ticket's *Owner* field is changed.
Status Change	The ticket's *Status* field is changed.
Comment	Information, attachments, or screen shots are added to the ticket's *Comments* section. The system sends email notifications for comments when users add comments and click **Submit** on the ticket form. When users add comments and click **Save** on the ticket form, however, only the *Any Change* notification is sent.
Approval Change	The ticket's approval status has changed.
Resolution Change	The ticket's resolution has changed.
Response SLA Escalation	The ticket has not been updated to a stalled or closed status within the escalation time defined by the ticket priority.
Resolution SLA Violation	The ticket has not been resolved by its due date.
Ticket Closed	The ticket's *Status* field is changed to **Closed**. This event is used to present a Satisfaction Survey to submitters. See Using the Satisfaction Survey.
New Ticket Via Email	A user sends an email message to the Service Desk and a ticket is created.
New Ticket Via Portal	A ticket is created through the **User Console**.

8. Click **Save**.

   The appliance is configured to forward email to the designated SMTP server. If you have multiple queues, repeat the preceding steps for each queue.

Rename Service Desk titles and labels

You can rename the Service Desk titles and labels used in the **Administrator Console** and **User Console** as needed.

1. Go to the Service Desk *Settings* page:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Service Desk**, then click **Configuration**.
   c. On the *Configuration* panel, click **Customize Service Desk terminology** in **Setting** section.
2. Specify the following settings in the **Screen Labels** tab:

Setting	Description
Main Tab	The text that appears on the component-level tab in the **Administrator Console** and on the tab in the **User Console**. The default is **Service Desk**. However, if you upgraded from an earlier version of the appliance, you might see **Help Desk** as the default.
Queue **Queues**	The text that you want to display instead of **Queue** and **Queues** on the *Service Desk Configuration* page and on the *Queue* list in the **Administrator Console**. This text also appears as an option in the *Choose Action* menu and as a heading on the *Ticket* page in the **User Console**.
Ticket **Tickets**	The text that you want to display instead of **Ticket** and **Tickets** on the *Ticket* tab and *Ticket* page in the **Administrator Console**. This text also appears on the *Ticket* page in the **User Console**.
Process **Processes**	The text that you want to display instead of **Process** and **Processes** on the *Service Desk Configuration* page and on the *Process* list in the **Administrator Console**.

3. Click **Save**.

Enable or disable the conflict warning

When the conflict warning dialog is enabled for a queue, administrators and ticket owners see a notification dialog when multiple users are editing tickets concurrently. The dialog enables users to view changes made by others and decide which changes to keep.

You have administrator privileges in the **Administrator Console**.

Administrators can enable or disable the conflict warning dialog for each queue separately.

1. Go to the Service Desk *Queue Detail* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Service Desk**, then click **Configuration**.
    c. On the **Configuration** panel, click **Create and manage queues** in **Queue** section.
    d. To display the *Queue Detail* page, do one of the following:
    # Click the name of a queue.
    # Select **Choose Action** > **New**.
2. In the *User Preferences* tab, enable or disable the conflict warning:

Field	Description
Enable ticket conflict warning for ticket owners	Display a dialog, to administrators and ticket owners, that summarizes conflicts between the changes they are submitting and the changes submitted concurrently by other users. When administrators and ticket owners click **Save** or **Apply Changes** on the *Ticket Detail* page, the dialog appears if other users have edited and saved the ticket while it was open for editing. This enables administrators and ticket owners to choose whether to discard their changes, or overwrite the changes made by other users if there are conflicts. The dialog is displayed only if other users have modified the ticket, and it is displayed to administrators and ticket owners only. The dialog is not displayed to other users.

Field	Description
	NOTE: The dialog summarizes all changes made by other users. However, the current user's changes are summarized only if they conflict with changes made by other users.

3. Click **Save**.

View and edit response templates

Response templates allow you to store common responses as comments or resolutions in Service Desk tickets.

Each response template is associated to a specific ticket queue and belongs to the user that created it. You can select the applicable response template on the *Ticket Detail* page.

The template text supports the use of email tokens. Token values are dynamically updated using the field values from the ticket in which they are referenced. You can use the same tokens that are available in email templates. For more information, see Configure email templates.

A response template can be public or private. Private response templates can be updated and referenced in applicable tickets only by the user that created them. A public response template is available for selection in the associated ticket queue by other users, however only the user that created it can edit the contents of the response message. Other users can view the contents of public response templates, but cannot edit them.

1. Go to the Service Desk *Response Templates* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Service Desk**, then click **Configuration**.
    c. On the **Configuration** panel, under **Queues**, click **Create and manage response templates**.
    d. To display the *Response Template Detail* page, do one of the following:
    # Click the name of a response template.
    # Select **Choose Action** > **New**.

NOTE: Those queue owners who do not have access to the *Queues* configuration pages can access the *Response Templates* page by clicking the *Manage* link that appears just above the *Predefined Response* option in the *Ticket Detail* page.

2. Specify the following settings:

Field	Description
Name	The name of the response template. This name appears available for selection in the *Predefined Response* field when you want to configure an automated response to applicable Service Desk tickets.
Make Public	Select this check box if you want to make this response template available for selection to other users. Other users can view the contents of public response templates, but cannot edit them.
Template	The contents of the response message. This field supports plain text and tokens.

3. If you made any changes to the response template, click **Save**.
4. To go back to the Response Templates list, click **Cancel**.

You can use a response template as a predefined response to a Service Desk ticket inquiry. For more information, see Add comments to tickets.

Configuring ticket settings

Each Service Desk ticket queue has default settings for new tickets, and you can configure those settings and add custom fields as needed.

Typical custom fields include:

- **Problem-related information**: Symptoms, how long the problem has been occurring, or other components that might contribute to the problem.
- **Software-related information**: Manufacturer, version, purpose, and installation date of the software.
- **Service Desk staff-only information**: Information that can be used for diagnosing, reporting, or planning purposes, such as “vendor contact for escalation,” “root cause,” or “previously fixed.”
- **Custom ticket characteristics**: Categories, Statuses, Priorities, and Impacts.

You can add or change these fields at any time, and the number of fields is restricted only by the number of columns that you can have in a database table. However, you cannot remove fields if they are used by tickets. To remove a field that is in use, change the tickets to use a different field, then remove the field.

Customize the Ticket Detail page

You can customize the *Ticket Detail* page for queues as needed. If you have multiple queues, you can customize the *Ticket Detail* page for each queue separately.

Service Desk has the following configurable ticket settings:

Setting	Available Values
Category	• Software • Hardware • Network • Other (default)
Status	• New (default) • Open • Closed • Need more info
Impact	• Many people cannot work • Many people inconvenienced • 1 person can't work (default) • 1 person inconvenienced
Priority	• High • Medium (default) • Low
States	• Open (default) • Closed • Stalled

1. Go to the *Service Desk Queue Detail* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Service Desk**, then click **Configuration**.
    c. On the **Configuration** panel, click **Create and manage queues** in **Queue** section.
    d. To display the *Queue Detail* page, do one of the following:
    # Click the name of a queue.
    # Select **Choose Action** > **New**.
2. In the **Restrictions** tab, add the **All Ticket Owners** label to the *Owner Label* field:
    a. In the *Owner Label* field, click **Manage Associated Labels**.
    b. In the *Select Labels* dialog, drag **All Ticket Owners** to the *Restrict Owners To* field, then click **OK**.

For more information about this label, see Add an All Ticket Owners label.

c. Click **Save**.

3. In the *General* tab, click **Customize Queue Fields** to display the *Queue Customization* page. **Or** From the left navigation bar, click **Configuration** and then in the **Queue** section click the *Customize fields* to display the **Queue Customization** page
4. In the *Category* tab, click the **Add** button in the column heading to add a category: +.

   Editable fields appear for the new value.
5. Specify the following settings:

Field	Description
Category Name	The text that appears in the drop-down list. By default, this text is **Please select a category**: This instructs users to select the category of the ticket.
Default Owner	Select **DefaultTicketOwners**.
CC List	Select **none** to prevent the CC List from being displayed on tickets. Because **DefaultTicketOwners** is the default owner, all potential ticket owners receive email notifications when a ticket is created.
User Settable	Make this category visible to users. When cleared, the appliance allows only the Service Desk staff users to see this category. Use this setting to present a simplified list of values to users and to provide a comprehensive list to your administrators and Service Desk staff. Users might see these categories as their tickets are processed, but they cannot set or change them.

6. Click **Save**.

   NOTE: You can add ticket categories at any time. See Create ticket categories and subcategories.
7. For the remaining categories in *Category Values*, click the **Edit** button: .
8. Make the following changes:
   a. In the *Default Owner* column, select **DefaultTicketOwners** to make this user account the default owner of all of these categories.

      For more information about this account, see Create the DefaultTicketOwners account.
   b. Remove anything in the **CC List**.
   c. Click **Save**.
9. In **Status** tab, create additional status values:
   a. In the *Status Values* section, click the **Add** button: +.

      The editable fields appear for the new value.
   b. In the *Name* column, type Waiting on end user, then in the *State* column, select **Stalled**.
   c. Click **Save**.
   d. In the *Status Values* section, click the **Add** button: +.
   e. In the *Name* column, type Waiting on Service Desk Staff, then in the *State* column, select **Stalled**, then click **Save .**
   f. In the *Status Values* section, click the **Add** button: +.
   g. In the *Name* column, type Reopened, then in the *State* column, select **Opened**, then click **Save**.

   NOTE: Only tickets with an **Opened** state can be escalated. See Using the ticket escalation process.
10. In **Priority** tab, create a **Critical** priority with an escalation time of 15 minutes:
    a. In the *Priority Values* section, click the **Add** button: +.

The editable fields appear for the new value.

b. In the *Name* column, type Critical, then in the *Escalation Time* column, select **15 minutes**.

c. Click **Save**.

11. Change the *Escalation Time* for **High** priority to 1 hour, and select the color you want to use to identify high priority tickets.
12. Click the **Save** button at the bottom of the page.

Customizing the User Console home page

You can customize the logo, title, welcome message, announcements, and links that appear on the **User Console** home page to match your company branding, policies, and communication requirements.

Change the User Console logo and text at the System level

If the Organization component is enabled on your appliance, you can change the title, welcome text, and logo of the **User Console** at the System level.

The logos selected at the System level are used for every organization unless you configure the organization settings separately at the Admin level. See Change the User Console logo and login text at the Admin-level.

1. Go to the System-level *General Settings* page:
   a. Log in to the appliance System Administration Console, `http://`**appliance_hostname**`/system`, or select **System** from the drop-down list in the top-right corner of the page.
   b. On the left navigation bar, click **Settings**, then click **Control Panel**.
   c. On the *Control Panel* page, in the **General Settings** section, you can either click **Customize general configurations** and then click the **Login screens and Logos** Or just click **Customize login screens and logos** to open the **Login screens and Logos** page.
2. In the User Console section, customize the text in the following fields:

Option	Description
Title	The heading that appears on the **User Console** login page.
Welcome Message	A welcome note or description of the **User Console**. This text appears following the title on the **User Console** login page.

3. To use custom User Console logo and background color, in the *Login Screen Options* sections, provide the following information.

Option	Description
User Console Login Background Color	Click and use the color chooser to specify the color that you want to appear in the background of the **User Console** login screen. You can select the color using the mouse, or specify the RGB values, as needed. When you close the color chooser, the *HTML Color Code* field on the right displays the HTML code of the selected color. To undo your selection, click **Reset** and start over. **NOTE:** The color chooser is not supported in Internet Explorer 11.
User Console Logo	In each applicable section, click **Choose File**, and specify the graphic file that you want to use as the custom logo in the **User Console**. The supported graphic file formats are `.bmp`, `.gif`, `.jpg`, and `.png`

4. Click **Save and Restart Services**.

The default Home page and a customized version appear in the following figures.

Figure 12. Default logoUser Console Home page

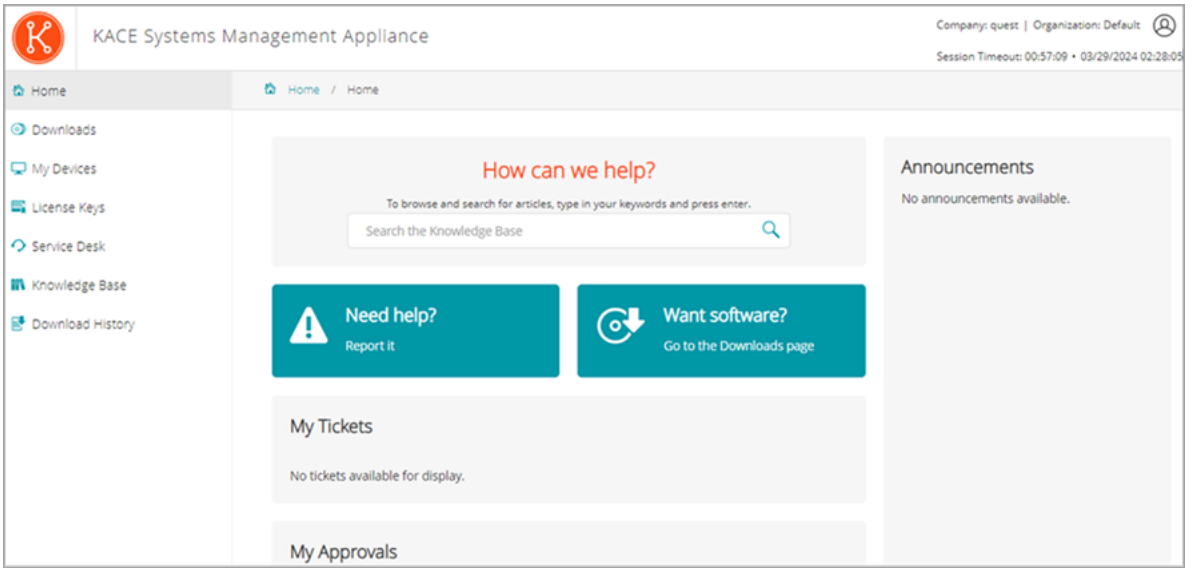


Figure 13. Custom logo onUser Console Home page

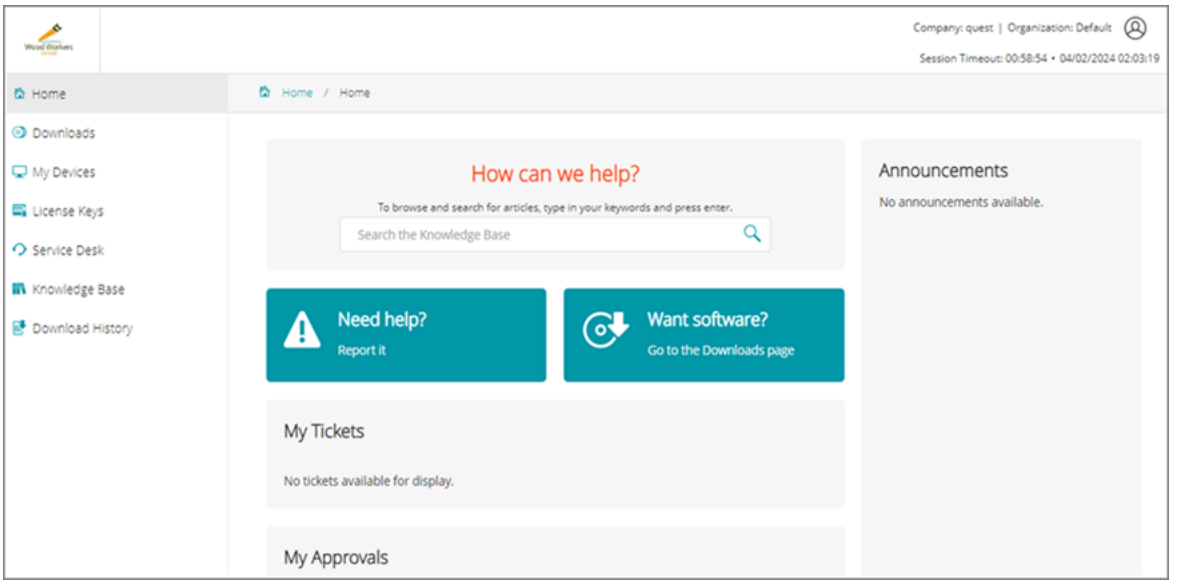


Figure 14. Default report logo

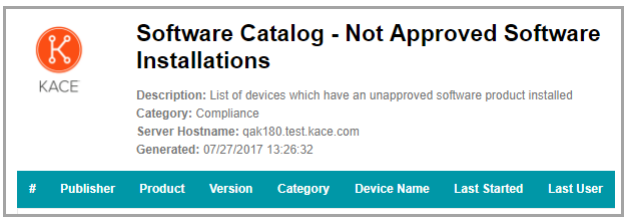
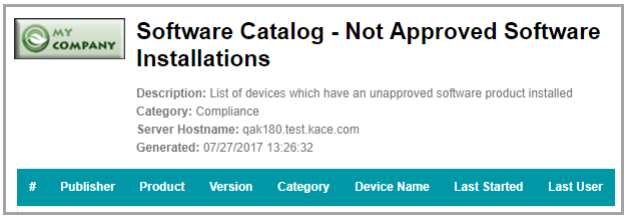


Figure 15. Custom report logo



Change the User Console logo and login text at the Admin-level

You can change the title, welcome text, and logo of the **User Console** to match your company's branding needs.

If the Organization component is enabled on your appliance, you can specify custom logos at the Admin (organization) level as well as the System level. Admin-level logo settings, however, take precedence over System-level logo settings, which enables you to specify different logos for each organization. If you do not select a custom logo for an organization, the System-level setting is used. See Change the User Console logo and text at the System level.

1. Go to the Admin-level *General Settings* page:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`.
   b. On the left navigation bar, click **Settings**, then click **Control Panel**.
   c. On the *Control Panel* page, in the **General Settings** section, you can either click **Customize general configurations** and then click the **Login screens and Logos** Or just click **Customize login screens and logos** to open the **Login screens and Logos** page.
2. In the User Console section, customize the text in the following fields:

NOTE: If the Organization component is enabled on your appliance, these **User Console** settings are available at the System level. See Change the User Console logo and text at the System level.

Option	Description
Title	The heading that appears on the **User Console** login page.
Welcome Message	A welcome note or description of the **User Console**. This text appears following the title on the **User Console** login page.

3. To use custom User Console logo and background color, in the *Login Screen Options* sections, provide the following information.

Option	Description
User Console Login Background Color	Click and use the color chooser to specify the color that you want to appear in the background of the **User Console** login screen. You can select the color using the mouse, or specify the RGB values, as needed. When you close the color chooser, the *HTML Color Code* field on the right displays the HTML code of the selected color. To undo your selection, click **Reset** and start over. **NOTE:** The color chooser is not supported in Internet Explorer 11.
User Console Logo	In each applicable section, click **Choose File**, and specify the graphic file that you want to use as the custom logo in the **User Console**. The supported graphic file formats are `.bmp`, `.gif`, `.jpg`, and `.png`

4. Click **Save and Restart Services**.

The default home page and a customized version appear in the following figures.

Figure 16. Default logoUser Console home page

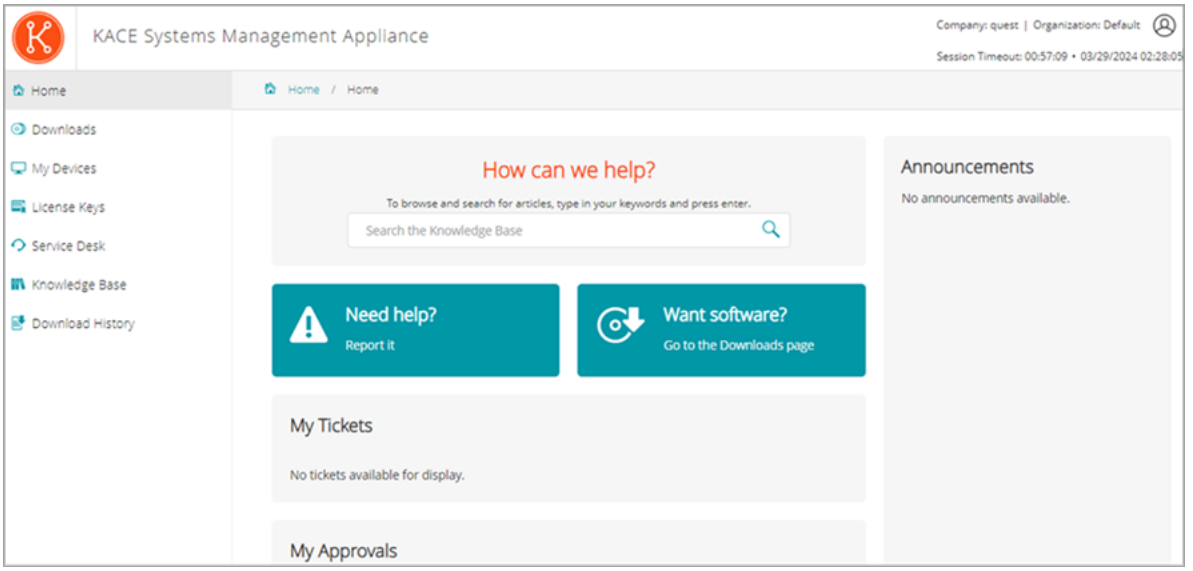


Figure 17. Custom logo onUser Console home page

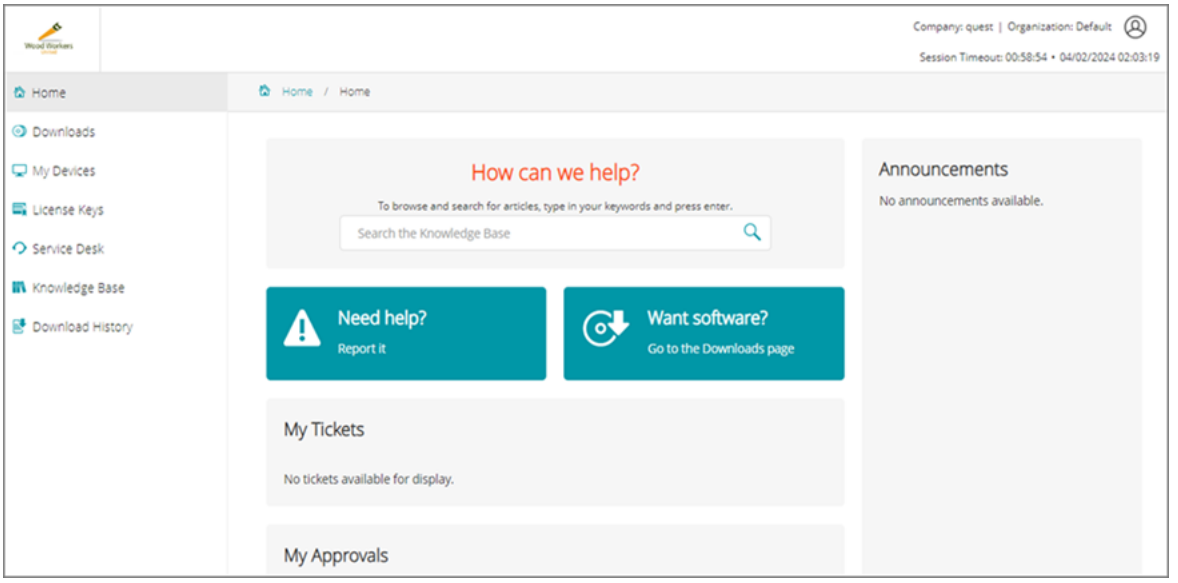


Figure 18. Default report logo

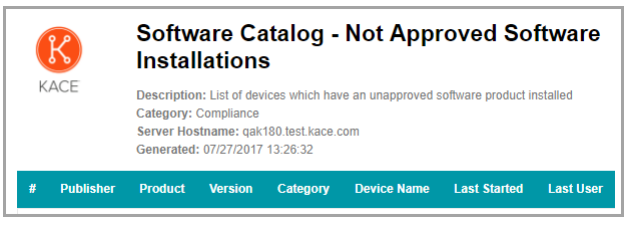
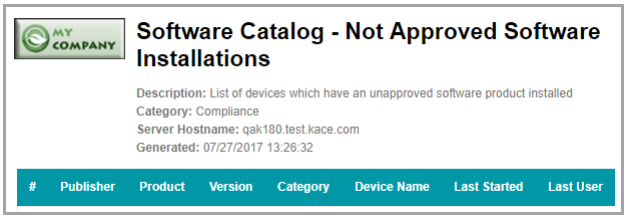


Figure 19. Custom report logo



Show or hide action buttons and widgets on the User Console home page

You can show or hide the action buttons and widgets that appear on the home page of the **User Console**. Action buttons enable users to quickly access the pages where they can file Service Desk tickets and download software through the **User Console**. Widgets enable you to add customized links and announcements to the **User Console** home page.

Action buttons are displayed the **User Console** for each Service Desk globally, regardless of a user's ticket queue permissions. However, if the Organization component is enabled on your system, you manage action buttons and widgets for each organization's Service Desk separately.

1. Go to the *User Console Home Page Settings* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Service Desk**, then click **Configuration**.
    c. On the **Configuration** panel, in the *User Console Home Page* section, click **Configure User Console Home Page**.
2. Select the display options for each item. Select check boxes to show items, clear check boxes to hide items.

Option	Description
Top Panel Widgets • Knowledge Base Search Widget	Show or hide the widgets for: • **Knowledge Base Search**: Searches the links to Knowledge Base articles for the user.
Display Quick Actions • Ticket Quick Action • Downloads Page Quick Action	Show or hide the quick-action links that appear on the **User Console** download page. Text for these links includes: • **Ticket Quick Action**: Have a problem? Report it • **Downloads Page Quick Action**: Want software? Go to the Downloads page **NOTE:** The link text cannot be changed. However, if you change the label for Service Desk tickets, that label is used in this link. For example, if you change your Service Desk to use the label **Incident** instead of **Ticket**, the quick-action link becomes *Incident Quick Action*. See Rename Service Desk titles and labels.
Main Panel Widgets • Tickets Widget • Knowledge Base Widget	Show or hide the widgets for: • **Tickets**: Links to tickets filed by the user and the link, View My Tickets, which takes users to the Tickets list. • **Knowledge Base**: Links to Knowledge Base articles available to the user.

Option	Description
Left Panel Widgets • Helpful Links Widget	Show or hide the widgets for: • **Helpful links**: HTML links to your corporate intranet, wiki, cloud applications, or any other web resource.
Right Panel Widgets • Announcements Widget	Show or hide the widgets for: • **Announcements**: Messages you want to display to the user.

3. Click **Save**.

   Quick Actions and widgets are shown or hidden on the User Console home page immediately. If users are logged in and viewing the User Console home page, the link is displayed when the page is refreshed.

   NOTE: Widgets are empty until announcements, links, or Knowledge Base articles are added.

Add announcements, links, and Knowledge Base articles. See:

- Add, edit, hide, or delete User Console announcements
- Add, edit, or delete custom links on the User Console home page
- Add, edit, or duplicate Knowledge Base articles

Show or hide links to Knowledge Base articles on the User Console home page

You can show or hide links to Knowledge Base articles that appear on the home page of the **User Console**. In addition, you can use labels to show Knowledge Base articles to, or hide them from, different groups of users.

To manage links to Knowledge Base articles, you must create at least one Knowledge Base article. See Add, edit, or duplicate Knowledge Base articles.

To use labels to show or hide Knowledge Base article links, you must create at least one user label. See Add or edit manual labels.

1. Go to the *User Console Home Page Settings* page:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Service Desk**, then click **Configuration**.
   c. On the **Configuration** panel, in the *User Console Home Page* section, click **Configure User Console Home Page**.
2. In the *Main Panel Widgets* section, select the check box next to **Knowledge Base Widget**.
3. Click **Save**.

   The setting is saved and the *Service Desk Configuration* panel appears.
4. To control access to Knowledge Base articles, go to the *Article Detail* page and apply user labels to articles:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Service Desk**, then click **Knowledge Base**.

c. To display the *Article Detail* page, do one of the following:

Click the name of an article.

Select **Choose Action** > **New**.

d. In the *Assign to Labels* section, select the label you want to associate with the article, then click **Save**.

Access to the Knowledge Base article is limited to users with the appropriate label applied.

5. To enable users to view the article, go to the *Users* list and apply the label to user accounts:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Settings**, then click **Users**.
   c. On the *Users* list, select the check boxes next to the users who should be able to view the article.
   d. Select **Choose Action** > **Apply Labels**.
   e. Drag the label associated with the Knowledge Base article into the *Apply these labels* box, then click **Apply Labels**.

Users who have the label applied can access the Knowledge Base article.

Add, edit, hide, or delete User Console announcements

You can add announcements to be displayed on the **User Console** home page, and you can edit, hide, or delete existing announcements as needed.

To display announcements, you must configure Service Desk to show the *Announcements* widget. See Customizing the User Console home page.

Announcements are displayed the **User Console** for each Service Desk globally, regardless of a user's ticket queue permissions. However, if the Organization component is enabled on your system, you manage announcements for each organization's Service Desk separately.

NOTE: The first 140 characters of each announcement are displayed on the **User Console** home page. If announcements exceed 140 characters, a **Show More** link enables users to read the entire announcement.

1. Go to the *User Console Announcements* page:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Service Desk**, then click **Announcements**.
2. To add an announcement, do the following:
   a. Click **Add Announcement**.
   b. Provide the following information:

Option	Description
Message Title	(Required) The title you want to use for the Announcement. **NOTE:** Links cannot be used in the *Message Title* field.
Message Body	(Optional) Any additional information you want to display, including links. This information appears below the title.

Option	Description
	When creating links for announcement messages, use any of these formats: • http://example.com • https://example.com • http://www.example.com • www.example.com
Hidden	(Optional) Whether to show or hide the announcement on the **User Console** home page. This action is useful when you have messages that you want to show or hide periodically, such as announcements about system status or planned maintenance. Select the check box to hide the announcement. Clear the check box to show the announcement.
Restrict to Labels	(Optional) The user labels to which the announcement applies. If you select a label, the announcement is displayed to users only if the label is applied to their user account. This action is useful if you want to display announcements to groups of users, such as users located in different geographic locations, and you have created and applied labels for those users.

c. Click **Save**.

If the Announcements widget is enabled for Service Desk, the Announcement appears on the User Console Home page according to the settings you selected.

3. To edit an announcement, click **Edit** under the announcement title, then click **Save**.

The changes appear on the User Console home page immediately. If users are logged in and viewing the User Console home page, the announcement is deleted when the page is refreshed.

4. To hide an announcement:
   a. Click **Edit** under the announcement title.
   b. Select the check box next to *Hidden*.
   c. Click **Save**.

The announcement is hidden from the User Console home page immediately. If users are logged in and viewing the User Console home page, the announcement is hidden when the page is refreshed.

5. To change the priority of an announcement, use the drag icon on the left side of the announcement. See Prioritize User Console announcements or mark an announcement as urgent.

The announcement is hidden from the User Console home page immediately. If users are logged in and viewing the User Console home page, the announcement is hidden when the page is refreshed.

6. To delete an announcement, click **Delete** under the announcement title, then click **Yes** in the confirmation window.

The announcement is removed from the User Console home page immediately. If users are logged in and viewing the User Console home page, the announcement is deleted when the page is refreshed.

Prioritize User Console announcements or mark an announcement as urgent

You can set the order in which announcements appear on the **User Console** home page. In addition, you can display an urgent announcement in a highlighted banner to increase its visibility.

To prioritize announcements, you must configure Service Desk to show the *Announcements* widget and you need to add announcements. See:

- Show or hide action buttons and widgets on the User Console home page
- Add, edit, hide, or delete User Console announcements

1. Go to the *User Console Announcements* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Service Desk**, then click **Announcements**.
2. To prioritize announcements, use the drag icon on the left side of the announcement as follows:
    # To change an announcement's priority, drag it up or down in the list. Announcements are displayed on the **User Console** home page in the order shown on the *User Console Announcements* page.
    # To set an announcement as urgent, drag it into the *Urgent Announcement* box. The urgent announcement appears in a banner at the top of the **User Console** home page.

    NOTE: Only one announcement can appear in the *Urgent Announcement* banner at a time.

    # To change the urgent announcement, drag a different announcement into the *Urgent Announcement* box.
    # To change an urgent announcement to a regular announcement, drag it out of the *Urgent Announcement* box.

    The announcements are prioritized accordingly on the User Console home page immediately. If users are logged in and viewing the User Console home page, the announcement priority is updated when the page is refreshed.

Add, edit, or delete custom links on the User Console home page

You can add custom links to be displayed on the **User Console** home page, and you can edit or delete existing custom links as needed.

To display custom links, you must configure Service Desk to show the *Helpful Links* widget. See Customizing the User Console home page.

Custom links are displayed the **User Console** for each Service Desk globally, regardless of a user's ticket queue permissions. However, if the Organization component is enabled on your system, you manage custom links for each organization's Service Desk separately.

1. Go to the *User Console Home Page Links* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Service Desk**, then click **Configuration**.
    c. On the **Configuration** panel, in the *User Console Home Page* section, click **Define Helpful Links**.
2. To add a link:
    a. Click +.
    b. Provide the following information:

Option	Description
Title	The text to display as the link text. You can use the URL itself, or any text string.

Option	Description
URL	The URL of the link. Acceptable link formats include: • http://example.com • https://example.com • http://www.example.com **NOTE:** You cannot use the same URL in more than one link.

c. Click **Save** at the right of the *URL* field, then click **Save** at the bottom of the page.

The link appears on the User Console home page immediately. If users are logged in and viewing the User Console home page, the link is displayed when the page is refreshed.

3. To edit a link:
   a. Click .
   b. Change the *Title* or *URL* as needed.
   c. Click **Save** at the right of the *URL* field, then click **Save** at the bottom of the page.

The change appears on the User Console home page immediately. If users are logged in and viewing the User Console home page, the link is displayed when the page is refreshed.

4. To change the order in which links are displayed on the User Console home page:
   a. Drag the link up or down in the list using .
   b. Click **Save** at the bottom of the page.

The change appears on the User Console home page immediately. If users are logged in and viewing the User Console home page, the link order is changed when the page is refreshed.

5. To delete a link:
   a. Click .
   b. In the dialog window, click **Yes**.
   c. Click **Save** at the right of the *URL* field, then click **Save** at the bottom of the page.

The link is deleted from the User Console home page immediately. If users are logged in and viewing the User Console home page, the link is deleted when the page is refreshed.

Add ticket links to the User Console home page

You can configure Service Desk to automatically add links to a user's tickets on the **User Console** home page. This link enables users to access ticket details with a single click.

Ticket links appear only if the user has created at least one ticket.

1. Go to the *User Console Home Page Links* page:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Service Desk**, then click **Configuration**.
   c. On the **Configuration** panel, in the *User Console Home Page* section, click **Configure User Console Home Page**.
2. In the *Main Panel Widgets* section, select the check box next to **Tickets Widget**.
3. Click **Save**.

The setting is saved and the *Service Desk Configuration* panel appears. The User Console home page shows tickets filed by the user, and a My Tickets link, which takes users directly to the *Tickets* page.

NOTE: If the user has not created any tickets, the *Tickets* widget appears with a note stating that no tickets are available for display.

Add a quick-action link for reporting problems on the User Console home page

You can add a quick-action link to the *New Ticket* page on the **User Console** home page. This enables users to access the new ticket form with a single click.

1. Go to the *User Console Home Page Settings* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Service Desk**, then click **Configuration**.
    c. On the **Configuration** panel, in the *User Console Home Page* section, click **Configure User Console Home Page**.
2. In the *Display Quick Actions* section, select the check box next to **Ticket Quick Action**.
3. Click **Save**.

    The setting is saved and the *Service Desk Configuration* panel appears. The *Have a problem? Report it* button appears on the User Console home page. When users click this button, the *New Ticket* page appears.

About the session timeout period

By default, the appliance automatically logs users out of the **Administrator Console** or **User Console** after one hour of inactivity. This is referred to as the **Session Timeout**.

Sessions are restarted at every server interaction, such as reloading the current page, saving changes, or moving to a new page. If the Session Timeout period elapses without any interaction, any unsaved changes are lost, and the login page appears. The Timeout Session counter appears in the upper right of each console.

For instructions on changing the Session Timeout, see:

- Configure appliance General Settings with the Organization component enabled
- Configure appliance General Settings without the Organization component

Using the Satisfaction Survey

The Satisfaction Survey enables Service Desk ticket submitters to provide feedback on the handling of tickets.

If the Satisfaction Survey is enabled, an email message describing the survey is sent to submitters immediately when a ticket is closed. This email message uses the **Ticket Closed** email template.

By default, the survey is visible to submitters when they access a closed ticket for the first time, and thereafter until the survey is completed. After the survey is completed, it is hidden. Survey scores and comments are stored in the ticket and are not editable by the Service Desk staff.

You can run various reports to display and analyze survey data using Service Desk reports. In addition, you can change the *Ticket Closed* email template that describes the survey, change the survey label, or prevent the survey from being displayed. See:

- Run Service Desk reports
- Configure email templates
- Change the Satisfaction Survey label
- Remove the Satisfaction Survey field from tickets

Changing the Satisfaction Survey default behavior

The satisfaction survey can be modified by changing the default prompt in the survey box, or it can be removed and not shown to the ticket submitter.

Change the Satisfaction Survey label

The Satisfaction Survey introduction label can be modified to suit your needs.

1. Go to the Service Desk *Queue Detail* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Service Desk**, then click **Configuration**.
    c. On the **Configuration** panel, in the **Queue** section, click **Modify configurations and preferences**. Now in **General** tab, select **Customize Queue Fields** or in the **Queue** section, click **Customize Fields** to display the *Queue Customization* page.
2. In the *Default Fields* tab, click the **Edit** button in the *SAT_SURVEY* row:
3. In the *Label* section, type the new label for the survey box.
4. Click the **Save** button to the right of the item.
5. Click the **Save or Apply Changes** button at the bottom of the page.

Remove the Satisfaction Survey field from tickets

You can prevent the Satisfaction Survey from being displayed to ticket submitters.

1. Go to the Service Desk *Queue Detail* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Service Desk**, then click **Configuration**.
    c. On the **Configuration** panel, in the **Queue** section, click **Modify configurations and preferences**. Now in **General** tab, select **Customize Queue Fields** or in the **Queue** section, click **Customize Fields** to display the *Queue Customization* page to display the *Queue Customization* page .
2. In the *Default Fields* tab, click the **Edit** button in the *SAT_SURVEY* row:
3. In the *Permissions* section, select **Hidden** in the drop-down list.
4. Click the **Save** button to the right of the item.
5. Click the **Save** button at the bottom of the page.

    The Satisfaction Survey is disabled, and it is no longer presented to ticket submitters when tickets are closed.

Enable or disable security for Service Desk attachments

You can enable or disable security for Service Desk attachments to prevent files from being accessed from outside the **Administrator Console** or **User Console**.

By default, security for Service Desk attachments is enabled. Disable this feature if you want users to be able to access ticket attachments through ticket links outside the **Administrator Console** or **User Console**. Also, security settings for Service Desk attachments are appliance-level settings. If the Organization component is enabled on your system, the settings you select apply to all organizations.

1. Go to the appliance *Control Panel*:
   - **If the Organization component is not enabled on the appliance, log in to the appliance Administrator Console, `https://appliance_hostname/admin`, then select Settings > Control Panel.**
   - **If the Organization component is enabled on the appliance, log in to the appliance System Administration Console, `https://appliance_hostname/system`, or select System in the drop-down list in the top-right corner of the page, then select Settings > Control Panel.**
2. Click **Security Settings** to display the *Security Settings* page.
3. In Security Options, in the *Secure Service Desk attachments* section, choose whether to add security for files that are attached to Service Desk tickets:
   - **Select the check box to enable security for files attached to tickets. If you choose this option, users can access files attached to tickets only from within the appliance Administrator Console or User Console.**
   - **Clear the check box to enable users to access files by clicking ticket links from outside the Administrator Console or User Console.**
4. Click **Save and Restart Services** to save changes and restart the appliance.

Using the Service Desk Dashboard

The Service Desk Dashboard provides an overview of Service Desk tickets for the selected organization (if applicable), or the appliance.

If the Organization component is enabled on the appliance, and you are logged in to the Administrator Console (`http://`**appliance_hostname**`/admin`), the *Service Desk Dashboard* shows information for the selected organization. When you are logged in to the System Administration Console (`http://`**appliance_hostname**`/system`), this dashboard shows information for the appliance, including all organizations.

You can access the *Service Desk Dashboard* if one or more roles associated with your user account grants access to this dashboard. If you want to hide it, edit your user roles, as needed. For more information, see Add or edit User Roles.

TIP: The appliance updates the summary widgets periodically. To update most of the widgets any time, click the icon and then the **Force Refresh** button. To update an individual widget, hover over the widget, then click the **Refresh** button above the widget. Some widgets may require additional steps.

About the Service Desk Dashboard widgets

Service Desk Dashboard widgets provide overviews of Service Desk tickets for the organization or appliance, as selected.

This section describes the widgets available on the *Service Desk Dashboard*. If the Organization component is enabled on your appliance, the widgets show the information for the selected organization at the Admin level and for the appliance at the System level.

This dashboard provides a high-level overview of your device usage. Use it to quickly review the state of your devices and look for any indicators that can improve your ticket management. For example, you can see the numbers of active or overdue tickets per owner.

The title, chart type, and grouping of items in some widgets can be updated. The grouping options vary slightly between these widgets.

Widget	Description
Shortcuts	This widget contains links to common Service Desk actions. Use them to quickly initiate specific tasks, such as creating a new KB (Knowledge Base) article, scheduling a report, and so on.
Views	This widget contains links to common Service Desk pages and wizards, including any custom views that you created. Use them to quickly navigate to specific pages, such as *My Recent Tickets*, *All Unassigned Tickets*, and *Tickets Due Today*. It also displays link to custom views, as applicable. The list of custom views is sorted alphabetically. If you want the custom views to appear in a specific order, you can prefix their names with numbers, as needed.
Reports	This widget contains links to common Service Desk reports. Use them to quickly generate a specific report, such as *Open Tickets last 7 days by Owner*, *Stalled/Open Tickets by Owner*, and others.
Tickets Opened Today	This widget contains the number of Service Desk tickets that were opened today.
Active Tickets By Owner Active Tickets By Category Active Tickets By Priority Active Tickets Closed Tickets Overdue Tickets Overdue Tickets By Owner Overdue Tickets Today Tickets Due Today Reopened Tickets	These widgets display the numbers of active, closed, overdue, overdue today, due, due today, or reopened Service Desk tickets, grouped into any of the following categories: • Category • Priority • Owner • Queue • Range The resulting data can appear in a *Bar Chart* or a *Donut Chart*. To change the widget title, choose how you want to group the tickets, or select the chart type, click in the widget. In the dialog box that appears, make your edits and click **Save**.

Widget	Description
Average Ticket Resolution Time	This widget displays the average number of days the ticket resolution takes over that last 30 days, grouped into any of the following categories: • Category • Priority • Owner • Queue • Month The resulting data can appear in a *Bar Chart* or a *Doughnut Chart*. To change the widget title, choose how you want to group the tickets, or select the chart type, click in the widget. In the dialog box that appears, make your edits and click **Save**.
Overdue Tickets Count	This widget displays the number of Service Desk tickets that are currently overdue.

Customize the Service Desk Dashboard

You can customize the Service Desk Dashboard to show or hide widgets as needed.

These widgets are also all available in the Home dashboard, if they are installed.

1. Go to the *Service Desk Dashboard*.
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Service Desk**, then click **Dashboard**.
2. Hover over the widget, then use any of the following buttons:
   # : Refresh the information in the widget.
   # : Display information about the widget.
   # : Edit the widget.
   # : Remove the widget.
   # : Resize the widget.
   # : Drag the widget to a different position on the page.
3. The widgets are editable, allowing you to filter the information that they display. To edit a widget, click and in the dialog box that appears, provide the required information. You can edit the chart type. Based on the chart type you select here from the drop down list, the relevant fields populate.
4. Click the button in the top-right corner of the page to view the list of available widgets.

   For information on how to add widgets to the dashboard refer Adding Widget to Service Desk Dashboard

Work with Service Desk Dashboard

When you click the icon, the dashboard settings panel displays. You get to see the following options:

Dashboard Name	Description
Dashboard Settings	You can customize the look and feel of the widgets. For more information, refer Setting a Service Desk Dashboard
Add Widget	You can add a new widget. For more information, refer Adding Widget to Service Desk Dashboard
Email Dashboard	You can share a dashboard snapshot through email. For more information, refer Emailing a Service Desk Dashboard
Force Refresh	You can refresh all the widget data on the dashboard. For more information, refer to Refreshing Service Desk Dashboard Data Manually

Setting a Service Desk Dashboard

You can customize the look and feel of the widgets and the dashboards.

You can change the color used in the dashboard charts, edit the dashboard name and its description, change the display of the widgets.

To customize a dashboard,

1. Click the icon to open the Dashboard Settings panel.
2. Make changes to the fields as required:

Fields	Description
Name	Add/Edit name for the dashboard. This is displayed on the dashboard.
Description	Add/Edit description of the dashboard. This describes the dashboard.
Choose Your Colors	Click on the color selector to choose your dashboard chart colors. Drag and drop the colors to arrange them in the desired order. The colors at the top of the list will be used first by each chart.
Layout	Chose one of the layout options. The widgets and other elements are displayed in the selected layout.

3. Click **Save**.

   The changes gets reflected on the dashboard.

Adding Widget to Service Desk Dashboard

You can add widgets to the Dashboard.

There is a list of widgets in the panel. You can enter a keyword in the Search text box to refine the list, then click on your selection.

To add widgets to the dashboard,

1. Click the icon to open the **Add Widget** panel.
2. Search for the desired widget in the following ways:
   - **In the Sort By drop-down, select the widget by title or newest.**
   - **In the Search field, enter a keyword to refine the list.**

   The refined result displays.
3. Click the desired widget.

   The widget gets added to the dashboard.

Emailing a Service Desk Dashboard

You can share a dashboard snapshot through email, send it to multiple users, and configure the frequency of email.

To email a dashboard,

1. Click the icon to open the dashboard settings panel.
2. Click the Email Dashboard option to open the Email Dashboard panel.
3. Select appropriate option from the given options:
   a. **Send Now**: You can send an email immediately.
   b. **Schedule**: You can set the frequency of sending a snapshot of dashboard through email.

The detailed steps for each option are given below:

Send email now

To send email immediately,

1. Click **Send Now** to open the Email Dashboard dialog.
2. Enter details in the Email Address, Subject, and Message fields.
3. Choose the layout in which you want the widgets to appear.
4. Click Send.

The dashboard is sent through email.

Schedule

To set the frequency of sending a snapshot of dashboard through email,

1. Click **Schedule** to open the Schedule dialog.
2. Enter details in the Subject and **Message** fields.
3. Choose the layout in which you want the widgets to appear.
4. To add recipients, select the names from the **Select user to add drop down list**.

   NOTE: You can add multiple recipients from the list.
5. Select the frequency from the drop down list.
6. In the **Next Run** field that appears after you select the **Frequency**, set the date, month, and time for the next email delivery.
7. Click Save. The dashboard is sent through email according to the set schedule.

Refreshing Service Desk Dashboard Data Manually

To update the widgets,

1. Click the icon to open the dashboard settings panel.
2. Click **Force Refresh** to open the Confirm dialog box.
3. Click Yes to confirm refresh all widget data on the dashboard.

Managing Service Desk tickets, processes, and reports

You manage Service Desk tickets, processes, and reports using the **Administrator Console**. Tickets can also be managed using the **User Console** and through email.

Before you can manage tickets, you must configure the Service Desk. See Setting up Service Desk.

Overview of Service Desk ticket lifecycle

Service Desk tickets progress through several stages during their lifecycle.

These stages include:

1. The ticket is submitted, either through the User Console, the Administrator Console, or through email. See Creating tickets from the Administrator Console and User Console and Creating and managing tickets by email.
2. The ticket is assigned to an owner according to the ticket rules. See Configuring ticket settings and Using Ticket Rules.
3. The ticket owner reviews the ticket, adjusts the impact if necessary, and assigns a priority.
4. If Service Level Agreements are enabled on the queue where the ticket resides, the ticket due date is calculated based on the priority.
5. If the issue is straightforward, the owner resolves and closes the ticket, and email notifications are sent. See Configuring email settings.
6. If the ticket is complex, the ticket might stay open for a period of time and have multiple owners.
7. If the owner is unable to resolve the ticket within its escalation time limit, the ticket is escalated. See Using the ticket escalation process.
8. When tickets are closed, users can complete a satisfaction survey to provide feedback about the way the ticket was handled. See Using the Satisfaction Survey.
9. The ticket is archived. See Archiving, restoring, and deleting tickets.

Creating tickets from the Administrator Console and User Console

You can create Service Desk tickets from either the **Administrator Console** or the **User Console**.

Tickets can also be created using email. See Creating and managing tickets by email.

Create tickets from the User Console

You can create Service Desk tickets using the **User Console**.

When you create tickets from the **User Console**, your user information is automatically added to the *Submitter* field on the *New Ticket* page.

1. Go to the User Console *New Ticket* page:
    a. Go to the User Console: `http://`**appliance_hostname**`/user` where **appliance_hostname** is the hostname of your appliance.
    b. On the left navigation bar, click **Service Desk**, then click **Tickets**.
    c. To display the *New Ticket* page for **Queue** option> **All Queue**, do one of the following:
    # Select **Choose Action** > **New Ticket From Queue** > **Queue name**.

    If you have a high number of queues, use the search box to quickly find a specific queue.

    # Select **Choose Action** > **New Ticket From Queue** > **Queue name** > **Ticket Template name**
    # Select **Choose Action** > **New Ticket From Process** > **Process name**.
2. If you are creating a new ticket from a process, and the process template is configured to display the process description page, review the information on the description page that appears, and click **Continue**.

    This page typically displays some important pre-requisites that you need to complete before proceeding to create a ticket. For example, if the process template defines how to add a new employee to the system, you can to instruct the users to verify if the employee acquisition process is complete and if the employee ID is created. For more information on how to create and configure process templates, see Add, edit, and enable process templates.
3. **Queue-based and process tickets only**. Provide the following information:

Option	Description
Title	(Required) A brief description of the issue. If the associated Service Desk queue displays this field, a few moments after you stop typing, a list of Knowledge Base articles appears, associated with the information you provide in this field. The suggested articles can help you find out more about the issue you are encountering and to resolve your problem before creating a Service Desk ticket.
Summary	A more detailed description of the issue. This field includes a full range of text editing options for formatting your content, such as buttons for bold text, hyperlinks, lists, or text color. For example: • To apply bold text to a text string, select it in the editor, and click B. • To add images, click, and provide the URL to the image file. # Any images you include this way will not be added as file attachments to the ticket. # Deleting an image from the text field will permanently remove it as the image in this field is not stored as an attachment. • To add external links, click. • To embed externally hosted videos, click.
Submitter	The login name of the user submitting the ticket. To change the submitter, select a different login name in the drop-down list.

Option	Description
Impact	The number of people that are inconvenienced or cannot work.
Category	A classification of the issue.
Attachments	Files that you want to add to the ticket. You can paste up to five files. See Add or delete screen shots and attachments from Service Desk tickets.
Screenshots	Screenshots that you want to add to the ticket. You can paste up to five screenshots to a ticket. See Add or delete screen shots and attachments from Service Desk tickets.

4. **Template-based tickets only.** Provide the information about this ticket. Ticket fields are defined in the associated ticket template.

   For more information about ticket templates, see Configure a ticket template.

5. Do one of the following:

   # Click **Save** to save the ticket and return to the *Ticket* list.

   # Click **Apply Changes** to save the ticket and continue editing it.

   # Click **Cancel** to discard the ticket changes.

   If other users have modified the ticket concurrently, the *Update Notification* dialog appears, provided that the dialog is enabled for the queue and you are the ticket owner or an administrator. This dialog is displayed to administrators and ticket owners only. It is not displayed to other users. Administrators can enable or disable the conflict warning message for each queue separately. See Enable or disable the conflict warning.

Create tickets from the Administrator Console Ticket page

You can create Service Desk tickets from the **Administrator Console** *Ticket* page as needed.

When you create tickets from the **Administrator Console** *Ticket* page, your user information is automatically added to the *Submitter* field of the *New Ticket* page.

1. Go to the Service Desk *New Ticket* page:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Service Desk**, then click **Tickets**.
   c. To display the *New Ticket* page, do one of the following:

   # Select **Choose Action** > **New**.

   # Select **Choose Action** > **New Ticket From Queue** > **Queue name**.

   If you have a high number of queues, use the search box to quickly find a specific queue.

   # Select **Choose Action** > **New Ticket From Queue** > **Queue name** > **Ticket Template name**

   # Select **Choose Action** > **New Ticket From Process** > **Process name**.

2. If you are creating a new ticket from a process, and the process template is configured to display the process description page, review the information on the description page that appears, and click **Continue**.

   This page typically displays some important pre-requisites that you need to complete before proceeding to create a ticket. For example, if the process template defines how to add a new employee to the system, you can to instruct the users to verify if the employee acquisition process

is complete and if the employee ID is created. For more information on how to create and configure process templates, see Add, edit, and enable process templates.

3. **Queue-based and process tickets only**. Provide the following information:

Option	Description
Title	(Required) A brief description of the issue.
Summary	A more detailed description of the issue. This field includes a full range of text editing options for formatting your content, such as buttons for bold text, hyperlinks, lists, or text color. For example: • To apply bold text to a text string, select it in the editor, and click B. • To add images, click, and provide the URL to the image file. # Any images you include this way will not be added as file attachments to the ticket. # Deleting an image from the text field will permanently remove it as the image in this field is not stored as an attachment. • To add external links, click. • To embed externally hosted videos, click.
Submitter	The login name of the user submitting the ticket. The submitter can be changed by selecting a different login name in the drop-down list. To view the submitter contact information, click. If you are creating or editing a child ticket from a process template, you also have an option to set this field to the *Parent Owner* or the *Parent Submitter* of the associated parent ticket.
Asset	The asset that the information in the ticket is about. Select an asset in the drop-down list. To view the asset details, click.
Filter on submitter assigned assets	Filter the asset list based on the assets that are assigned to the submitter. This check box is selected by default.
Device	The device that the information in the ticket is about. If any devices are assigned to the ticket submitter, they are listed here, with the submitter's primary device selected by default. Select a device in the drop-down list, as needed. To view the device details, click.
Filter on submitter assigned devices	Filter the device list based on the devices that are assigned to the submitter. If any devices are assigned to the ticket submitter, this option appears selected by default on this page. However, when you open this ticket on the *Ticket Detail* page, this option is not selected, and the Device field shows the device selected when the ticket was first created. This is default behavior. Leaving this check box cleared prevents you from accidentally selecting a device that may not be related to the issue associated with the ticket.
Impact	The number of people that are inconvenienced or cannot work.
Category	A classification of the issue.

Option	Description
Status	The current state of the ticket. This field does not appear if you are creating or editing a ticket from a process template.
Priority	The importance of priority of the ticket.
Owner	The user responsible for managing the ticket through its lifecycle. If you are creating or editing a child ticket from a process template, you also have an option to set this field to the *Parent Owner* or the *Parent Submitter* of the associated parent ticket. **TIP:** To quickly assign a ticket to yourself, on the *Tickets* list page, click in the row containing the ticket.
Due	Date and time the ticket is scheduled to be completed. If Service Level Agreements are not enabled, the due date is set to None, by default. If Service Level Agreements are enabled, the due date is automatically calculated according to the SLA settings. The due date is calculated based on the priority set when the ticket is submitted. If the priority is changed after the ticket is initially submitted, the calculated due date will be recalculated according to the new priority but based on the original submitted date and time. If the SLA resolution time configuration is changed, it is only applicable on new tickets. Old tickets are not affected. See Configuring Service Level Agreements. Select **Manual Date** to manually set the due date and time. In this case, if Service Level Agreements are enabled, the due date and time is calculated and displayed as an option, but not selected.
CC List	A list of users who receive a notification email when a ticket event occurs. The CC List is emailed based on the ticket event and **Ticket CC** being configured for the queue **Email on Events** configuration.
Resolution	The resolution of the issue associated with the ticket. This field includes a full range of text editing options for formatting your content, such as buttons for bold text, hyperlinks, lists, or text color. For example: • To apply bold text to a text string, select it in the editor, and click B. • To add images, click , and provide the URL to the image file. # Any images you include this way will not be added as file attachments to the ticket. # Deleting an image from the text field will permanently remove it as the image in this field is not stored as an attachment. • To add external links, click . • To embed externally hosted videos, click .
Predefined Response	If you want to add an automatic response as a resolution to this ticket, click **Predefined Response** and select a response template. The selected response template appears in the **Resolution** field. You can add multiple response templates as resolution entries. They appear in the order you selected them.

Option	Description
	TIP: To create or edit a response template, save your changes and click **Manage**. This will take you to the *Response Templates* page. For more information about response templates, see View and edit response templates.
Related Ticket Information	This section does not appear if you are creating a ticket from a process template.
Add Ticket	Click to add an additional ticket to this ticket's related information.
Referrers	The **Referrer** is a read-only field that holds a ticket reference to any ticket that references this ticket by way of the **See also** section.
Merged Tickets	This section allows you to edit the list of tickets merged with this ticket, as applicable. Any tickets that you want to merge must belong to the same queue. When you merge tickets using the *Ticket Detail* page, the open ticket becomes the primary ticket. All other merged tickets are archived when you merge them. For more details, see Merging tickets. To add a merged ticket, click **Add Tickets to Merge/Edit Merged Tickets**, and select a ticket from the list that appears.
Process Information	This section only appears if you are creating a ticket from a process template. All of the settings appearing in this section are read-only. For complete information about creating and configuring process templates, see Add, edit, and enable process templates.
Process	The name of the process template associated with this ticket.
Process Type	The type of the process. In a default installation, only the *Service Desk* and *Software Request: Approval Required* process types are included. You can create new process types, as required. For example, you can create a process type for accessing a specific application, or a group of applications. For more information, see Define process types.
Process Status	The status of the workflow associated with this process template. For example, *Pending Approval*.
Parent	The name of the parent ticket, as defined in the process template associated with this ticket.
Process Approvals	A list of users that are assigned as approvers for this ticket, if applicable. • If all approvals for the ticket are received, this section appears collapsed by default. To review them, click **Expand**. • If one or more approvals are pending for this ticket, this section is displayed. To hide it, click **Collapse**. The approvers are listed in stages, as defined in the process template. Each stage can have one or more approvers, as needed. The settings related to each approver and stage are also listed in this section, such as approval timeouts and notifications. When you create a process ticket, the timeout period starts for the first approver. When that user approves the ticket, the timeout starts for the next one, and so on. If the process template associated with this process indicates that the ticket submitter's manager is an approver for one or more stages, and the logged-on user

Option	Description
	has a manager's account associated with it, the manager's user name appears in the list. If the logged on user account is not associated with a manager, and the associated process template specifies that the submitter's manager must approve the related process tickets, an error is displayed when you attempt to save the ticket. However, if the submitter's managers is just one of the approvers, the *Process Approvals* section lists the other approvers, and you can save the ticket without any errors being displayed.
Process Activities	A list of process activities, each representing a child ticket, and listed in stages, as defined in the process template. Multiple tickets can be assigned to the same stage, if needed. For example, if the first stage is to obtain equipment and supplies for a new-hire, you can have several separate child tickets for ordering devices, office equipment, and supplies, all assigned to stage 1. When you create a process ticket, all child tickets assigned to stage 1 are created automatically. Stage 2 tickets are created when all stage 1 tickets are closed, stage 3 tickets are created when all stage 2 tickets are closed, and so on. If any of the approvals times out, none of the child tickets related to that or any subsequent stages are created.
Add Ticket	Click to add an additional ticket to this ticket's related information.
Referrers	The **Referrer** is a read-only field that holds a ticket reference to any ticket that references this ticket by way of the **See also** section.
Comments	Comments that you want to add to the ticket. You can also add file attachments, screenshots, provide automatic responses or Knowledge Base article contents as ticket comments. For more information see: • Add comments to tickets • Add or delete screen shots and attachments from Service Desk tickets If you want to add an automatic response as a resolution to this ticket, click **Predefined Response** and select a response template. The selected response template appears in the **Resolution** field. You can add multiple response templates as resolution entries. They appear in the order you selected them. **TIP:** To create or edit a response template, save your changes and click **Manage**. This will take you to the *Response Templates* page. For more information about response templates, see View and edit response templates.
Knowledge Base Article	Look up a Knowledge Base article and append its contents to the ticket comments. For more information about Knowledge Base articles, see Managing Knowledge Base articles.

4. **Template-based tickets only.** Provide the information about this ticket. Ticket fields are defined in the associated ticket template.

   For more information about ticket templates, see Configure a ticket template.

5. Do one of the following:

   # Click **Save** to save the ticket and return to the *Ticket* list.

   # Click **Apply Changes** to save the ticket and continue editing it.

   # Click **Cancel** to discard the ticket changes.

If other users have modified the ticket concurrently, the *Update Notification* dialog appears, provided that the dialog is enabled for the queue and you are the ticket owner or an administrator. This dialog is displayed to administrators and ticket owners only. It is not displayed to other users. Administrators can enable or disable the conflict warning message for each queue separately. See Enable or disable the conflict warning.

6. Review any changes reported in the *Update Notification* dialog:

Option	Description
Their Change(s)	A summary of the changes that were submitted by other users during the time that you were editing the ticket.
Your Change(s)	A summary of the changes you are submitting for the same fields listed in the *Their Changes* column. These changes might conflict with the changes submitted by other users. **NOTE:** The dialog summarizes all changes made by other users. However, your changes are summarized only if they conflict with changes made by other users. Also, if a different user has modified a field, such as *Category* and you have not modified that field, the change appears in the *Modified!* section. The *Your Changes* column displays - -, which indicates that you have not modified the content, and the other user's changes will be preserved.
Conflict!	Changes that are contradictory. For example, if you changed the ticket *Category* to **Software**, and a different user changed the *Category* to **Network**, the changes would be summarized in the *Conflict!* section.
Modified!	A summary of the changes that do not conflict. For example, if you added information to the ticket *Summary* and a different user changed the **Impact**, each of the changes would be summarized in the *Modified!* section.

7. Do one of the following:
   - # Click **Save** to save the ticket and return to the *Ticket* list.
   - # Click **Apply Changes** to save the ticket and continue editing it.
   - # Click **Cancel** to discard the ticket changes.

If other users have modified the ticket concurrently, the *Update Notification* dialog appears, provided that the dialog is enabled for the queue and you are the ticket owner or an administrator. This dialog is displayed to administrators and ticket owners only. It is not displayed to other users. Administrators can enable or disable the conflict warning message for each queue separately. See Enable or disable the conflict warning.

8. Review any changes reported in the *Update Notification* dialog:

Option	Description
Their Change(s)	A summary of the changes that were submitted by other users during the time that you were editing the ticket.
Your Change(s)	A summary of the changes you are submitting for the same fields listed in the *Their Changes* column. These changes might conflict with the changes submitted by other users. **NOTE:** The dialog summarizes all changes made by other users. However, your changes are summarized only if they conflict with changes made by other users. Also, if a different user has modified a field, such as *Category* and you have not modified that field, the change appears in the *Modified!* section. The *Your Changes* column displays - -, which indicates that you have not modified the content, and the other user's changes will be preserved.
Conflict!	Changes that are contradictory. For example, if you changed the ticket *Category* to **Software**, and a different user changed the *Category* to **Network**, the changes would be summarized in the *Conflict!* section.
Modified!	A summary of the changes that do not conflict. For example, if you added information to the ticket *Summary* and a different user changed the **Impact**, each of the changes would be summarized in the *Modified!* section.

9. In the *Update Notification* dialog box, do one of the following:
   - Click **Keep Your Changes** to save changes you have made. This option appears when your changes do not conflict with the changes made by other users.

     NOTE: If a different user has modified a field, such as *Category* and you have not modified that field, the change appears in the *Modified!* section. The *Your Changes* column displays - -, which indicates that you have not modified the content, and the other user's changes will be preserved.
   - Click **Overwrite Conflicts** to save changes you have made to the ticket. For any changes marked as **Conflict!**, your changes overwrite the changes made by other users.
   - Click **Cancel** to return to the *Ticket Detail* page and continue editing the ticket.

Create tickets from the Device Detail page

You can create Service Desk tickets for devices from the *Device Detail* page as needed.

When you create Service Desk tickets from the *Device Detail* page, user and device information is automatically added to the ticket.

1. Go to the *Device Detail* page:

a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
b. On the left navigation bar, click **Inventory**, then click **Device**s.
c. Click the name of a device.

2. In the *Activities* tab, click **Total Service Desk Tickets** to display a table showing tickets related to the device.
3. Click **New** to display the *New* page.

   # If you want to create a ticket based on a queue, if there are multiple ticket queues in the organization, select a queue from the **Ticket** drop-down list.

   # If you want to create a ticket based on a process template, select the process from the **Process** drop-down list.

   The *Ticket Detail* page appears.
4. Provide the required information. See Create tickets from the Administrator Console Ticket page for a description of the ticket fields.
5. Do one of the following:

   # Click **Save** to save the ticket and return to the *Ticket* list.

   # Click **Apply Changes** to save the ticket and continue editing it.

   # Click **Cancel** to discard the ticket changes.

   If other users have modified the ticket concurrently, the *Update Notification* dialog appears, provided that the dialog is enabled for the queue and you are the ticket owner or an administrator. This dialog is displayed to administrators and ticket owners only. It is not displayed to other users. Administrators can enable or disable the conflict warning message for each queue separately. See Enable or disable the conflict warning.

Create tickets from the Asset Detail page

You can create Service Desk tickets for assets from the *Asset Detail* page as needed.

When you create Service Desk tickets from the *Asset Detail* page, user and asset information is automatically added to the ticket.

1. Go to the *Asset Detail* page:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Asset Management**, then click **Assets**.
   c. Click the name of an asset.

   In the Service Desk Tickets section, a table is displayed showing tickets related to the asset.
2. Click **New** to display the *New* page.

   # If you want to create a ticket based on a queue, if there are multiple ticket queues in the organization, select a queue from the **Ticket** drop-down list.

   # If you want to create a ticket based on a process template, select the process from the **Process** drop-down list.

The *Ticket Detail* page appears.

3. Provide the required information. See Create tickets from the Administrator Console Ticket page for a description of the ticket fields.
4. Do one of the following:

   # Click **Save** to save the ticket and return to the *Ticket* list.

   # Click **Apply Changes** to save the ticket and continue editing it.

   # Click **Cancel** to discard the ticket changes.

   If other users have modified the ticket concurrently, the *Update Notification* dialog appears, provided that the dialog is enabled for the queue and you are the ticket owner or an administrator. This dialog is displayed to administrators and ticket owners only. It is not displayed to other users. Administrators can enable or disable the conflict warning message for each queue separately. See Enable or disable the conflict warning.

Create a Service Desk ticket from an alert

You can create a Service Desk ticket from a server monitoring alert, with information from the alert automatically populating fields in the ticket form.

1. Go to the *Monitoring Alerts* list in one of the following ways:

   - **If you have the *Monitoring Alerts* widget installed on your open *Dashboard*, click Monitoring Alerts.**
   - **In the left navigation bar, select Monitoring > Alerts.**

2. Select the check box for the row that contains the alert message, then select **Choose Action > New Ticket**.

   # If you want to create a ticket based on a queue, if there are multiple ticket queues in the organization, select a queue from the **Ticket** drop-down list.

   # If you want to create a ticket based on a process template, select the process from the **Process** drop-down list.

   The *Title*, *Summary*, *Submitter*, and *Device* fields contain information from the alert.

3. **Optional**: Change the *Title* and *Summary* to conform to your corporate procedures.
4. Provide the rest of the information needed to complete the form, then click **Save** to save the ticket and leave the *Ticket Detail* page, or **Apply Changes** to save the ticket and continue editing it.

Option	Description
Title	(Required) A brief description of the issue. You can replace the monitoring-provided title with one of your choosing.
Summary	A more detailed description of the issue. This field includes a full range of text editing options for formatting your content, such as buttons for bold text, hyperlinks, lists, or text color. For example: • To apply bold text to a text string, select it in the editor, and click B. • To add images, click, and provide the URL to the image file. # Any images you include this way will not be added as file attachments to the ticket. # Deleting an image from the text field will permanently remove it as the image in this field is not stored as an attachment. • To add external links, click. • To embed externally hosted videos, click.

Option	Description
Submitter	The login name of the user submitting the ticket. The submitter can be changed by selecting a different login name in the drop-down list. Click to view the submitter contact information.
Asset	The asset that the information in the ticket is about. Select an asset in the drop-down list. Click to view the asset details.
Filter on submitter assigned assets	Filter the asset list based on the assets that are assigned to the submitter.
Device	The device that the information in the ticket is about. Monitoring provides this information. Click to view the device details.
Filter on submitter assigned devices	Filter the asset list based on the devices that are assigned to the submitter.
Impact	The number of people that are inconvenienced or cannot work.
Category	A classification of the issue.
Status	The current state of the ticket. This field does not appear if you are creating or editing a ticket from a process template.
Priority	The importance of priority of the ticket.
Owner	The user responsible for managing the ticket through its lifecycle.
Due	Date and time the ticket is scheduled to be completed. If Service Level Agreements are not enabled, the due date is set to None, by default. If Service Level Agreements are enabled, the due date is automatically calculated according to the SLA settings. The due date is calculated based on the priority set when the ticket is submitted. If the priority is changed after the ticket is initially submitted, the due date will be recalculated according to the new priority, but based on the original submitted date and time. If the SLA resolution time configuration is changed, it is only applicable on new tickets. Old tickets are not affected. See Configuring Service Level Agreements. Select **Manual Date** to manually set the due date and time. In this case, if Service Level Agreements are enabled, the due date and time is calculated and displayed as an option, but not selected.
CC List	A list of users who receive a notification email when a ticket event occurs. The CC List is emailed based on the ticket event and **Ticket CC** being configured for the queue **Email on Events** configuration.
Resolution	The resolution of the issue associated with the ticket. This field includes a full range of text editing options for formatting your content, such as buttons for bold text, hyperlinks, lists, or text color.

Option	Description
	For example: • To apply bold text to a text string, select it in the editor, and click B. • To add images, click , and provide the URL to the image file. # Any images you include this way will not be added as file attachments to the ticket. # Deleting an image from the text field will permanently remove it as the image in this field is not stored as an attachment. • To add external links, click . • To embed externally hosted videos, click .
Related Ticket Information	This section does not appear if you are creating a ticket from a process template.
Add Ticket	Click to add an additional ticket to this ticket's related information.
Referrers	The **Referrer** is a read-only field that holds a ticket reference to any ticket that references this ticket by way of the **See also** section.
Merged Tickets	This section allows you to edit the list of tickets merged with this ticket, as applicable. Any tickets that you want to merge must belong to the same queue. When you merge tickets using the *Ticket Detail* page, the open ticket becomes the primary ticket. All other merged tickets are archived when you merge them. For more details, see Merging tickets. To add a merged ticket, click **Add Tickets to Merge/Edit Merged Tickets**, and select a ticket from the list that appears.
Process Information	This section only appears if you are creating a ticket from a process template. All of the settings appearing in this section are read-only. For complete information about creating and configuring process templates, see Add, edit, and enable process templates
Process	The name of the process template associated with this ticket.
Process Type	The type of the process.
Process Status	The status of the workflow associated with this process template. For example, *Pending Approval*.
Parent	The name of the parent ticket, as defined in the process template associated with this ticket.
Process Approvals	A list of users that are assigned as approvers for this ticket, if applicable. The approvers are listed in stages, as defined in the process template. Each stage can have one or more approvers, as needed. The settings related to each approver and stage are also listed in this section, such as approval timeouts and notifications. When you create a process ticket, the timeout period starts for the first approver. When that user approves the ticket, the timeout starts for the next one, and so on.
Process Activities	A list of process activities, each representing a child ticket, and listed in stages, as defined in the process template. Multiple tickets can be assigned to the same stage,

Option	Description
	if needed. For example, if the first stage is to obtain equipment and supplies for a new-hire, you can have several separate child tickets for ordering devices, office equipment, and supplies, all assigned to stage 1. When you create a process ticket, all child tickets assigned to stage 1 are created automatically. Stage 2 tickets are created when all stage 1 tickets are closed, stage 3 tickets are created when all stage 2 tickets are closed, and so on.
Add Ticket	Click to add an additional ticket to this ticket's related information.
Referrers	The **Referrer** is a read-only field that holds a ticket reference to any ticket that references this ticket by way of the **See also** section.
Comments	Comments that you want to add to the ticket. You can also add file attachments, screenshots, provide automatic responses or Knowledge Base article contents as ticket comments. For more information see: • Add comments to tickets • Add or delete screen shots and attachments from Service Desk tickets If you want to add an automatic response as a resolution to this ticket, click **Predefined Response** and select a response template. The selected response template appears in the **Resolution** field. You can add multiple response templates as resolution entries. They appear in the order you selected them. **TIP:** To create or edit a response template, save your changes and click **Manage**. This will take you to the *Response Templates* page. For more information about response templates, see View and edit response templates.
Knowledge Base Article	Look up a Knowledge Base article and append its contents to the ticket comments. For more information about Knowledge Base articles, see Managing Knowledge Base articles.

Related topics

Managing Service Desk tickets, processes, and reports

Creating and managing tickets by email

You can enable users to create and manage tickets by email. This is useful for users who do not have access to the appliance **Administrator Console** or **User Console**.

About attachments to tickets created through email

Users can attach files to Service Desk tickets submitted through email, and those attached files can be up to 8 MB in size.

If attachments exceed 8 MB in size, email messages are rejected. No error messages are displayed to users.

If the appliance detects any threats in a file attachment included with Service Desk tickets, access to the file is blocked and can be managed on the *Antivirus Quarantine* page. For details, see Manage quarantined file attachments.

Enable email ticket creation

You can enable users to create and manage Service Desk tickets using email.

1. Go to the Service Desk *Ticket Detail* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Service Desk**, then click **Configuration**.
    c. On the **Configuration** panel, under **Email Configuration** section, click **Configure queue email settings**.
    d. Click the name of a queue.
2. In the General tab, add a valid email account, such as Support@mydomain.com, where users can send email to create tickets.
3. Add the email address to the *Alternate Email Address* field.
4. Select the **Allow all users as submitters** check box.
5. Select the **Accept email from unknown users** check box.

    If **Accept email from unknown users** is enabled in the queue configuration, any email sent to the Service Desk queue to create a ticket is allowed to set the *Submitter* field. In this case the username must be passed in the **@submitter** token and is that of an existing user, or is the current email address if it is an unknown user.

    If **Accept email from unknown users** is disabled, the preceding process works only when the email address of the sender is already associated with a Service Desk user account.
6. Click **Save**.

Tickets created from email messages receive the default values for Impact, Category, and Priority as configured on the *Queue Detail* page. The body of the email message is added as a comment. The *Submitter* field is derived from the sender's email address.

Create a ticket by email

You can quickly create a ticket by email when you specify the name of the ticket template in the email subject line.

Any replies made to the original email thread used to create a ticket, or to the emails sent from Service Desk associated with the ticket, appear on the ticket's *Comments* tab. For more information, see View ticket comments.

1. Log in to your email account and create a new email message.
2. In the email subject line, specify the ticket template name enclosed in braces. For example: `{Printer Issues}`.

    If you do not specify the ticket template, the appliance uses the default ticket template associated with the queue.
3. Describe your issue in the email message, and send it to the email address associated with the queue the specified ticket template belongs to.

    For details on how to configure queue email settings, see Configure queue-specific email settings.
4. When you receive an email confirmation from Service Desk, click the link in the email to review the ticket contents.

    The *Ticket Details* page appears, displaying the newly created ticket.
5. Make any changes, as required.

    For more information about editing the ticket page, see Create tickets from the Administrator Console Ticket page.

Modifying ticket attributes using email

You can change ticket attributes by email using variables that contain the **@** symbol at the beginning of email messages.

Any text after the last email variable is added to the ticket *Comment* field.

For example, the following email text closes the ticket, changes the ticket owner, and adds a comment:

```
@status=closed
@owner=joe
I fixed that problem. If it happens again, talk to Joe.
```

Invalid fields and field values produce errors that are emailed back to the sender using the email error template. For more information on email templates, see Configuring email triggers and email templates.

Clearing a ticket field using email

You can clear any field by sending an email with the prescribed syntax.

The syntax takes the form @fieldname=. For example, the following entry clears the *Due Date* field:

```
@due_date=
```

Changing ticket fields using email

You can change the following ticket attributes using email messages if the value of the ticket field is set to *User Create & Modify*.

For information on changing ticket field permissions, see Using ticket approvers.

Field	Description
@category	A valid category.
@cc_list	A comma-separated list of email addresses or distribution lists.
@due_date	A due date. The date can be in any format. For example, 4/3/2014, April 3, 2014, or next Thursday.
@impact	A valid ticket impact.
@owner	The owner's username, full name, or email address.
@priority	A valid ticket priority.
@resolution	A resolution.
@status	A valid ticket status.
@submitter	The submitter's username, full name, or email address. The email address is used for the username and email address fields. The full name is set to the *Name* portion of the email address. For example, **name**@domain.com.
@title	A title for the ticket.

Field	Description
@summary	A detailed description of the issue.
@asset	The asset associated with the ticket.
@machine	The device associated with the ticket.
@approval	The state of the ticket approval process. You can set this field to one of the following values: `Approved`, `Rejected`, `None`, or `More Information Needed`.
@approval_note	A note associated with the approval.
@owners_only	Indicates if only owners can comment on the ticket through email. When set to `1`, the flag is `True`. Any other numeric value sets this indicator to `False`.
@custom_<number>	The value of a custom ticket field, where `<number>` is the custom field ID. For example, `$custom_2=ABC` assigns the value of `ABC` to the `CUSTOM_2` ticket field.

Changing ticket approval fields using email

Users who are designated as ticket approvers can change a number of approval fields using email messages.

Approvers can change the following approval fields:

Field	Description
@approval	Modify the ticket. Use one of the following: **Approved**, **Rejected**, **None**, or **More Information Needed**.
@approver	Change the ticket approver. Enter a username from the ticket approval label. For instructions on setting up the label of approvers, see Using ticket approvers.
@approval_note	Enter a comment.

Setting or changing custom fields using email

You can set custom fields for Service Desk tickets through email using the prescribed syntax.

The syntax takes the form @custom_fieldname=newvalue.

Custom fields cannot contain spaces. Use an underscore between words. For example, new_value.

You can also use:

- @priority = high
- @priority = very_urgent

For multiselect custom fields, use a comma-separated list of values. Invalid values in select or multiselect custom fields produce errors.

Viewing tickets and managing comments, work, and attachments

You can navigate among tickets, and the devices and assets that are related to tickets, using links on detail pages. In addition, you can add work information, comments, and attachments, such as screenshots, to tickets.

On ticket detail pages, the related devices and assets are listed and linked for quick access. Similarly, you can access related tickets from device and asset detail pages. In addition, you can view and create tickets from device and asset detail pages.

Navigate among tickets, related devices, and assets

Links on ticket detail pages enable you to navigate among related Service Desk tickets and related devices and assets.

1. Go to the Service Desk *Ticket Detail* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Service Desk**, then click **Tickets**.
    c. Click the title of a ticket.
2. View tickets by submitter, asset, or device.
    - **Click the Submitter Ticket History.**
    - **Click the Asset Ticket History.**
    - **Click the Device Ticket History.**

    A new window displays all tickets for the asset with the ticket number, title, and status for each ticket.

    To view the ticket details, click the link in the *Number* or *Title* column to display the *Ticket Detail* page.
3. View related tickets in the *Related Ticket Information* tab.
    - **Click a ticket referenced as *See Also*.**
    - **Click a ticket referenced as a *Referrer*.**
    - **Click a ticket referenced as a *Merged Ticket*.**
    - **Click a ticket referenced as a *Child Ticket*.**
    - **Click a ticket referenced as a *Parent Ticket*.**

    The *Ticket Detail* window displays for the selected ticket.

Add work information for tickets

You can add work information to Service Desk tickets, such as the date the work started or stopped, the total number of hours spent on the ticket, and notes about the work performed. This information is available to ticket submitters and owners.

1. Go to the Service Desk *Ticket Detail* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Service Desk**, then click **Tickets**.

c. Click the title of a ticket.

2. Select the **Work** tab at the bottom of the page.
3. Click **Add**.
4. Provide the following information:

Option	Description
Date	The date work begins. To change the date, click in the date field and select a different date. To remove the date, click **Clear**.
Start	The time work begins (24-hour clock format).
End	The time work ends (24-hour clock format).
Adjustment	The amount of time to add or subtract to the hours logged. This can be useful for billing and tracking purposes. For example, work on a ticket might start at 08:00 and end at 12:00. However, the actual time an administrator spent working on the ticket might be 2 hours. You could enter -2.0 in this field to accurately report the actual time spent.
Note	Any additional information you want to provide.

5. Click **Add Work**.

Use default views for tickets

There are several built-in system views you can use to restrict the tickets displayed on the *Tickets* page.

1. Go to the Service Desk *Tickets* page:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Service Desk**, then click **Tickets**.

   The *Tickets* page shows tickets in the default queue.
2. To limit the tickets shown in the queue, select a view from the **View By** drop-down list.

The available built-in views are:

Group	View
My Tickets	All My Tickets **NOTE:** This includes any tickets submitted by me or owned by me, or any tickets where I am the approver. My Active Tickets **NOTE:** This includes any tickets submitted by me or assigned to me with 'Opened' or 'Stalled' states. My Tickets Submitted Today My Tickets Due Today My Overdue Tickets My Recent Tickets

Group	View
My Tickets by State	My Opened State Tickets My Stalled State Tickets My Closed State Tickets My Not Closed State Tickets
My Tickets by Status	**NOTE:** This option is only displayed when viewing a specific queue. My New Tickets My Opened Tickets My Closed Tickets My Need More Info Tickets
All Tickets	All Tickets All Active Unassigned Tickets **NOTE:** This includes any tickets with no owner and with a state of opened or stalled. This is only available if the user logged in is an owner of the selected queue. All Tickets Submitted Today All Tickets Due Today All Overdue Tickets
My Process Tickets by Type	My Service Request Process Tickets My Software Request: Approval Required Process Tickets
All Tickets by State	All Opened State Tickets All Stalled State Tickets All Closed State Tickets All Not Closed State Tickets
All Tickets by Status	**NOTE:** This option is only displayed when viewing a specific queue. All New Tickets All Opened Tickets All Closed Tickets All Need More Info Tickets
All Process Tickets by Type	All Service Request Process Tickets All Software Request: Approval Required Process Tickets
My Employee Tickets By State	**NOTE:** This option is only displayed when: • Your user account has a manager role, and one or more employee account associated with it. • You are using the **User Console**.

Group	View
	NOTE: Administrators can turn off this feature on the *Queue Settings* page. My Employee Tickets: Opened My Employee Tickets: Stalled My Employee Tickets: Closed My Employee Tickets: Not Closed
Submitter Label	<submitter label>
Custom View	List of available custom views. **NOTE:** This option is only displayed if there are any custom views created by the logged in user.

Set the custom view as the default. See Set a view as the default view for tickets.

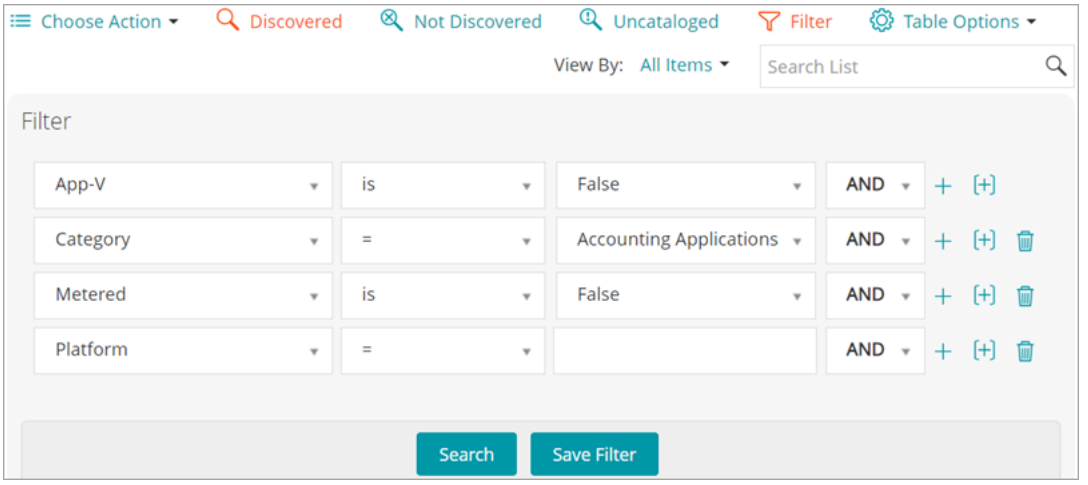
Create Filter views for tickets

You create custom views to restrict the type or number of Service Desk tickets displayed on the *Tickets* page. This enables you to see only those tickets that you want to view.

NOTE: Custom views are available only to the user accounts in which they are created. They are not available to multiple user accounts. To enable other users to access a custom view you created, send them the URL of the custom view.

1. Go to the Service Desk *Tickets* page:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Service Desk**, then click **Tickets**.
2. Select the **Filter** tab above the list.

   The *Custom View* panel appears.



3. Specify the criteria to use for the custom view. For example, you could create a custom view that shows open tickets with the priority of High.
4. Click **Search** to confirm the results.
5. Click **Save Filter** to save the custom view.

Set the custom view as the default. See Set a view as the default view for tickets.

Set a view as the default view for tickets

You can set a view as the default view for the Service Desk *Tickets* page. The default view is user-specific, and must be configured for each user independently.

1. Go to the Service Desk *Tickets* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Service Desk**, then click **Tickets**.
2. **Optional**: Click the **Filter** tab above the list and choose the settings for the filter. See Create Filter views for tickets .
3. Select **Choose Action** > **Set Default View** > **Set Current View As Default**.

    The current view is saved as the logged-in user's default view for the *Tickets* lists.

Add comments to tickets

As a ticket is worked on, comments can be added to provide further information to the ticket.

1. Go to the Service Desk *Ticket Detail* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Service Desk**, then click **Tickets**.
    c. Click the title of a ticket.
2. Click the **Comments and Attachments** tab at the bottom of the ticket detail page, if it is not already selected.
3. Enter the comment in the **Comment** text box.

    This field includes a full range of text editing options for formatting your content, such as buttons for bold text, hyperlinks, lists, or text color.

    For example:

    # To apply bold text to a text string, select it in the editor, and click B.
    # To add images, click , and provide the URL to the image file.
        # Any images you include this way will not be added as file attachments to the ticket.
        # Deleting an image from the text field will permanently remove it as the image in this field is not stored as an attachment.
    # To add external links, click .
    # To embed externally hosted videos, click .
4. Select the **Owners-only** check box to designate the comment be hidden from non-owners, such as submitters, and visible only to ticket owners.
5. If you want to add an attachment to the ticket, click **Add Attachment** and select the file to attach.

    You can add up to five file attachments to a ticket. For more information, see Add or delete screen shots and attachments from Service Desk tickets

6. If you want to add a screenshot to the ticket, click **Paste Screenshot** and paste the screenshot into the dialog box that appears.

You can add up to five screenshots to a ticket. For more information, see Add or delete screen shots and attachments from Service Desk tickets

7. If you want to add an automatic response as a comment to this ticket, click **Predefined Response** and select a response template.

   The selected response template appears in the Comments field. You can add multiple response templates as comments. They appear in the order you selected them.

   TIP: To create or edit a response template, save your changes and click **Manage**. This will take you to the *Response Templates* page.

   For more information about response templates, see View and edit response templates.

8. If you want to add the contents of a Knowledge Base article as a comment to this ticket, click **Knowledge Base Article** and select an applicable topic.

   The selected article contents appear in the Comments field.

   For more information about Knowledge Base articles, see Managing Knowledge Base articles.

9. If you are viewing a ticket for which you already provided comments, and you want to edit your own comments, you can do that, if the queue associated with the ticket is configured to allow users to edit their comments. For information on how to configure queue preferences, see Configure ticket queues.
10. If you are viewing a ticket that you submitted, and you want to edit other users' comments, you can do that, if the queue associated with the ticket is configured to allow technicians to edit the comments submitted by other users. For information on how to configure queue preferences, see Configure ticket queues.
11. If your account has a manager role, the queue associated with the ticket is configured to allow managers to edit comments to employee tickets, and you are viewing a ticket submitted by your employee, you can add or edit the comments, add file attachments or screen shots to the ticket, as needed. For information on how to configure queue preferences, see Configure ticket queues.
12. If there is a related Knowledge Base article to append to the ticket comments, select an article from the drop-down list. You can enter a search word to find a specific article.
13. Click **Submit Comment** to save the newly added comment.

    NOTE: Comments are saved independently of all other ticket information. If Email notifications based on comments are enabled, the subscribed users will receive the email instantly for the comment added. When users respond to an email notification that is sent regarding an existing ticket, only the new text that users type above the reply line will be added as a comment.

Add owner-only comments to tickets

You can add ticket comments that are hidden from non-owners, such as submitters, and visible only to ticket owners.

When adding owner-only comments, however, be aware that other ticket owners have permission to change this setting. Owner-only comments become viewable to other users when the setting is changed.

Quest recommends these best practices for owner-only comments:

- Always use discretion when adding comments.
- Have a clear, well documented policy for changing the *Owners only* setting.

1. Go to the Service Desk *Ticket Detail* page:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Service Desk**, then click **Tickets**.
   c. Click the title of a ticket.
2. Click the **Comments and Attachments** tab at the bottom of the ticket detail page, if it is not already selected.
3. Select the **Owners only** check box, then add the comment, Knowledge Base article reference, or attachment.

NOTE: The **Owners only** check box can be enabled by default by selecting the **Default ticket owner comments to Owners Only visibility** check box on the queue detail page. See Configure ticket queues.

4. Click **Submit Comment**.

NOTE: Comments are save independently of all other ticket information.

The comment is added to the ticket. It is visible to ticket owners only, unless a user with the appropriate permissions clears the *Owners only* check box.

View ticket comments

As a ticket is worked on, comments are displayed when the **Comment** tab is selected. They are also shown in the **History** tab along with other history items.

1. Go to the Service Desk *Ticket Detail* page:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Service Desk**, then click **Tickets**.
   c. Click the title of a ticket.
2. At the bottom of the *Ticket Detail* page, select the **Comments and Attachments** tab.

   A list of comments belonging to the ticket are displayed below the Comments tab.
3. Select the **Show attachments only** check box to filter the comment list and display only comments that have attachments.

Add or delete screen shots and attachments from Service Desk tickets

You can paste up to five screen shots into each Service Desk ticket. In addition, you can add up to five files as attachments to each ticket.

To paste screen shots into tickets:

- The content that you want to capture must be visible on your screen and you must be able to save a screen shot to your computer's clipboard.
- You must access the **Administrator Console** using a supported browser excluding Safari. For a complete list of supported browser, see the *Technical Specifications*.

NOTE: The paste screen shot feature is hidden if you are using an earlier or unsupported browser. However, you can still attach screen shots to tickets as files.

To attach files you must be able to browse to the files from the **Administrator Console**. You can attach files that are up to 8 MB in size.

When you add screen shots and attachments to a ticket, they appear listed in a separate section of the ticket screen. You can also add images (including screen shots) directly to the *Summary* and *Comment* fields. For more information, see Create tickets from the Administrator Console Ticket page.

1. With the content you want to capture visible, do one of the following to save a screen shot to your computer's clipboard:
   # On Windows, press the **Prnt Scrn** or **Print Screen** key.
   # On Mac, hold the following keys: **Command**, **Shift**, and **3**.

The screen shot is copied to your computer's clipboard.

2. Go to the Service Desk *Ticket Detail* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Service Desk**, then click **Tickets**.
    c. To display the *Ticket Detail* page, do one of the following:
    # Select **Choose Action** > **New**.
    # Select **Choose Action** > **New Ticket From Queue** > **Queue name**.

        If you have a high number of queues, use the search box to quickly find a specific queue.

    # Click the name of a ticket.
3. Attach a file to the ticket:
    a. On *Ticket Detail* page, scroll down to the *Attachments* section of the *Comments and Attachments* tab, and click **Add Attachment**.
    b. In the file browser dialog box that appears, select and open the file that you want to attach to the ticket.

        You can add up to five file attachments to a ticket.

        If the appliance detects any threats in a file attachment included with Service Desk tickets, access to the file is blocked and can be managed on the *Antivirus Quarantine* page. A *Quarantine* link appears next to the file name, allowing you to go to the *Antivirus Quarantine* page. When a quarantined file is released, access to the file is restored. For details, see Manage quarantined file attachments.

        The file browser closes and the file name of the attachment appears in the *Attachment* section, under Add Attachment.
    c. At the bottom of the page, click **Submit Comment**, then click **Apply Changes**.

        The file attachment is added to the ticket.
4. Add a screen shot to the ticket.
    a. On the *Ticket Detail* page, scroll down to the bottom of the page, and on the *Comments and Attachments* tab, in the *Attachment* section, click **Paste Screenshot**.

        The *Paste Screenshot* dialog box appears.
    b. Capture a screen shot and copy it to the clipboard.
    c. Use one of the following key combinations to paste the screen shot into the dialog window:
    # On Windows, hold down **Ctrl**, then press **V**.
    # On Mac, hold down **command**, then press **V**.

        The screen shot appears in the *Paste Screenshot* dialog box.
    d. Click **Add Screenshot**.

        The *Paste Screenshot* dialog box closes and the file name assigned to the screen shot appears in the *Attachment* section, under Paste Screenshot. You can add up to five screen shots to a ticket.
    e. At the bottom of the page, click **Apply Changes**.

        The screen shot is added to the ticket.
5. Delete a screen shot or a file attachment from a ticket:
    a. On *Ticket Detail* page, scroll down to the *Attachments* section of the *Comments and Attachments* tab.
    b. To delete a file attachment, under **Add Attachment**, locate the file that you want to delete, and click on the right of the file name.

c. To delete a screen shot, under **Paste Screenshot**, locate the file containing the screen shot that you want to delete, and click on the right of the file name.

d. At the bottom of the page, click **Apply Changes**.

The file is deleted from the ticket.

6. At the bottom of the page, click **Save** to save your changes to the ticket.

View ticket activity history

The history tab displays all activity history performed for the ticket. This includes updates to any ticket detail field and comments.

1. Go to the Service Desk *Ticket Detail* page:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Service Desk**, then click **Tickets**.
   c. Click the title of a ticket.
2. At the bottom of the ticket detail page, select the **History** tab.

Send ticket information through email

Service Desk ticket information can be manually emailed to recipients as needed.

The content and format of the email is controlled by the *Email Ticket Manually* notification template. Also, the *$ticket_fields_visible* token in the template displays all of the fields that are visible to the logged-in user who is sending the email. See Configuring email triggers and email templates.

1. Go to the Service Desk *Ticket Detail* page:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Service Desk**, then click **Tickets**.
   c. Click the title of a ticket.
2. Select **Choose Action** > **Email ticket**.
3. On the *Email ticket* page, enter the **Email address** of the recipient and update the **Subject** if necessary.
4. Click **Send**.

The ticket information is emailed to the specified recipient.

Run Device Actions from tickets

For devices that are assigned to Service Desk tickets, you can run Device Actions from the *Ticket Detail* page.

- Device Actions have been added. See the *Device Actions* section of Configure appliance General Settings without the Organization component.
- Devices have been assigned to tickets.
- You are accessing the **Administrator Console** using an approved browser. See https://support.quest.com/kb/148787.

1. Go to the Service Desk *Ticket Detail* page:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Service Desk**, then click **Tickets**.

c. Click the title of a ticket.

2. Select a Device Action from the *Action* drop-down list under the *Device* drop-down list.

   The Device Action automatically attempts to run on the remote device immediately.

Start a Remote Control Session from Ticket Details page

You can trigger and initiate a Remote Control Session from Ticket Details page. This feature simplifies troubleshooting by providing quick access to remote support tools for assigned devices.

1. Go to the Service Desk *Ticket Detail* page:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Service Desk**, then click **Tickets**.
   c. Click the title of a ticket.
2. On the **Ticket Details** page, locate the **Device** field.

   If the ticket is associated with a supported Windows or macOS device with Splashtop Streamer installed, a Remote Control icon and label appears under Device.
3. Click the icon to initiate the session.

NOTE: The Remote Control icon should appear automatically for eligible devices. If it does not, verify if the Splashtop Streamer is installed and the device is properly assigned to the ticket.

Merging tickets

If you have a number of related tickets that are still active, instead of managing them separately, you can merge them into a single ticket and manage that one ticket without losing ticket trail of all the merged tickets.

When you merge tickets, you must select a primary ticket. The remaining tickets are automatically archived. All history related to the merged tickets remains unchanged. The ticket history also indicates when a ticket is merged.

You can only merge tickets that exist in the same queue. Tickets belonging to the same queue, but created using different templates can be merged. The fields associated with the primary ticket template are preserved, while the child ticket fields are removed and archived. This feature is only available when ticket archival is enabled.

Service, parent, child, and already merged tickets cannot be merged. Only those tickets without a parent and without a child can be merged.

You can unmerge tickets, as needed. Any users on a ticket's CC list, that are added during the merge process remain on the list if the ticket becomes unmerged.

Enable ticket merge

You can enable ticket merge for the Service Desk, or if the Organization component is enabled, for the Service Desk of the selected organization.

1. Go to the *Service Desk Settings* page:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Service Desk**, then click **Configuration**.
   c. On the **Configuration** panel, under Settings section, click the **Enable ticket archival** link.
2. In the *Ticket Archival/Merge* tab, select the **Enabled** check box.

Merge tickets from the Tickets list page

You can use the *Tickets* list page to merge tickets and specify a primary ticket.

1. Select the tickets that you want to merge.
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. Click **Service Desk** to display the *Tickets* page.
    c. On the *Tickets* list page, click **Queue**, and select the queue containing the tickets that you are about to merge.
    d. Select all of the tickets that you want to merge.
2. Merge the selected tickets.
    a. In the *Choose Action* menu, select **Merge Tickets**.

    The *Merge Tickets* dialog box appears.

    b. In the *Merge Tickets* dialog box, specify the ticket that you want to select as the primary ticket, and click **Save**.

    The *Merge Tickets* dialog box closes and the *Confirm* message box appears, indicating that all tickets (except the primary tickets) are about to be archived.

    c. In the *Confirm* message box, click **Yes** to proceed with the merge.

Merge tickets from the Ticket Detail page

You can merge one or more tickets with the ticket you are viewing on the *Ticket Detail* page. Any tickets that you want to merge must belong to the same queue.

When you merge tickets using the *Ticket Detail* page, the open ticket becomes the primary ticket. All other merged tickets are archived when you merge them. For more details, see Merging tickets.

1. Open a ticket that you want to merge with one ore more other tickets.
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Service Desk**, then click **Tickets**.
    c. Click the title of a ticket.

    The *Ticket Detail* page appears.
2. Merge one or more tickets with the selected ticket.
    a. On the *Ticket Detail* page, in the *Related Ticket Information* tab, click **Add Tickets to Merge/Edit Merged Tickets**, and select a ticket from the list that appears.
    b. Add more merged tickets, as needed.
3. Verify that the process of merging tickets appears in the ticket history.
    a. On the *Ticket Detail* page, open the *History* tab, and select the **Show Merged Ticket History** check box.
    b. *History* tab, review the entries related to the merged tickets, as applicable.

Using the ticket escalation process

The Service Desk ticket escalation process is a mechanism for alerting Service Desk staff and supervisors when a ticket is ignored for a specified period of time.

When a ticket meets certain criteria, email is sent to the specified group alerting them that a ticket has been ignored. This provides a way to monitor service level agreements and automatically notify the appropriate staff members when a ticket has not been handled properly.

An escalation email is sent at the end of the escalation time limit for tickets with:

- A Status of **Opened**.
- A Priority that includes an escalation time.

The following example shows the default ticket statuses, priorities, and escalation settings. These settings direct the Service Desk to send an escalation email for tickets with a Status and State of **Opened** and a Priority of **High**, after 30 minutes of inactivity.

You can:

- Configure an escalation email for tickets with other priorities.
- Change the escalation time limits.
- Determine who receives an escalation email.
- Customize the email form as needed.

NOTE: Ticket escalation and Service Level Agreements are two separate notification activities. Ticket escalation notifications are based on the duration a ticket has been opened for, while Service Level Agreement notifications are based on the due date of a ticket. Ticket escalation does not consider Business Hours and Holidays.

Understanding ticket states

Service Desk ticket states identify the current state of the ticket. States include **Opened**, **Stalled**, and **Closed**.

Tickets can be escalated only if they are in the **Opened** state. This requirement is not configurable.

NOTE: Using the default settings, tickets must have a priority of **High** and a status of **Opened** to be escalated.

Understanding the escalation time limit

As soon as a Service Desk ticket is assigned the state of **Opened**, a timer begins counting toward the escalation time limit.

Any change to the ticket resets the timer. If the timer runs out, an escalation email is sent and the timer starts again. If no changes are made to the ticket, the timer is reset. An escalation email is sent each time the escalation time limit is reached. By default, the escalation email is sent every 30 minutes until the ticket is changed.

Understanding escalation

When Service Desk tickets are escalated, email messages are sent to recipients as specified in the queue settings.

You can choose to send escalation email to:

- Ticket owners
- Ticket submitters
- Users with the technical skills to resolve issues
- Users with the authority to dedicate more resources to the problem

The *Email on Events* section of the *Queue Detail* page, and the **Category CC** list on each ticket, determine who receives escalation email messages.

Changing ticket escalation settings

Service Desk ticket escalation settings determine the actions that are taken when ticket priority or status changes.

Escalation email is sent for tickets with a priority of **High** and a status change from **New** to **Opened**. If a ticket owner does not respond to a ticket within 30 minutes, you can change the escalation settings to make the ticket eligible for escalation.

Change the list of escalation email recipients

You can change the email recipients used for Service Desk ticket escalation as needed.

If you are using the default settings, change the ticket status from **New** to **Opened**. If you have changed the default settings, make sure that at least one status has a state of **Opened**, and assign the ticket that status. See Configuring ticket settings.

(Optional) Assign tickets the **Opened** state by default or create a policy requiring that ticket owners change the tickets status as soon as they take ownership.

1. Go to the Service Desk *Queue Detail* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Service Desk**, then click **Configuration**.
    c. On the **Service Desk Configuration** page, under the *Email Configuration* section, click the *Setup email on events* link.
    d. Click the name of a queue.
2. In the *Email on Events* section, select the appropriate check boxes to add owners, submitters, approvers, Ticket CC members, and Category CC members as escalation email recipients.
3. Click **Save**.

Change the Response and Resolution time limits

You can change the time limits used for ticket escalation as needed.

1. Go to the Service Desk *Queue Detail* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Service Desk**, then click **Configuration**.
    c. On the *Service Desk Configuration* panel, in the Queues section, click the *Configure SLAs* link
    d. Click the name of a queue.
2. In the *Service Level Agreement* tab, change the time in the **Response Time** and **Resolution Time** fields to change the priority.
3. Click **Save** at the bottom of the page.

Change the default escalation email message

You can change the text of the email message that is sent automatically when Service Desk tickets are escalated.

1. Go to the Service Desk *Queue Detail* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Service Desk**, then click **Configuration**.

c. On the *Service Desk Configuration* panel, in the *Email Configuration* section, click the **Setup email on events** link.

d. Select the name of the queue.

2. In the *Email on Events* tab, click **Customize Emails** to display the *Service Desk Email Notifications* page **Or** Go to Configuration > Email Configuration section > Configure queue email settings > Email on Event tab
3. Edit the *Ticket Escalated* message as needed.
4. Click **Save**.

For more information on the *Ticket Escalation* message, see Configuring email triggers and email templates.

Using Service Desk processes

A Service Desk process is a collection of tickets appearing in pre-defined order that allows you to track tasks requiring multiple steps or activities to complete.

For example, consider the tasks required to prepare systems and equipment for new-hires:

- Identify office space and furniture requirements
- Set up phone service
- Obtain devices and software
- Set up network credentials
- Complete required employment paperwork

You could create a process template that includes all of these required tasks as child activities. Then, when you create tickets based on that process template, the child tickets are created automatically for all of the required tasks at each stage of the process.

To set up a Service Desk process template see, Add, edit, and enable process templates.

Add, edit, and enable process templates

You can add process templates to the Service Desk. In order for a process template to be enabled and available for end users to create tickets based on that process, it must include at least one parent ticket.

1. Go to the Service Desk *Create Process Template* wizard:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Service Desk**, then click **Configuration**.
   c. Under the *Process Template* section, click *Define queue workflow and create ticket ownership rules*
   d. To create a new process template, on the *Process Templates* page, select **Choose Action** > **New**.

      Or

      To create a new process template directly from the *Service Desk Configuration* **page, under the** *Process Template* **section, click** *New Process Template* **link.**

   e. To edit or copy an existing process template, on the *Process Templates* page, click a process template name.

   The *Create Process Template* **wizard appears, with the** *Define Process Template* **page open.**
2. To copy an existing process template, on the *Define Process Template* page, click **Duplicate**.

   A copy of the duplicated process template appears. While the duplicated process template is disabled, all of the other options are the same as in the original template. When you finish updating the duplicated version, you can select the Enabled option on the *Step 6 of 6 - Publish Options* **page.**
3. On the *Step 1 of 6 - Define Template* tab, specify the following information:

Option	Description
Name	A name that describes the overall process, for example, New Hire, Employee Termination, or Office Move.
Description	A description of the process. For longer descriptions, this field expands automatically, as you type.
HTML/Markdown	An indicator of whether the description contains rich text. Some process descriptions can be longer than others, so formatting specific text elements can improve the overall readability and help the end user better understand the process. You can use the Markdown project syntax to format the contents of the *Description* box. For example: `<h1> Before you proceed:</h1>` `<h1><ol>` `<li>Ensure the new employee acquisition process is finalized by HR.` `<li>Ensure the Badge ID exists for the new employee  ` `<b>If you do not have a Badge ID, contact HR.</b>` `</ol></h1>` For more information about the Markdown syntax, visit http://daringfireball.net/projects/markdown/syntax.
Process Type	The type of the process. In a default installation, only the *Service Request* and *Software Request: Approval Required* process types are included. You can create new process types, as required. For example, you can create a process type for accessing a specific application, or a group of applications. For more information, see Define process types.
Allow child tickets to inherit fields at creation time from parent ticket	Select this option if you want to enable an option in child tickets to inherit field values from their parent tickets that belong to the same queue. Only the values that exist in parent tickets when child tickets are created can be inherited. Any subsequent changes to the associated parent ticket field values are not propagated to child tickets that have this option selected. Inherited field values are specified on a per-ticket basis, as you configure each ticket.

Click **Save and Continue**.

4. On the *Step 2 of 6 - Parent/Child Tickets* tab that appears in the *Create Process Template* wizard, associate a parent ticket with this process template.
    a. **Software Request: Approval Required process types only**. This process type is meant for building special process templates that can be used to set up user downloads that require one or more approvals. If selected, a parent ticket is created from this process type by default.
    # To view or edit the contents of the ticket, click **Software Request: Approval Required**.
    # Tickets of this type do not allow you to edit the *Title*, *Summary*, *Device*, or *Submitter* fields. These fields will be populated with the values from the request that initiated the process.
    # Approvals for this process type are mandatory.
    b. Select a queue containing the parent ticket that you want to associate with this process template, and click **Add Parent Ticket**.

c. On the *New Parent Ticket* page, create a new parent ticket for this process template:

If you have multiple queues, select a queue. Parent and child tickets can each be located in different queues. If you do not have multiple queues, queue selection is not offered.

If you select a queue that has one or more ticket templates associated with it, select the ticket template.

Most fields are similar to those on the *Ticket Detail* page. See Create tickets from the Administrator Console Ticket page. You do not have to use the same category, owner, and so on, for the parent as you use for the child tickets.

The *Due Date Offset* is the amount of time required to complete work on a child ticket, and this amount of time is used to calculate the ticket due date. For example, if you set the *Due Date Offset* to four days, the child ticket's due date is offset to be four days after the ticket's creation date. Due dates are not enforced, but if the due date has passed, tickets are marked as Overdue on the *Ticket* list and they appear as Overdue on reports.

For additional information about creating tickets, see Create tickets from the Administrator Console Ticket page.

d. Click **Save** to return to the *Create Process Template* wizard.

5. **Optional**. After adding a parent ticket for a process, you can configure child tickets or activities for that process. Child tickets can be from different queues and they can be assigned different stages.

a. On the *Parent Ticket* page that appears in the *Create Process Template* wizard, under *Child Tickets*, select a queue associated with the child ticket.

b. If the selected queue has one or more ticket templates associated with it, select a ticket template.

If the queue includes one or more templates, and you do not specify which template you want to use, the default queue template is selected.

c. Click **Add Child Ticket**.

When a ticket based on this process template is created, stage 1 child tickets are created automatically (after approvals and requirements are met, if needed). When the last child ticket in stage 1 is closed, the child tickets defined in the next stage are created.

d. On the *Child Ticket* page, create a new child ticket for this process template:

Stage: The stage of the process at which the ticket is created, such as 1, 2, 3, and so on. You can assign multiple tickets to the same stage if necessary. For example, if the first stage is to obtain equipment and supplies for a new-hire, you might have several separate child tickets for ordering devices, office equipment, and supplies, all assigned to stage 1.

When you create a process ticket, all child tickets assigned to stage 1 are created automatically. Stage 2 tickets are created when all stage 1 tickets are closed, stage 3 tickets are created when all stage 2 tickets are closed, and so on.

Title: A title for the child ticket.

Summary: A description of the task associated with this child ticket.

Category, **Owner**, and **Due Dates**: These values do not need to match those of the parent ticket.

If you selected Allow child tickets to inherit fields at creation time from parent ticket on the *Define Process Template* page, the Inherited check box appears in each field, allowing you to populate it with the current value of this field in the parent ticket. For more information, see step 3.

For additional information about creating tickets, see Create tickets from the Administrator Console Ticket page.

e. Click **Save** to return to the *Create Process Template* wizard.

6. If you want the tickets created from this process template to require approvals, on the *Step 3 of 6 - Approvals* tab that appears, select **One or more approvals required for this process to start**, and specify the information listed in the table below.

If you selected the *Software Request: Approval Required* process type, this check box is selected by default and cannot be cleared. Approvals for this process type are mandatory.

When a process ticket is created for a process that requires approval, child tickets are not created until all of the approvals are received. If there are multiple approval stages, emails requesting the approvals are first sent to step 1 approvers. Step 2 approvers receive their emails only after all of the step 1 approval requirements are met.

Approvers can approve or reject a process ticket by email using email tokens. For example, use the following syntax examples, as applicable:

To approve a ticket by email:

```
@approval = approved
@approval_note = This request is approved by email
```

To reject a ticket by email:

```
@approval = rejected
@approval_note = This request is rejected by email
```

For more information about these tokens, see Changing ticket approval fields using email.

Option	Description
Approval Step	
Approval Step 1	One or more ticket approvers. You can edit the list of approvers, as required. • **New process templates**. This field appears blank. • **Existing process templates**. If one or more approvers are already defined in the process template, they are listed in this field. **NOTE:** The submitter's manager appears selected by default.
Any one approval is required	At least one ticket approval is required.
All approvals are required	All ticket approvals are required.
Remove All	Removes all approvers from the list.
Add Another Step	Adds an approval step.
Approval Options	
Approval Timeout Period	The amount of time each ticket approver has to approve or decline a ticket that is based on this process template. Approval Timeout period does not span over multiple approval steps. For example, if a process has two approval steps and the approval timeout period is defined as eight hours: • Step 1 approvers have 8 hours to approve. • When all of the step 1 approvals are received, step 2 approvers are given eight hours to act on their approval requests.

Option	Description
Approval Notification Recurrence	Indicates how often the system sends notifications to each approver about a ticket that is pending approval. Leaving this option set to zero '0' causes one-time notification to be sent without any recurrences.
Use business hours and holidays for approval timeout and notification frequency	Indicates if the system calculates the approval times using business hours.
Approval Override	Overriding an approval advances the process ticket forward without waiting on any pending approvals. After the override, any pending approvals are closed out, a ticket history is written, and an Approval Received email is sent to approvers, as defined in the email notification.
None	Approval overrides are not allowed.
Allow All Admins to Override	Any users with administrative access can override approvals.
Specify Label	Any users belonging to group with this label can override approvals.

Click Save and Continue.

7. On the *Step 4 of 6 - Approval Event Notifications* tab that appears, select the recipients of email notifications for each stage of the ticket lifecycle. Click the indicated link to configure these options on the *Service Desk Queue Email Settings* page. For more information, see Configure queue-specific email settings.

Click Save and Continue.

8. On the *Step 5 of 6 - Recurring Ticket Schedule* tab that appears, specify the frequency at which a ticket is created. This is useful if you want this process to create tickets at regular intervals, for example, for checking system health or deleting file logs on a regular basis.

Option	Description
None	Run in combination with an event rather than on a specific date or at a specific time.
Every n hours	Run at a specified interval.
Every day/specific day at HH:MM	Run daily at a specified time, or run on a designated day of the week at a specified time.
Run on the nth of every month/ specific month at HH:MM	Run on the same day every month, or a specific month, at the specified time.
Run on the nth weekday of every month/specific month at HH:MM	Run on the specific weekday of every month, or a specific month, at the specified time.
Custom	Run according to a custom schedule.

Option	Description

	Use standard 5-field cron format (extended cron format is not supported):
	`* * * * *`
	`| | | | +————————day of week (0-6)(Sun=0)`
	`| | | +————————month (1-12)`
	`| | +————————day of month (1-31)`
	`| +————————hour (0-23)`
	`+————————minute (0-59)`
	Use the following when specifying values:
	• **Spaces ( )**: Separate each field with a space.
	• **Asterisks (*)**: Include the entire range of values in a field with an asterisk. For example, an asterisk in the hour field indicates every hour.
	• **Commas (,)**: Separate multiple values in a field with a comma. For example, `0,6` in the day of the week field indicates Sunday and Saturday.
	• **Hyphens (-)**: Indicate a range of values in a field with a hyphen. For example, `1-5` in the day of the week field is equivalent to `1,2,3,4,5`, which indicates Monday through Friday.
	• **Slashes (/)**: Specify the intervals at which to repeat an action with a slash. For example, `*/3` in the hour field is equivalent to `0,3,6,9,12,15,18,21`. The asterisk (`*`) specifies every hour, but `/3` restricts this to hours divisible by 3.
	Examples:
	• `15 * * * * Run 15 minutes after every hour every day`
	• `0 22 * * * Run at 22:00 every day`
	• `0 0 1 1,6 * Run at 00:00 on January 1 and June 1`
	• `30 8,12 * * 1-5 Run weekdays at 08:30 and 12:30`
	• `0 2 */2 * * Run every other day at 02:00`

View Task Schedule	Click to view the task schedule. The *Task Schedule* dialog box displays a list of scheduled tasks. Click a task to review the task details. For more information, see View task schedules.

9. On the *Step 6 of 6 - Publish Options* tab that appears, select any publishing options, as required:

Option	Description
Enabled	Processes must be enabled before you can use them to create process tickets. Select this check box if you want to enable users to create tickets from this process template.
Hide approval information from non-owner users	Select this option if you do not want the users who do not own the ticket to view approval information.
Hide process steps from Submitters	Select this option if you do not want to display the process steps (child tickets) to submitters in the parent ticket details page.
Display process to all users	This option is selected by default. If you want to restrict end user access to this process, clear this option. Alternatively, select a label associated with the group to which you want to grant access.

Option	Description
Display process description page while creating new process requests	Select this option if you want to show the process description page when creating new tickets based on this process template.
Use process status workflow instead of ticket status	When you want to take advantage of the approval and notification features available in the process template, you must select this option. If you already configured approvals or notifications, this option is selected by default and cannot be cleared. Choosing to use the process status workflows causes the parent ticket to automatically advance through various process-specific states such as Pending Approval, Approval Denied, Approval Timed Out, In Progress, or Process Complete. If you choose not to select this option and continue to use the ticket status workflows instead, you must create custom ticket rules to achieve desired approval and notification functionality. When you use process status workflows, the *Status* field does not appear on the *Ticket Detail* page, even if that field is configured to appear for the related queue. The ticket *Status* field is still displayed for the child tickets.
Parent Ticket Closed Status	Select the status that you want to use when the parent ticket associated with this process is closed. When the last child activity is closed, the parent ticket is closed automatically, and its status appears in this field.

Click Finish.

The *Create Process Template* wizard closes, and your newly created or updated process template appears on the *Process Templates* page.

Define process types

In a default installation, only the *Service Request* and *Software Request: Approval Required* process types are included. You can create new process types, as required. For example, you can create a process type for accessing a specific application, or a group of applications.

The *Software Request: Approval Required* process type is meant for building special process templates that can be used to set up user downloads that require one or more approvals.

Create a parent ticket.

1. Go to the Service Desk *Process Detail* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Service Desk**, then click **Configuration**.
    c. On the **Configuration** panel, under **Process Templates**, click **Define Process Types**.
2. To add a new process type, in the top-right corner, click +. In the text box that appears, type the process type name, and click **Add**.
3. To change the name of an existing process, in the row containing the process type that you want to edit, click . In the text box that appears, type the new process type name, and click **Add**.

Create process tickets to manage related tasks

If you have added and enabled process templates in a queue, you can create process tickets to manage sets of related tasks, such as the tasks required to set up systems for new employees, as a group.

You have added and enabled process templates. See Add, edit, and enable process templates.

1. Go to the Service Desk *New Ticket* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Service Desk**, then click **Tickets**.
    c. Select a queue from the queue selection drop-down, then **Choose Action** > **New Ticket From Process** > **Process name**.

    The *New Ticket* page appears. The activities related to each stage of the process are listed in the *Process Information* section.
2. Provide the required ticket information. See Create tickets from the Administrator Console Ticket page.
3. Do one of the following:

    # Click **Save** to save the ticket and return to the *Ticket* list.

    # Click **Apply Changes** to save the ticket and continue editing it.

    # Click **Cancel** to discard the ticket changes.

    If other users have modified the ticket concurrently, the *Update Notification* dialog appears, provided that the dialog is enabled for the queue and you are the ticket owner or an administrator. This dialog is displayed to administrators and ticket owners only. It is not displayed to other users. Administrators can enable or disable the conflict warning message for each queue separately. See Enable or disable the conflict warning.

See Create tickets from the Administrator Console Ticket page. The process ticket is created, and child tickets are created automatically for activities assigned to stage 1. Stage 2 child tickets are created when all stage 1 tickets are closed, and so on. If approvals are defined for the process, child tickets are created after the approvals are received for the process ticket.

Create process tickets by email

You can quickly create a process ticket by email for any existing process templates.

Prior to creating a process ticket by email, you must obtain and obtain the following information:

- Process name
- Email address of the ticket queue associated with the process template parent ticket

1. Log in to your email account and create a new email message.
2. In the email recipient line, type the email address of the ticket queue associated with the process template parent ticket.
3. In the email subject line, specify the process template name enclosed in curly braces. Any text you add after that segment is added to the ticket title. For example: `{New Hire} Jane Smith`.
4. Email body is optional. Any contents you add to the email body is added to the ticket description.
5. Send the email.
6. Go to the Service Desk *Tickets* list page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.

b. On the left navigation bar, click **Service Desk**, then click **Tickets**.

7. Look for the newly created ticket and click the ticket title.
8. Make any applicable changes.

For more information about editing the ticket page, see Create tickets from the Administrator Console Ticket page.

View process information

If you have created process tickets to manage sets of related tasks, you can view the related process information in those tickets.

You have created a ticket based on a process template. See Create process tickets to manage related tasks.

1. Go to the Service Desk *Ticket* page:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Service Desk**, then click **Tickets**.
   c. Click the title of a ticket.

   The *Ticket* page appears. The activities related to each stage of the process are listed in the *Process Information* tab. The level of information appearing in this section depends on the settings configured on the *Publish* tab of the *Create Process Template* wizard. For example, if you configured the related process template to display Approval and Process information, they appear in this section. For complete information about this wizard, see Add, edit, and enable process templates.
2. Do one of the following:

   # Click **Save** to save the ticket and return to the *Ticket* list.

   # Click **Apply Changes** to save the ticket and continue editing it.

   # Click **Cancel** to discard the ticket changes.

   If other users have modified the ticket concurrently, the *Update Notification* dialog appears, provided that the dialog is enabled for the queue and you are the ticket owner or an administrator. This dialog is displayed to administrators and ticket owners only. It is not displayed to other users. Administrators can enable or disable the conflict warning message for each queue separately. See Enable or disable the conflict warning.

The process ticket is created, and child tickets are created automatically for activities assigned to stage 1. Stage 2 child tickets are created when all stage 1 tickets are closed, and so on.

Cancel or complete process tickets

If you have created process tickets to manage sets of related tasks, you can view the related process information in those tickets. A process can be marked as cancelled, by either its owner or submitter. It can be marked complete only by its owner.

You have created a parent ticket based on a process template. See Create process tickets to manage related tasks.

1. Go to the Service Desk *Ticket* page:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Service Desk**, then click **Tickets**.
   c. Click the title of a process parent ticket.

The *Ticket* page appears.

2. Do one of the following:
   - # To cancel the process ticket, select **Choose Action** > **Cancel Process**.
   - # To complete the process ticket, select **Choose Action** > **Complete Process**.
3. In the dialog box that appears, confirm that you want to cancel or complete the process ticket.
4. Do one of the following:
   - # Click **Save** to save the ticket and return to the *Ticket* list.
   - # Click **Apply Changes** to save the ticket and continue editing it.
   - # Click **Cancel** to discard the ticket changes.

   If other users have modified the ticket concurrently, the *Update Notification* dialog appears, provided that the dialog is enabled for the queue and you are the ticket owner or an administrator. This dialog is displayed to administrators and ticket owners only. It is not displayed to other users. Administrators can enable or disable the conflict warning message for each queue separately. See Enable or disable the conflict warning.

Delete process templates

You can delete processes using the Service Desk *Processes* list. If tickets exist for a particular process, the process can only be marked as disabled. To delete the process, the tickets created using this process must be deleted first.

1. Go to the Service Desk *Processes* list:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Service Desk**, then click **Configuration**.
   c. On the *Configuration* panel, in the *Process Template* section, select the **Define queue workflow and create ticket ownership rules** link
2. Select one or more Process Templates, then select **Choose Action** > **Delete**.
3. On the confirmation page, click **Yes** to delete the selected Process Templates.

Convert process tickets to regular tickets

If you have Service Desk process tickets, you can convert them to regular tickets as needed. This conversion is useful for tickets that have inadvertently been created as process tickets when they do not require all of the steps of a process.

For more information on process tickets, see Using Service Desk processes.

1. Go to the Service Desk *Ticket Detail* page:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Service Desk**, then click **Tickets**.
   c. Click the title of a ticket.
2. Select **Choose Action** > **Convert from process Process Name to a regular ticket**.

NOTE: This menu option is only available if the selected ticket was created from a process.

A confirmation window appears.

3. Click **Yes** to continue to convert the process to a regular ticket.
4. Do one of the following:

   # Click **Save** to save the ticket and return to the *Ticket* list.
   # Click **Apply Changes** to save the ticket and continue editing it.
   # Click **Cancel** to discard the ticket changes.

   If other users have modified the ticket concurrently, the *Update Notification* dialog appears, provided that the dialog is enabled for the queue and you are the ticket owner or an administrator. This dialog is displayed to administrators and ticket owners only. It is not displayed to other users. Administrators can enable or disable the conflict warning message for each queue separately. See Enable or disable the conflict warning.

Convert regular tickets to process tickets

Regular Service Desk tickets can be converted to process tickets. This conversion is useful for process-related tickets that are created through email, because tickets created through email are always created as single tickets.

In addition, users might create single tickets because they are unaware of processes, or because they do not have access to processes. Changing regular tickets to process tickets enables administrators and ticket owners to take advantage of processes, even if tickets were not originally submitted as process tickets. For more information on process tickets, see Using Service Desk processes.

1. Go to the Service Desk *Ticket Detail* page:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Service Desk**, then click **Tickets**.
   c. Click the title of a ticket.
2. Select **Choose Action** > **Convert to process** > **Process Name**.

   A confirmation window appears.
3. Click **Yes** to continue to convert the ticket to a process.
4. Do one of the following:

   # Click **Save** to save the ticket and return to the *Ticket* list.
   # Click **Apply Changes** to save the ticket and continue editing it.
   # Click **Cancel** to discard the ticket changes.

   If other users have modified the ticket concurrently, the *Update Notification* dialog appears, provided that the dialog is enabled for the queue and you are the ticket owner or an administrator. This dialog is displayed to administrators and ticket owners only. It is not displayed to other users. Administrators can enable or disable the conflict warning message for each queue separately. See Enable or disable the conflict warning.

Using Ticket Rules

Ticket Rules enable you to run queries on Service Desk tickets and perform actions on the list of tickets returned.

For example, you could use a Ticket Rule to automatically change the status of a ticket from *Closed* to *Reopened* if someone other than the owner responds to the ticket. There are four default Ticket Rules, and you can add as many custom Ticket Rules as needed.

Using and configuring system Ticket Rules

You can use and configure system Ticket Rules to meet the needs of your Service Desk environment.

Options include:

- Enable the default Ticket Rule and use the default settings
- Create custom Ticket Rules
- Duplicate custom Ticket Rules
- Delete custom Ticket Rules
- Move Ticket Rules from one queue to another

Understanding and customizing system Ticket Rules

System Ticket Rules automatically change the status of Service Desk tickets, or send email notifications, when specified conditions are met.

The following table shows the names, behaviors, and usage of system Ticket Rules:

Ticket Rule	Default behavior	Can be copied and used to...
WaitingOverdue	Moves tickets that have been dormant for 7 days to an Overdue status.	Change a ticket status after waiting for a configurable time period. You can also send an email message when the status change happens.
OverdueClose	Closes tickets that have been Overdue with no action for 7 days.	Change a ticket status after waiting for a configurable time period. You can also send an email message when the status change happens.
EmailOnClose	Sends an email message to the ticket submitters when their ticket is closed. Closed tickets require a response only if the ticket is being reopened.	Send an email message when a ticket is closed.
CustomerResponded	Moves ticket to a Responded status when a user responds to a ticket that has been waiting for customer action.	Change an open ticket's status and send an email message if it is updated.
ReopenTicket	Reopens a closed ticket if someone other than the owner responds to it.	If a closed ticket is reopened, this Ticket Rule can change the ticket's status and send an email message.

Create custom Ticket Rules

You can create custom Ticket Rules for Service Desk tickets as needed.

1. Go to the Service Desk *Queue Detail* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Service Desk**, then click **Configuration**.

c. On the **Service Desk Configuration** panel, in the **Rules** section, click **Create and manage custom ticket rules** link.

d. Select the queue name.

2. Select **Choose Action** > **New (Wizard)** to display the *Define Ticket Rule* panel.
3. Enter the criteria required to choose the tickets for the custom Ticket Rules. For example:

```
Priority | = | Medium
```

4. Click **Test** to display tickets that match the criteria.
5. Click **Next**.
6. Select the values you want to change to. For example:

```
Priority | change value to | High
```

7. Click **Done** to display the *Ticket Rule Detail* page.
8. Provide the following information:

IMPORTANT: Do not edit SQL queries without understanding the consequences. Incorrect SQL statements might reduce appliance performance.

Option	Description
Name	The name of the Ticket Rule.
Order	A number specifying the evaluation order level. The Ticket Rule runs according to the evaluation order specified. Lower numbers run before higher numbers.
Queue	(Read only) The name of the queue to which the ticket belongs.
Description	Any additional information you want to provide.
Enabled	The Ticket Rule is available. The Ticket Rule runs only if it is enabled.
Select SQL	Modify the SQL query as needed. The query is generated by the Ticket Rule wizard based on the criteria specified on the *Ticket Rule* page. The query returns a set of ticket IDs that the **Update Query** operates on. The **Select Query** runs according to the specified frequency. To view results of the query, click **View Ticket Search Results**. **IMPORTANT: Do not edit SQL queries without understanding the consequences. Incorrect SQL statements might reduce appliance performance.**
Email results	Send the results of the Select Query to the specified email addresses. All columns returned by the Select Query are included in the email. Enter the email addresses in the *Email* field; use commas to separate addresses.
Append comment to ticket	Add a comment to each ticket returned by the Select Query. This action is useful in case the Update Query specified later updates a ticket without logging that information. For example, add a message such as Ticket Rule: Increase Priority to High triggered. Having this message gives you an indication of which tickets have changed. Enter any comments in the *Comment* field.
Email each recipient in query results	Send text to the email addresses returned by the Select Query. An email is sent to each email address returned by the Select Query in the *Email* column.

Option	Description
	Variables are evaluated in the subject line or body of the email. Strings such as $title and $due_date are replaced by the values in the *TITLE* and *DUE_DATE* columns respectively. Any column returned by the Select Query can be replaced in that way. The SQL generated by the Ticket Rule wizard supplies **OWNER_**, **SUBMITTER_**, and **CC_LIST** as possible values. Enter the subject in the *Subject* field. Enter the email column name in the *Email* field, for example, OWNER_. Email is sent to each email address returned by the Select Query in this *Email* column. Enter an email message in the *Email Body* field.
Run update query	Run a second database query using the results from *Update Query* field as input. Use this field to run an additional SQL UPDATE statement using the comma-separated list of tickets returned by the Select Query as input. For example, “update HD_TICKET set TITLE = 'changed' where HD_TICKET.ID in (<TICKET_IDS>)” turns into “update HD_TICKET set TITLE = 'changed' where HD_TICKET.ID in (1,2,3)” Modify the SQL query as needed. The query is generated by the Ticket Rule wizard based on the criteria specified on the *Ticket Rule* page. This query operates on the tickets selected by the **Select Query**. The *Update Query* runs according to the specified frequency. **IMPORTANT: Do not edit SQL queries without understanding the consequences. Incorrect SQL statements might reduce appliance performance.**
Recalculate Due Dates	Select this option only if your update query involves updating the priority of existing tickets. Selecting this option recalculates the due dates based on the new priority being set by the ticket rule. **NOTE:** If any of the tickets contain a manually overridden due date, it will not be overridden by ticket rules.
Last Run Log	The last query results, including any failures or errors. These results are updated each time the Ticket Rule runs.
Frequency	The interval at which the Ticket Rule runs. **NOTE:** Ticket Rules that run *on Ticket Save* should be designed to operate on a single ticket and trigger a single event. Ticket Rules that run on a schedule can run against multiple tickets and trigger multiple events.
Next Run	The date and time the Ticket Rule is scheduled to run again.

9. Click **Run Now** to immediately run the Ticket Rule.
10. Click **Save**.

Duplicate a custom Ticket Rule

When you duplicate a custom Ticket Rule, its properties are copied into the new rule. If you are creating a rule that is similar to an existing rule, duplicating the Ticket Rule can be faster than creating a rule from scratch.

1. Go to the Service Desk *Queue Detail* page:

a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
b. On the left navigation bar, click **Service Desk**, then click **Configuration**.
c. On the *Service Desk Configuration* panel, in the *Rules* section, click **Create and manage custom ticket rules** link.
d. Select the queue name.

2. In the *Ticket Rules* section at the bottom of the page, click **[Customize]** to display the *Ticket Rules* page.
3. Select a Ticket Rule to open it.
4. Click the **Duplicate** button at the bottom of the page.

   The *Ticket Rules* page appears, with the new rule listed. The default name is Copy of original_rule.
5. Change or rename the duplicated Ticket Rule as needed.

For information about Ticket Rule fields, see Create custom Ticket Rules.

Delete a custom Ticket Rule

You can delete custom Ticket Rules from the Service Desk as needed.

1. Go to the Service Desk *Queue Detail* page:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Service Desk**, then click **Configuration**.
   c. On the *Service Desk Configuration* panel, in the *Rules* section, click **Create and manage custom ticket rules** link.
   d. Select the queue name.
2. Do one of the following:
   - **Select the check box beside the Ticket Rule, then select Choose Action > Delete.**
   - **Click the name of the Ticket Rule, then on the *Ticket Rule Detail* page, click Delete.**
3. Click **Yes** to confirm.

Move a Ticket Rule from one queue to another

If you have multiple Service Desk ticket queues, you can move Ticket Rules between queues as needed. If you want the Ticket Rule to exist in multiple queues, you can copy the rule and make the required changes.

1. Go to the Service Desk *Queues* list:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Service Desk**, then click **Configuration**.
   c. On the *Service Desk Configuration* panel, in the *Rules* section, click **Create and manage custom ticket rules** link.
2. Select the queue that includes the Ticket Rule you want to move. The *Queue Detail* page appears.

   TIP: To move between queues on the *Ticket Rules* page, use the *View By* drop-down list, which appears above the table on the right.
3. Select the check box next to the Ticket Rule.
4. Select **Choose Action > Move > Queue Name**.

The Ticket Rule is moved to the selected queue. The rule no longer appears in the list of rules for the current queue.

Run Service Desk reports

You can run reports on Service Desk items as needed.

The appliance includes a set of pre-configured reports for Service Desk data.

1. Go to the *Reports* list:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Reporting**, then click **Reports**.
2. In the *View By* drop-down list, which appears above the list on the right, select **Service Desk**.

    The *Reports* page shows Service Desk reports.
3. In the *Generate Report* column, click a format type to run the report.

NOTE: For more information on reports, see About reports.

Archiving, restoring, and deleting tickets

Archiving tickets involves physically moving ticket data out of the transactional tables while preserving access to ticket data. Archiving does not permanently remove ticket data from the appliance. This is useful for old tickets that you might still need to reference.

When tickets are archived, they remain available until they are manually deleted or deleted based on the date constraints configured in the queue. This restriction reduces the possibility of deleting tickets accidentally.

A typical life cycle for tickets involves creation, resolution, archiving, and finally deleting. You can also “restore” a ticket as discussed in Restore archived tickets. Restoring tickets returns the ticket data from an archive table back into a transactional table for use, making ticket data available again in the *Tickets* tab.

Deleting tickets permanently deletes the ticket data from the appliance.

Enable ticket archival

You can enable ticket archival for the Service Desk, or if the Organization component is enabled, for the Service Desk of the selected organization.

1. Go to the *Service Desk Settings* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Service Desk**, then click **Configuration**.
    c. On the *Service Desk Configuration* panel, in the *Settings* section, click the *Customize Service Desk terminology* link and Go to Archival/Merge tab **Or** under the *Setting* section, select **Enable ticket archival** link to directly go to **Ticket Archival/Merge**.
2. In the *Ticket Archival/Merge* section, select the **Enabled** check box to display scheduling options.
3. Specify the following settings:

NOTE: If you do not want to perform ticket archiving on a schedule, click **Run Now** to archive and delete tickets any time. This option affects all queues for which archiving is configured. **Run Now** is also available from each queue and uses the settings from that queue when archiving and deleting tickets.

Option	Description
Every __ hours	Run at a specified interval.
Every day/specific day at HH:MM	Run daily at a specified time, or run on a designated day of the week at a specified time.
Run on the nth of every month/specific month at HH:MM	Run on the same day every month, or a specific month, at the specified time.
Run on the nth weekday of every month/specific month at HH:MM	Run on the specific weekday of every month, or a specific month, at the specified time.

Custom	Run according to a custom schedule.
	Use standard 5-field cron format (extended cron format is not supported):
	`* * * * *`
	`| | | | +————————day of week (0-6)(Sun=0)`
	`| | | +————————month (1-12)`
	`| | +————————day of month (1-31)`
	`| +————————hour (0-23)`
	`+————————minute (0-59)`
	Use the following when specifying values:
	• **Spaces ( )**: Separate each field with a space.
	• **Asterisks (*)**: Include the entire range of values in a field with an asterisk. For example, an asterisk in the hour field indicates every hour.
	• **Commas (,)**: Separate multiple values in a field with a comma. For example, `0,6` in the day of the week field indicates Sunday and Saturday.
	• **Hyphens (-)**: Indicate a range of values in a field with a hyphen. For example, `1-5` in the day of the week field is equivalent to `1,2,3,4,5`, which indicates Monday through Friday.
	• **Slashes (/)**: Specify the intervals at which to repeat an action with a slash. For example, `*/3` in the hour field is equivalent to `0,3,6,9,12,15,18,21`. The asterisk (`*`) specifies every hour, but `/3` restricts this to hours divisible by 3.
	Examples:
	• `15 * * * *` Run 15 minutes after every hour every day
	• `0 22 * * *` Run at 22:00 every day
	• `0 0 1 1,6 *` Run at 00:00 on January 1 and June 1
	• `30 8,12 * * 1-5` Run weekdays at 08:30 and 12:30
	• `0 2 */2 * *` Run every other day at 02:00

Option	Description
View Task Schedule	Click to view the task schedule. The *Task Schedule* dialog box displays a list of scheduled. Click a task to review the task details. For more information, see View task schedules.

4. Do one of the following:
   - **Click Run Now to run immediately for all queues for which archiving has been configured. See Archive selected tickets.**
   - **Click Save.**

     Ticket archival is enabled for the Service Desk or, if the Organization component is enabled, for the selected organization. However, you must configure specific queues to select the tickets that you want to archive. See Configure queue archive settings.
     The *Service Desk > Archive* link appears on the left navigation bar.

Configure queue archive settings

When ticket archival is enabled, you can configure archive settings for each queue.

You have enabled ticket archival for the Service Desk. For information on enabling ticket archival see Enable ticket archival.

1. Go to the Service Desk *Queue Detail* page:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Service Desk**, then click **Configuration**.
   c. In the Service Desk Configuration panel in the **Queues** section, select **Modify configurations and preferences** link.
   d. Select the queue name.
2. In the *Preferences* section, select settings for ticket archival. click the **Settings** link to enable ticket archival.

NOTE: If Ticket Archival is turned off, see Enable ticket archival.

Option	Description
Archive closed tickets older than	The age of tickets to be archived. For example, if you select **3 months**, tickets are archived when three months have passed since the tickets were closed. To prevent tickets in the queue from being archived, select **Never**. Archived tickets can be restored to the queue if necessary. See Restore archived tickets.
Delete archived tickets older than	The age of tickets to be permanently removed from the archive. For example, if you select **6 months**, archived tickets are deleted from the archive when six months have passed since the tickets were archived. To prevent tickets in the queue from being deleted from the archive, select **Never**. Deleted tickets cannot be restored to the queue.

3. Click **Save** at the bottom of the page.
4. Click **Run Now** to archive and delete tickets that meet the criteria specified in *Archive Preferences*.

Archive selected tickets

When Service Desk ticket archival is enabled, you can archive selected tickets as needed.

You have enabled ticket archival for the Service Desk. For information on enabling ticket archival see Enable ticket archival.

TIP: Selecting tickets to archive is useful when you want to archive specific tickets, or if you do not set archiving to occur on a schedule, as discussed in Enable ticket archival.

1. Go to the Service Desk *Tickets* list:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Service Desk**, then click **Tickets**.
2. Select the check box next to one or more tickets.
3. Select **Choose Action** > **Archive**.
4. On the confirmation dialog, click **Yes**.
5. To access archived tickets, click **Service Desk** > **Archive**, then click the link for the ticket you want to view.

Restore archived tickets

Tickets that have been archived can be restored to the ticket queue as needed.

1. Go to the Service Desk *Archived Tickets* list:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Service Desk**, then click **Archive**.
2. Select the check box next to one or more archived tickets.
3. Select **Choose Action** > **Restore**, then click **Yes** to confirm.

The ticket is immediately restored to the *Tickets* tab.

Delete archived tickets

You can delete archived tickets to permanently remove them from the Service Desk. Deleted tickets cannot be restored.

1. Go to the Service Desk *Archived Tickets* list:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Service Desk**, then click **Archive**.
2. Select the check box next to one or more archived tickets.
3. Select **Choose Action** > **Delete**, then click **Yes** to confirm.

The ticket is immediately removed from the appliance.

Managing ticket deletion

By default, any Service Desk administrator or ticket owner can delete tickets from a queue. You can change that setting as needed. If you have multiple queues, you can have different settings for each queue.

Configure ticket deletion settings

You can configure Service Desk ticket deletion settings for queues. If you have multiple queues, you can configure different settings for each queue.

1. Go to the Service Desk *Queue Detail* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Service Desk**, then click **Configuration**.
    c. In the *Service Desk Configuration* panel in the *Queues* section, select **Modify configurations and preferences** link.
    d. Select the queue name.
2. In the *Preferences* tab, do one of the following:
    - **To prevent administrators and ticket owners from deleting tickets, clear the *Allow Ticket deletion* check box.**
    - **To enable administrators and ticket owners to delete tickets, select the *Allow Ticket deletion* check box.**
3. Click **Save**.

Delete tickets

If ticket deletion is enabled in the Service Desk queue settings, you can delete tickets as needed.

You have enabled ticket deletion for the queue. See Configure ticket deletion settings.

1. Go to the Service Desk *Tickets* list:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Service Desk**, then click **Tickets**.
2. Select the check boxes next to one or more tickets.
3. Select **Choose Action** > **Delete**, then click **Yes** to confirm.

Managing Service Desk ticket queues

By default, Service Desk has a single ticket queue, and in many cases, a single queue is all an organization requires to function effectively. However, you can add, duplicate, and delete queues as needed. You can also create one or more ticket templates in a queue. If multiple templates exist in a queue, you must select one ticket template as the default template.

About Service Desk ticket queues

Service Desk tickets are stored in one or more queues on the appliance. Most organizations need only a single queue, but you can create and manage additional queues as needed.

Having multiple ticket queues is useful when:

- **You have different sets of tickets with different requirements**. For example, if you use tickets for typical Service Desk tasks such as fixing device-related problems, and you also use tickets to keep track of problems with a fleet of automobiles, you can set up separate queues for each type of problem.
- **Service Desk staff are assigned to a specific set of tickets**. For example, if your organization has offices in different cities, and each city has a Service Desk staff dedicated to that location, you can manage tickets in separate queues. However, if your Service Desk staff handles multiple offices from a single location, a single queue is sufficient.

For information about configuring ticket queues, see Configuring Service Desk ticket queues.

Adding and deleting queues

You can add, duplicate, and delete queues as needed. This activity can be useful if you want to set up different types of tickets for different groups in your organization.

Add a queue

You can add Service Desk ticket queues as needed.

If you plan to move Service Desk tickets from one queue to another, be sure to use the same values, including custom fields, in each queue. Otherwise, data from the old queue is altered to match the new queue. See Move tickets between queues.

1. Go to the Service Desk *Queue Detail* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Service Desk**, then click **Configuration**.
    c. In the Service Desk Configuration panel in the **Queues** section, click **Create queues** link to create new queues.

    Or

    In the Service Desk Configuration panel in the Queues section, click Create and manage queues link.

    d. Select **Choose Action** > **New**.
2. Enter values for the *Name*, *Email Address*, and *Alternate Email Address* for the new queue.

    CAUTION: When delivering email to the appliance directly (forwarding email to the appliance), the local portion of the appliance address and the alternate address must match. For example, servicedesk@kbox and servicedesk@company.com.

    CAUTION: Each new queue must use its own unique email addresses. The appliance confirms this before allowing you to save the new queue. If you specify an email address that is already associated with another queue, a warning appears.
3. In the *Email Configuration* section, go to the *Inbound* tab and select the POP3 option. If you have set up a POP3 server, enter the POP3 email user ID and password in the *User / Password* fields.

    See About POP3 email accounts.

    TIP: When using POP to download email to the appliance, you can use any valid mailbox.
4. For the POP3 authentication, you can apply Secure Sockets Layer (SSL) to the queue by selecting the *SSL* check box.

Whether you select this check box depends on how you have configured your POP3 account.

5. Click **Save**.
6. Choose additional settings for the queue as needed. See Configuring Service Desk ticket queues.

Add a queue by duplicating an existing queue

When you duplicate or clone a queue, all data from the existing queue is copied into the new queue, which can be faster than adding a queue from scratch. Ticket Rules are copied to the duplicated queue, but they are disabled by default.

1. Go to the Service Desk *Queues* list:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Service Desk**, then click **Configuration**.
    c. On the **Configuration** panel, click **Create and manage queues** in **Queue** section.
2. Click the name of a queue to display the *Queue Detail* page.
3. Click **Duplicate** at the bottom of the page.

    The new queue contains the same name as the queue from which it was duplicated with an appended unique identifier number. By default, Ticket Rules are disabled in the new queue.
4. Change the name and settings of the queue as needed.
5. Click **Save**.

Delete a queue or queues

You can delete queues as needed.

CAUTION: Before you delete a queue, be sure that you want to delete all of the data in a queue. This includes associated tickets and processes. This action cannot be undone.

1. Go to the Service Desk *Queue Detail* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Service Desk**, then click **Configuration**.
    c. On the **Configuration** panel, click **Create and manage queues** in **Queue** section.
    d. Click the name of a queue.
2. At the bottom of the page, click **Delete**, then click **Yes** to confirm.

Viewing tickets in queues

You can sort the *Tickets* page to show all of the tickets in all of your queues in one list. If you have multiple queues, you can specify the queue to be displayed by default on the *Tickets* page.

If you have multiple queues, you can choose which queue to be displayed by default on the *Tickets* page. The default queue can be specified:

- **At the system level**. This setting is used if no user settings are specified. See Set the default queue at the system level.
- **At the user level**. This setting overrides the system level settings. Individual users and administrators who have permission to change user settings can specify the default queue at the user level. See Set the default queue at the user level.

View tickets across all queues

If you have multiple queues, you can view tickets from all queues in the same list.

1. Go to the Service Desk *Tickets* list:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Service Desk**, then click **Tickets**.
2. In the *Queue* drop-down list, which appears above the table, select **All Queues**.
3. In the *View By* drop-down list, to the right of the *Queue* drop-down list, select the group of tickets you would like to view.

If you have a high number of queues, use the search box to quickly find a specific queue.

Setting the default queue

If you have multiple queues, you can choose which queue to be displayed by default on the *Tickets* page.

The default queue can be specified:

- **At the system level**. This setting is used if no user settings are specified. See Set the default queue at the system level.
- **At the user level**. This setting overrides the system level settings. Individual users and administrators who have permission to change user settings can specify the default queue at the user level. See Set the default queue at the user level.

Set the default queue at the system level

The system-level default queue settings determine which ticket queue is displayed by default provided that user-level settings are not specified.

1. Go to the Service Desk *Settings* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Service Desk**, then click **Configuration**.
    c. On the *Service Desk Configuration* panel, click under **Settings** section click the **Customize Service Desk terminology** option.
2. On the *Service Desk Settings* page, under *Settings*, click *Customize Service Desk terminology* link and Go to *Queue Preference* tab

    Or

    under **Settings** section, click the **Set default queue** option to directly go to the **Queue Preference** tab

Select an option in the *Ticket List Default Queue* **drop-down list :**

Option	Description
No Default	Use no default when displaying queues. When this is selected, the first queue that was added to the system is displayed by default when users select **Service Desk** > **Tickets**. This setting is disregarded if a setting is specified at the user level.

Option	Description
All Queues	Display the *All Queues* view by default. When this is selected, the *All Queues* view is displayed when users select **Service Desk** > **Tickets**. This setting is disregarded if a setting is specified at the user level.
<Queue Name>	Display the selected queue by default. When this is selected, the specified queue is displayed when users select **Service Desk** > **Tickets**. This setting is disregarded if a setting is specified at the user level. If a queue does not appear on this list, verify that you have permission to view it.

TIP: These settings can be overridden at the user level. See Set the default queue at the user level.

3. Click **Save**.

Set the default queue at the user level

The user-level queue settings determine which ticket queue is displayed by default. User-level settings override system-level settings. Individual users and administrators who have permission to change user settings can specify the default queue at the user level.

If no user-level default queue is specified, the system-level default queue is used.

1. Go to the *User Detail* page:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Settings**, then click **Users**.
   c. Click the name of a user.
2. In the *Default Queue* drop-down list, select an option:

Option	Description
No Default	Use no default when displaying queues. When this is selected, the first queue that was added to the system is displayed by default when the selected user selects **Service Desk** > **Tickets**.
All Queues	Display the *All Queues* view by default. When this is selected, the *All Queues* view is displayed when the selected user selects **Service Desk** > **Tickets**.
<Queue Name>	Display the selected queue by default. When this is selected, the specified queue is displayed when the selected user selects **Service Desk** > **Tickets**. If a queue does not appear on this list, verify that you have permission to view it.

3. Click **Save**.

Set the default fields for the All Queues ticket list

You can specify the ticket fields you want to display in the *All Queues* view.

If you have multiple queues, the *All Queues* view is a useful way to view all of the tickets in your system on a single list.

For example, each queue might have different names for ticket fields. One queue might use the ticket field *Priority* and another queue might use the ticket field *Business Impact*. You can choose which field to display in the *All Queues* view.

Fields are displayed according to these settings:

- The field names used in the queue selected as the *Default Queue for All Queues View Field Labels*
- The fields specified in the *Customize List Layout for All Queues View* setting

1. Go to the Service Desk *Settings* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Service Desk**, then click **Configuration**.
    c. On the *Service Desk Configuration* panel, in the **Layout** section, click *Customize "All Queues" tickets list* link.
2. In the *Queue Preferences* section, select a queue in the *Ticket List Layout for All Queues* drop-down list.

    The field names from this queue appear on the *Tickets* page.
3. Modify the fields using the following icons:
    # : Add a field.
    # : Change the field name or the width of the field column.

    NOTE: The width indicates the amount of available page width that is assigned to the field column. For example, if you have 10 columns, and each column is assigned a width of 10, the total of all numbers in the *Width* column would be 100. Therefore, each field column would have a width of 10 percent of the available page width. If the total of all numbers in the *Width* column is more or less than 100, the numbers are normalized to percentages to determine the width. For example, if you have three columns, and you assign a width of 10 to each column, the total of all numbers in the Width column would be 30. However, when normalized to percentages, the width of each column would be approximately 33.3 percent.

    TIP: The field column widths specified in the *All Queues View* overrides the properties of individual queues.

    # : Drag and change the order in which the fields are displayed.
    # : Delete the field.
4. For each field you edit, click **Save** at the end of the row.

    The default queue settings are saved.
5. To see the new settings:
    a. Select **Service Desk** > **Tickets** to display the page.
    b. In the *Queue* drop-down list, select **All Queues**. In the *View By* drop-down list, select **All Tickets**.

    Fields from the selected queue appear on the list in the order specified in the queue settings.

    CAUTION: When the system displays Active Tickets or All Tickets in the *All Queues* view, the *Choose Action* menu and *View By* drop-down list use default settings. Customizations that appear in individual queues are not available in the *All Queues* view.

Move tickets between queues

If you have multiple queues, you can move tickets between them as needed.

When you move a ticket to different queue, the ticket's original settings, such as status, impact, priority, or category are overwritten by the settings in the queue to which it is being moved. The ticket change history stores the original values.

The following example shows how a custom field is treated when tickets are moved between queues:

1. The *CUSTOM_1* field in the ticket being moved lists the root cause of the problem as **Pilot Error**.
2. The *CUSTOM_1* field in the target queue lists locations, such as **Tampa**, **Los Angeles**, and **Denver**.

   The CUSTOM_1 value, **Pilot Error**, is retained in the ticket being moved.
3. If you change the *CUSTOM_1* value of the ticket being moved to **Tampa**, the **Pilot Error** value is no longer available for the ticket that has been moved.

1. Go to the Service Desk *Ticket Detail* page:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Service Desk**, then click **Tickets**.
   c. Click the title of a ticket.
2. Select **Choose Action** > **Move to queue** > **queue name**.

   If you have a high number of queues, use the search box to quickly find a specific queue.
3. Click **Yes** to confirm the ticket move.
4. Click **Save** to save the ticket in the new queue.

Bulk edit tickets in a queue

The bulk ticket update feature allows you to edit one or more fields of multiple tickets at the same time. The tickets must belong to the same queue. You can only bulk edit tickets if you are the queue owner.

Performing a bulk edit against a set of tickets does not affect ticket rules. Any ticket rules associated with the tickets you bulk edit continue to run, as configured. For more information about ticket rules, see Using Ticket Rules.

1. Go to the Service Desk *Tickets* list:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.

b. On the left navigation bar, click **Service Desk**, then click **Tickets**.

2. In the *Queue* drop-down list, which appears above the table, select a queue containing the tickets that you want to edit.
3. On the *Tickets* list page, select the tickets that you want to bulk edit.
4. Select **Choose Action** > **Bulk Ticket Update**.
5. In the *Bulk Ticket Update* dialog box that appears, in the *Field Name* column, select a field whose value you want to update. Then, in the *Field Value* column, set the value that you want to assign to the selected field.

   # To add a field to this bulk edit, click **Add field to update**, and specify the field's name and value.

   # To delete a field from the list, in the *Action* column, click *Remove item*.

   # To suppress email notifications to the applicable users about this change, select **Supress Notifications**.

   # When editing the *CC List* field, any email addresses you add are appended to the existing CC list. To replace the items in the CC list with the values you provide here, ensure the **Append to existing CC list** check box is cleared.

   # Bulk edits of the *Comment* field does not replace the existing comments, it only adds a new comment to the existing ones.

   # Failing to provide the value of a required field results in an error.

   # Bulk update does not allow you to change the ticket Status. You can bulk edit this field using the commands from the **Choose Action** menu.

   # When done, click **Save**.

About User Downloads and Knowledge Base articles

You can distribute software, scripts, and other downloadable files to users through the **User Console**. In addition, you can make Knowledge Base articles available for users to view in the **User Console**.

To enable users to access the **User Console**, you must create user accounts on the appliance or enable LDAP authentication. See About user accounts and user authentication.

Managing User Downloads

You can create, label, and delete *User Downloads* using the **Administrator Console**.

To make items available in the **User Console**, you must upload them in the *User Downloads* section of the **Administrator Console**. See Add User Downloads.

To run installers and scripts, users must have the KACE Agent software installed on their devices. See About managing devices.

To limit user access to downloadable items, select the device labels to which the items apply, or apply labels to the items themselves. See Apply labels to User Downloads.

Add User Downloads

You add software, scripts, and other downloadable files to the **User Console** using the **Administrator Console**.

All items that you want to add to the **User Console** must already exist in the appliance *Inventory* or *Scripting* sections. You cannot create software or scripts using the **Administrator Console**.

TIP: Software distribution is available for items on the *Software* page and for Agent-managed devices only. It is not available for items on the *Software Catalog* page or Agentless devices.

1. Go to the *User Downloads Detail* page:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Service Desk**, then click **User Downloads**.
   c. Select **Choose Action** > **New**.
2. Select the **Enabled** check box to make the item visible on the User Console; clear the check box to hide the item.
3. In the *Configure* section, select a *Type*:

Option	Description
Download	Select one of the following options: • **Cataloged Software**: Choose this option to select an item from the software catalog that includes one or more associated files. First select the application, and then the file that you want to be available for download. An application in the software catalog can include multiple files, such as installers for different application versions and platforms. **TIP:** When you add a cataloged software item to user downloads, the *User Downloads* (**Administrator Console**) and *Downloads* (**User Console**) pages display some additional information about that application in the *Category*, *License Type*, *Platform*, *End of Life*, *General Availability*, and *MSRP ($)* columns. For more information about cataloged software, see About the Software Catalog and View details of Software Catalog applications. • **Software**: Create an item that downloads documentation, files, or other software that does not install automatically.
Install	Create an item that runs a software program on the user's device. A device must have the Agent installed to run installations. Select one of the following options: • **Use existing Managed Install**: Choose this option to select an existing Managed Installation (MI). Each MI includes a specific application title and version to be installed or removed, including installation commands, installation files, and target devices (identified by label). For more information, see Using Managed Installations. • **Default Installation**: Choose from the programs available in **Inventory** > **Software**. You must include both the installation File Name and associated Parameters in the **Enter Parameters** box. For more information, see About the Software page.
Script	Create an item that runs a script on the user's device. Choose from the scripts available in **Scripting** > **Scripts**. Devices must have the Agent software installed to run scripts.

4. If you selected the **Install** package type in the previous step, enter the parameters required to run the installation, including any necessary installation switches or parameters.
5. Specify the information to include:

Field	Description
Product Key	Send the product key to users when they download the application. To view *Asset Detail* license information, click **Assets**.

Field	Description
Unit Cost	(Optional) The cost per unit.
Installation Instructions	Instructions, legal notes, or any other information you want to upload to the **User Console** along with the application.
Description	Any additional information you want to provide.
Vendor License	(Optional) Any vendor-specific license text.
Corporate Licensing Policy	(Optional) Any organization-specific license text.
Email Product Key to End User	Send the product key to users when they download the application. To view *Asset Detail* license information, click **Assets**.
Notify Manager	Require users to enter their manager's email address before enabling them to download or install applications.
Attachment	(Optional) The file to be included as documentation. The file size appears after the item is saved.

6. In the *Access Control* section, specify distribution restrictions:

Field	Description
Assign to User Labels	(Optional) Click **Manage Associated Labels** and select a label to limit application deployment to users who are included in the label.
Restrict User Labels to Assigned Devices	(Optional) Limits access to this User Download package only to those users and devices associated with the selected label.
Requires Approval	(Optional) Select this check box if you want to the end user to obtain one or more approvals to download the software, and configure the following fields: • **Approval Process Template**: Select the process template containing the desired approval process. The process template must be based on the *Software Request: Approval Required* process type which applies to software download requests. • **Approval Frequency**: Indicate how often you want the user to request a permission to download the selected software: *One-time Approval* or *Every Download Approval*. **NOTE:** When an end user attempts to download an item that requires approval, the system automatically creates a ticket using the configured process template. Approvers are automatically notified. Upon approval, the user receives a notification and can proceed to download the selected item.

7. Click **Save**.

Apply labels to User Downloads

You can use labels to group User Downloads. This is useful for managing and distributing multiple items at once and for restricting access to items.

1. Go to the *User Downloads* list:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Service Desk**, then click **User Downloads**.
2. Select the check box next one or more items.
3. Select **Choose Action** > **Apply Labels**.
4. Drag a label to the *Apply these labels* field, then click **Apply Labels**.

The label is listed next to the item in brackets.

Remove labels from User Downloads

You can remove labels from User Downloads as needed.

1. Go to the *User Downloads* list:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Service Desk**, then click **User Downloads**.
2. Select the check box next to an item.
3. Select **Choose Action** > **Remove Labels**.
4. Click the **Delete** button next to the label you want to remove: .
5. Click **Remove Labels**.

The label is removed from the item.

Delete User Downloads

You can delete User Downloads as needed.

1. Go to the *User Downloads* list:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Service Desk**, then click **User Downloads**.
2. Select the check box next to one or more items.
3. Select **Choose Action** > **Delete**, then click **Yes** to confirm.

Managing Knowledge Base articles

You add, edit, duplicate, and delete Knowledge Base articles using the **Administrator Console**.

Users can search for articles by keyword, and sort by article ID, Title, Category, Platform, or Importance in the **User Console**. Users can also rate the helpfulness of Knowledge Base articles.

To insert Knowledge Base article text into Service Desk tickets, click the **Find Related Articles** link on ticket pages.

Add, edit, or duplicate Knowledge Base articles

You can add, edit, and duplicate Knowledge Base articles. These articles are available to users in the **User Console**.

1. Go to the *Article Detail* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Service Desk**, then click **Knowledge Base**.
    c. To display the *Article Detail* page, do one of the following:
    # Click the name of an article.
    # Select **Choose Action** > **New**.
2. Provide the following information:

Field	Description
Title	A specific description of the issue covered in the Knowledge Base article. Write descriptive titles and use common terms to make it easy for users to find information.
Category	A general description of the type of issue, for example, “printing” or “network access.”
Platform	The operating systems to which this Knowledge Base article applies.
Importance	The value of the Knowledge Base article. For example, “reference” or “low”; or “critical” or “high.”
Restrict to Labels	To limit access to the article to specific sets of users, select the appropriate user labels from the list. If this field is empty, all users who have access to the **User Console** can see the Knowledge Base article.
Text	The content of the Knowledge Base article. This field includes a full range of text editing options for formatting your content, such as buttons for bold text, hyperlinks, lists, text color, embedding images and videos.

Field	Description
	For example: • To apply bold text to a text string, select it in the editor, and click B. • You can add images to Knowledge base articles using three different methods. To do that, click, and in the image panel that appears, complete one of the following steps: # To navigate to a file from your computer and upload it to the article, click. Any images added this way will be automatically saved as attachments to the KB article. # To link to a file that is hosted elsewhere or is a part of another KB article, click. # To link to a file that is already attached to the KB article, click. • To add external links, or links to other KB articles, click. • To attach a file, click. Any files uploaded using this option are saved as attachments to this KB article. • To embed an externally hosted video, click. • When you remove an image file from the article content, but do not delete the file attachments, you can add them back to the article content. To do that, click, and in the image panel that appears, click. • To delete a file attachment, click

3. **Optional**: In the *Attachments* section, click **Add**, then click **Browse** or **Choose File** to add an attachment.
4. Click **Save**.

   TIP: To create a Knowledge Base article from the comments in a ticket, click **Create KB article** on the *Ticket Detail* page.

   The appliance assigns the Knowledge Base article an Article ID and displays it on the *Knowledge Base* page. To see how the Knowledge Base article appears to users in the User Console, click the Knowledge Base article's title on the *Knowledge Base* page, then click the User URL on the *Article Detail* page.
5. **Optional**: Click **Duplicate**.

Delete Knowledge Base articles

You can delete Knowledge Base articles to permanently remove them from the appliance.

1. Go to the *Knowledge Base Articles* list:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Service Desk**, then click **Knowledge Base**.
2. Select the check box next to one or more articles.
3. Select **Choose Action** > **Delete**, then click **Yes** to confirm.

View user ratings and the number of views for Knowledge Base articles

You can view user ratings for Knowledge Base articles as well as the number of times Knowledge Base articles have been viewed.

1. Go to the Knowledge Base *Article Detail* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Service Desk**, then click **Knowledge Base**.
    c. Click the name of an article.

    The current user rating for the article and the number of page views appear at the bottom of the page.
2. Mouse over the stars to view the definitions of the five-star rating system.

    On the scale, 1 star is low, 5 stars are high.

> **NOTE:** Users can change their ratings. However, the database stores only the user's most recent rating for each article.

Customizing Service Desk ticket settings

You can customize Service Desk ticket settings to meet the needs of your users and your environment. If you have multiple queues, you can customize ticket settings for each queue separately.

About customizing Service Desk ticket settings

You can customize ticket values, add custom fields, create ticket categories, and create ticket sub-categories to meet your Service Desk requirements.

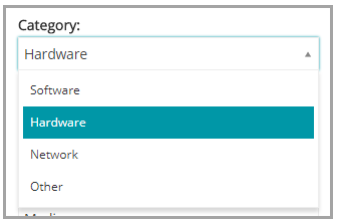
Default ticket values include category, status, priority, and impact.

- Ticket characteristics include:
    # Field name
    # Field order displayed on the ticket
    # Whether the field is required or not
    # Who has permission to change the field
- Custom field definitions include:
    # Field type (check box, date, timestamp, link, multiple select, notes, number, single select, text, or user)
    # Acceptable values for the field
    # The default value for the field

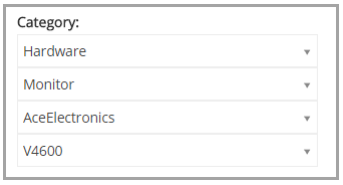
Create ticket categories and subcategories

You can create ticket categories and subcategories as needed. Categories and subcategories are queue-specific, and they become available to all new and existing tickets in the selected queue when they are created.

You can add as many ticket categories as you need, each with one or more subcategories. For example, in the ticket category *Hardware*, you might want to have a subcategory such as *Monitor*. These categories would appear on the *Ticket Detail* page as:



When users select the *Monitor* subcategory, you might want to display additional subcategories, such as model information:



Most customers use a two-tiered approach to categories and subcategories. They create general categories and subcategories for users, such as:

- Hardware – Monitor

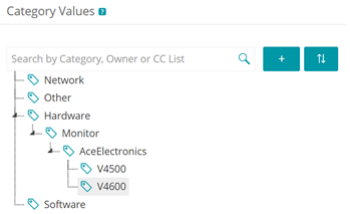
Then they create additional subcategories with model information for Service Desk staff, such as:

- Hardware – Monitor – AceElectronics – V4500
- Hardware – Monitor – AceElectronics – V4600

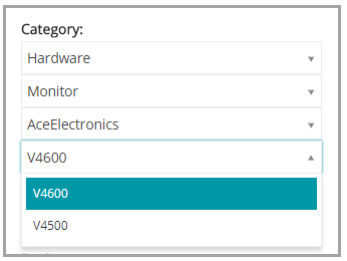
1. Go to the Service Desk *Queue Detail* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Service Desk**, then click **Configuration**.
    c. On the **Configuration** panel, click **Create and manage queues** in **Queue** section.
    d. To display the *Queue Detail* page, do one of the following:
    # Click the name of a queue.
    # Select **Choose Action** > **New**.
2. In the *Queues* section, click **Customize fields** to display the *Queue Customization* page.

    On the *Queue Customization* page, in the *Category Values* tab, the *Tree View* tab opens by default, allowing you to create and manage ticket categories and subcategories. You can review existing categories and sub-categories in list form on the *List View* tab, if needed.
3. Create and edit ticket category and subcategory nodes using the tree widget, as required.
    - **To add a new root category, click , and specify the category name.**
    - **To add a new subcategory, right-click the parent category node, and in the menu that appears, choose Create.**

    On the *Queue Customization* page, categories and subcategories appear as follows:



On the *Ticket Detail* page, categories and subcategories appear as follows:



- **To rename a category, right-click the category note, choose Rename in the menu, and type the new name.**
- **To delete a category, right-click the category note, choose Delete in the menu, and in the *Confirm* dialog box that appears, click Yes.**
- **To sort all subcategories in a category, right-click the category note, and in the menu, choose Sort > Ascending or Sort > Descending, as applicable.**
- **To sort all categories and their subcategories in ascending order, click , and in the *Confirm* dialog box that appears, click Yes.**

  NOTE: Deleting a category does not remove its subcategories from the tree.

- **To find a specific category, start entering the category name in the search box. The matching results appear highlighted in the tree widget as you type.**
- **To move a category, drag the category node to a desired position in the tree.**

4. To edit a category, select it in the tree, and provide the following information in the area on the right. When you finish making changes to the category, click **Add**.

Field	Description
Default Owner	The user that is automatically assigned as owner of the ticket category or subcategory when tickets are created. If you move an existing ticket to a category with a different default owner, the owner of the ticket does not automatically change. The owner of the ticket must be changed manually.
CC List	Clear this check box to prevent the CC List from being displayed on tickets. Because **DefaultTicketOwners** is the default owner, all potential ticket owners receive an email when a ticket is created.
User Settable	Allows users to change the corresponding category. Clear the check box to reserve the action for Service Desk staff only. Users see categories even if they cannot change them.

5. Click **Save** at the bottom of the page or continue editing ticket values.

The new categories and subcategories appear on the *Ticket Detail* page and are available to new and existing tickets.

Customizing ticket values

You can customize the values available for ticket status, ticket priority, and ticket impact.

Customize ticket status values

You can customize the values that indicate ticket status, such as open or closed.

IMPORTANT: Status values are often used in Ticket Rules. Make sure you review your Ticket Rules and understand how status values are used in those rules before you modify status values. See About Ticket Rules.

1. Go to the Service Desk *Queue Detail* page:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Service Desk**, then click **Configuration**.
   c. On the **Configuration** panel, click **Create and manage queues** in **Queue** section.
   d. To display the *Queue Detail* page, do one of the following:
   # Click the name of a queue.
   # Select **Choose Action** > **New**.
2. In the *Queues* section, click **Customize fields** to display the *Queue Customization* page.
3. In the *Status Values* tab, click the **Edit** button beside a value to modify it: , or click the **Add** button at the top of the list to add a new value, +
4. Edit the *Status Values* fields:

Field	Description
Name	The name for the status value.
State	The state assigned to the status value. • Opened: The ticket is active. Only this State can be escalated. See Using the ticket escalation process. • Closed: The ticket has been resolved. • Stalled: The ticket is open past its due date, but is not in escalation.

5. Click **Save** in the row.

To update categories, use the icons to the right of each row:

: Change the sort order of columns.
+: Add a field.
: Change the values.
: Change the order of values.
: Remove the values.

NOTE: You cannot remove a value if it is in use, or if it is the default ticket value. To remove a value that is being used, add a value, then, in the ticket where the value is used, change the old value to the new value. When the old value is no longer in use, the **Delete** button appears next to the value: .

6. Click **Save** at the bottom of the page or continue editing ticket values.

Customize ticket priority values

You can customize the values that indicate ticket priority as needed.

1. Go to the Service Desk *Queue Detail* page:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Service Desk**, then click **Configuration**.
   c. On the **Configuration** panel, click **Create and manage queues** in **Queue** section.
   d. To display the *Queue Detail* page, do one of the following:
   # Click the name of a queue.
   # Select **Choose Action** > **New**.
2. In the *Queues* section, click **Customize fields** to display the *Queue Customization* page.
3. In the *Priority Values* tab, click the **Edit** button beside a value to modify it: , or click the **Add** button at the top of the list to add a new value, .
4. Edit the *Priority Values* fields:

Field	Description
Name	Enter a name for the custom field.
Color	(Optional) Select a color to use for this status on the ticket list pages.

5. Click **Save** in the row.
6. Use the icons to the right of each row to modify additional values:
   # : Change the sort order of columns.
   # : Add a field.
   # : Change the values.
   # : Change the order of values.
   # : Remove the values.

   NOTE: You cannot remove a value if it is in use, or if it is the default ticket value. To remove a value that is being used, add a value, then, in the ticket where the value is used, change the old value to the new value. When the old value is no longer in use, the **Delete** button appears next to the value: .
7. Click **Save** at the bottom of the page to save changes and return to the *Queue list* page.

Customize ticket impact values

You can customize the values that indicate ticket impact.

NOTE: Only ticket owners can categorize tickets using the *Category* and *Priority Values* fields. Ticket submitters can make this type of assessment in the ticket *Impacts* field.

1. Go to the Service Desk *Queue Detail* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Service Desk**, then click **Configuration**.
    c. On the **Configuration** panel, click **Create and manage queues** in **Queue** section.
    d. To display the *Queue Detail* page, do one of the following:
    # Click the name of a queue.
    # Select **Choose Action** > **New**.
2. In the *Queues* section, click **Customize fields** to display the *Queue Customization* page.
3. In the *Impact Values* tab, click the **Edit** button beside a value to modify it: , or click the **Add** button at the top of the list to add a new value, +
4. Modify the *Name* field as needed.
5. Click **Save** in the row.

    The icons to the right of each row enable the category to be updated.

    # : Change the sort order of columns.
    # +: Add a field.
    # : Change the values.
    # : Change the order of values.
    # : Remove the values.

    NOTE: You cannot remove a value if it is in use, or if it is the default ticket value. To remove a value that is being used, add a value, then, in the ticket where the value is used, change the old value to the new value. When the old value is no longer in use, the **Delete** button appears next to the value: .
6. Click **Save** at the bottom of the page or continue editing ticket values.

Customizing ticket layout

You can customize the way tickets are displayed on the *Tickets* page for each queue.

Customization options include:

- Change the order of most of the default fields or hide them.
- Add one or more custom fields; the number is restricted only by the number of columns you can have in a table. Specify static values for these fields or pull the values from a database dynamically using a database query.
- Customize ticket views and set read/write access for users, ticket owners, and administrators. This includes the ability to hide, view, view but not change, or change individual ticket fields for each of these roles.
- Preview the customized ticket page, to ensure that the resulting layout meets your needs.
- Set up parent-child ticket relationships between tickets and either prohibit the parent from closing until all the child tickets are closed, or allow the parent ticket to close all the child tickets. See Using parent-child ticket relationships.
- Prevent a ticket from being opened or closed without the required approval. Or, require approval only when a ticket closes. See Using ticket approvers.

TIP: Remember that the changes you make here are automatically propagated to all existing tickets in the queue.

Customize Layout and Related Ticket Fields

You can customize the way the *Layout Ticket Fields* and *Related Ticket Fields* are displayed on the *Ticket Detail* page.

1. Go to the Service Desk *Queue Detail* page:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Service Desk**, then click **Configuration**.
   c. On the **Configuration** panel, click **Create and manage queues** in **Queue** section.
   d. To display the *Queue Detail* page, do one of the following:
   # Click the name of a queue.
   # Select **Choose Action** > **New**.
2. Under the Queues section, click **Customize Fields** to display the *Queue Customization* page. Then go to the *Related Ticket Information*, and *Default Ticket Layout*::

Section	Description
Layout Ticket Fields	This section includes the *Survey*, *Title*, and *Summary* fields, the *Submitter*, *Asset*, and *Device* sections, and any other fields that are not displayed in the *Related Ticket Fields* section. This section also includes any custom fields. Fields in this section can be freely moved around within this section and they appear on the *Ticket* page in the specified order. All fields in this section are displayed in a two-fields-per-row format except the *Resolution* field, which occupies a full row. **NOTE:** If the *Summary* field is hidden, the *Comment* field is displayed on the *New Ticket* page. Text entered in the *Summary* field is stored as the first comment, and the first comment is stored as the Summary in order to maintain backward compatibility.

Section	Description
Related Ticket information tab	This section includes fields that capture information about related tickets. You can hide these fields, but you cannot change their position. • *PARENT_INFO*: Tickets that have a parental relationship to the selected ticket. • *SEE_ALSO*: Tickets that are similar to, or provide additional information about, the selected ticket. • *REFERERS*: Users who have referenced the ticket.

3. Click the **Edit** button next to the field you want to customize .
4. In the *Label* and *Required* fields, choose options to use:

Section	Description
Label	The name you want to appear next to the field on the *Ticket Detail* page.
Required	Whether the field is required or optional. • **Not Required**: The field is never required. It can be left blank. • **Always Required**: The field cannot be left blank. It must be completed before tickets can be saved. • **Required on Close**:Tickets cannot be closed until the field is completed.

5. In the *Permissions* field, choose the permission setting to use:

Permission setting	Can be viewed by	Can be changed by	Can be created by
Hidden	No one	No one	No one
Read Only	Users, Ticket Owners, Administrators*	No one	No one
Owners Only - Hidden from Users	Ticket Owners, Administrators*	Ticket Owners, Administrators*	Ticket Owners, Administrators*
Owners Only - Visible to Users	Users, Ticket Owners, Administrators*	Ticket Owners, Administrators*	Ticket Owners, Administrators*
User Create	Users, Ticket Owners, Administrators*	Ticket Owners, Administrators*	Users, Ticket Owners, Administrators*
User Create & Modify	Users, Ticket Owners, Administrators*	Users, Ticket Owners, Administrators*	Users, Ticket Owners, Administrators*

* Indicates the default setting. You can remove this default setting by clearing the following check box on the *Queue Detail* page: *Allow users with an Administrator role to read and edit tickets in this queue (Administrator Console only)*.

6. **Optional**: Use the following controls to change field display:
   - **: Change the sort order of columns.**
   - **: Change the order of values.**
7. Click **Save** in the row.
8. At the bottom of the page, click **Save** to apply your changes.

Configure Comment Field Options

The Comment Options Field allow you configure the appearance of the Comment field and Attachments sections on the *New Ticket* page.

1. Go to the Service Desk *Queue Detail* page:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Service Desk**, then click **Configuration**.
   c. On the **Configuration** panel, click **Create and manage queues** in **Queue** section.
   d. To display the *Queue Detail* page, do one of the following:
   # Click the name of a queue.
   # Select **Choose Action** > **New**.
2. Under the Queues section, click **Customize Fields** to display the *Queue Customization* page.
3. In the *Comment Field Options* tab, select or clear these check boxes, as needed.
   - **Display Comment field on ticket input form. Select this check box if you want the Comment field to appear on the ticket input form.**
   - **Display Attachments section on ticket input form. Select this check box if you want the Attachments section to appear on the ticket input form.**

   When these options are enabled, the Comment field and the Attachments section appear on the *New Ticket* page, when new tickets are created. They are not displayed on the *Ticket Detail* page, when an existing ticket is modified.
4. At the bottom of the page, click **Save** to apply your changes.

Define custom ticket fields

You can add custom fields to your Service Desk tickets; the number of custom fields you can create is limited only by the number of columns you can have in a table.

Creating a custom field involves two areas of the *Queue Customization* page:

- The custom field characteristics using the *Custom* field.
- The custom field behavior in the *Ticket Layout* section.

1. Go to the Service Desk *Queue Detail* page:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Service Desk**, then click **Configuration**.

c. On the **Configuration** panel, click **Create and manage queues** in **Queue** section.

d. To display the *Queue Detail* page, do one of the following:

Click the name of a queue.

Select **Choose Action** > **New**.

2. Under the *Queues* section, click **Customize Fields** to display the *Queue Customization* page.
3. In the *Custom Fields* tab, do one of the following:

- **Click the Edit button to change a field:** .
- **Click the Add button to create a field:** .

The editable fields appear.

4. Select the field type from the *Field Type* drop-down list.

Options include:

Checkbox: Add a check box field type to the ticket.

Date: Add a formatted date field type to the ticket.

Timestamp: Add a timestamp field type to the ticket.

Link: Add and define a link to an internal/external URL to the ticket.

Multiple Select: Add a multi-value select field type to the ticket; use commas to separate entries.

Notes: Add a notes field type to the ticket.

Number: Add an integer selection field type to the ticket.

Single Select: Add a single value select field type to the ticket.

Text: Add a text field type to the ticket.

User: Add a filterable and searchable drop-down list containing users from the user table.

NOTE: The *User* custom field stores the user ID from the USER table in the HD_TICKET table, which is the table that holds the ticket record. When writing a report or query against the HD_TICKET table, you need to JOIN on the USER table if you want to display the username instead of the user ID in the report.

5. In the *Select Values* field, specify the allowed values.

Use the *Select Values* field for the Single Select or Multiple Select custom field types. Enter multiple values as comma-separated strings.

You can use a database query to specify values for this field with the syntax: `query:` **query_instructions** . Select the **Help** button next to *Custom Fields* to view an example: .

6. Enter a value in the *Default* field.

This value is filled in by default when a ticket is created.

NOTE: If you remove the name of a custom field, values for that field are removed from all tickets. If you rename a custom field, values for that custom field are retained.

You can use a database query to specify values for this field with the syntax: `query:` **query_instructions** . Select the **Help** button next to *Custom Fields* to view an example: .

7. Click **Save**.
8. Scroll to the *Layout Ticket Fields* section, then click the **Edit** button next to the custom field you configured: .

The custom field behavior options become editable.

9. Enter a name in the *Label* field.
10. In the *Required* field select the option to use:
    - **Not Required. The field is not required.**
    - **Always Required. Fields with this option must be completed before a ticket can be saved and submitted.**
    - **Required on Close. Fields with this option must be completed before a ticket can be closed.**
11. In the *Permissions* field, choose the permission setting to use:

Permission setting	Can be viewed by	Can be changed by	Can be created by
Hidden	No one	No one	No one
Read Only	Users, Ticket Owners, Administrators*	No one	No one
Owners Only - Hidden from Users	Ticket Owners, Administrators*	Ticket Owners, Administrators*	Ticket Owners, Administrators*
Owners Only - Visible to Users	Users, Ticket Owners, Administrators*	Ticket Owners, Administrators*	Ticket Owners, Administrators*
User Create	Users, Ticket Owners, Administrators*	Ticket Owners, Administrators*	Users, Ticket Owners, Administrators*
User Create & Modify	Users, Ticket Owners, Administrators*	Users, Ticket Owners, Administrators*	Users, Ticket Owners, Administrators*

* Indicates the default setting. You can remove this default setting by clearing the *Allow users with an Administrator role to read and edit tickets in this queue (Administrator Console only)* check box on the *Queue Detail* page.

12. **Optional**: Use the **Sort** button at the top of a column, or drag the move icon, , to change the order in which the fields are displayed.
13. Click **Save** in the row.
14. At the bottom of the page, click **Save** to apply your changes.

Customize the ticket list layout

You can customize the Service Desk ticket list layout, such as field name, field order, and column size, as needed. This is how the Ticket list is displayed in the queue.

1. Go to the Service Desk *Queue Detail* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Service Desk**, then click **Configuration**.
    c. On the **Configuration** panel, click **Create and manage queues** in **Queue** section.

d. To display the *Queue Detail* page, do one of the following:

Click the name of a queue.

Select **Choose Action** > **New**.

2. On the *Service Desk Configuration* page, under *Layout* section, click *Customize queue specific tickets list* link. **Ticket List Layout** section. To customize the layout, use these buttons:

: Change the order in which the fields are displayed.

: Edit the field to display, and the width allowed for the column.

> **NOTE:** The width indicates the amount of available page width that is assigned to the field column. For example, if you have 10 columns, and each column is assigned a width of 10, the total of all numbers in the *Width* column would be 100. Therefore, each field column would have a width of 10 percent of the available page width. If the total of all numbers in the *Width* column is more or less than 100, the numbers are normalized to percentages to determine the width. For example, if you have three columns, and you assign a width of 10 to each column, the total of all numbers in the Width column would be 30. However, when normalized to percentages, the width of each column would be approximately 33.3 percent.

: Add a ticket field to the ticket layout.

: Delete the field from the ticket list.

3. Click **Save** at the bottom of the page.

Manage ticket templates

Ticket templates allow you to create different ticket types within the same queue. This mechanism allows you to better control the information your end users provide for different request scenarios, without having to create different queues.

Each queue can have one or more ticket templates. If multiple templates exist in a queue, you must select one ticket template as the default template.

1. Go to the Service Desk *Queue Detail* page:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Service Desk**, then click **Configuration**.
   c. On the **Configuration** panel, click **Create and manage queues** in **Queue** section.
   d. To display the *Queue Detail* page, do one of the following:

   # Click the name of a queue.

   # Select **Choose Action** > **New**.

2. On the *Service Desk Configuration* page, under *Layout* section, click *Customize queue specific tickets list* link.
3. To add a new ticket template to the queue, in the *Ticket Templates* section, click . For more information on how to create a new ticket template, see Configure a ticket template.
4. To make a ticket template the default template for the selected queue, in the Ticket Template Detail page, click **Make Default**. Any queue with one or more ticket templates must have a default template.

When a ticket template is configured as a default template for a queue, each time you create a ticket in that queue without specifying a ticket template, the default template is applied. You can switch between templates, if needed. For more information, see Create tickets from the Administrator Console Ticket page.

Configure a ticket template

A ticket template specifies a set of fields that appear on the *Ticket Detail* page. Each queue can have one or more ticket templates.

Use the *Ticket Template Detail* page to configure a new or an existing template.

1. Go to the Service Desk *Queue Detail* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Service Desk**, then click **Configuration**.
    c. On the **Configuration** panel, click **Create and manage queues** in **Queue** section.
    d. To display the *Queue Detail* page, do one of the following:
    # Click the name of a queue.
    # Select **Choose Action** > **New**.
2. On the *Service Desk Configuration* page, in the *Layout* section, click **Create ticket templates** to display the *Ticket Templates* section.
    # To add a new ticket template to the queue, in the *Ticket Templates* list page, click Choose Action > New.
    # To modify an existing ticket template, in the *Ticket Templates* list page, click the ticket template name.

    The *Ticket Template Detail* **page appears.**
3. On the *Ticket Template Detail* page, provide the following information:

Option	Description
Name	(Required) The name of the template.
Enabled	Select this check box when the template is ready for use. This option is useful if you want to prevent this template from being exposed to end users before it is completed.
Description	A brief description of the template. This text appears as a tooltip on the **User Portal**, when you point to the link for this ticket template.
For process only	Select this check box if you want this ticket template to be available to process templates. This causes some options in the ticket template to become disabled, because they are not applicable in this context. For example, the **Limit template to selected users** option cannot be applied to process-based ticket templates because each process template has an option in the wizard to associate labels with process template tickets.
Limit template to selected users	Select this check box if you want to make this template available only to specific users using labels. Then, click **Manage Associated Labels**, and in the *Select Labels* dialog box that appears, select one or more labels associated with the users that you want to grant access to this ticket template. When done, close the dialog box.
Is default	Select this check box if you want to make this ticket template the default template in the queue. When a ticket template is configured as a default template for a queue, each time you create a ticket in that queue without specifying a ticket template, the default template is applied. You can switch between templates, if needed. For more information, see Create tickets from the Administrator Console Ticket page.

Option	Description
	NOTE: The **Ask any general KACE SMA Service Desk topic** queue is visible in the User UI if you do not select this option. To hide the Ask any general KACE SMA Service Desk topic queue in the User Ui, you must select this option.
Show in User Portal	Select this check box if you want end users to have a link to this ticket template on the *Need Help* page in the **User Console**.
Layout	Choose a layout that best suits your needs: • **3 Column Layout**: Use this layout if the template contains fields of average height in each row. • **2 Column + Right Panel Layout**: Use this layout if the template contains one or more fields that are taller than the rest of the fields in the same row, like *Summary*, or *Resolution*. Having one tall field in a row where other fields are of average height causes those other fields in the same row to be pushed down, creating random gaps in the layout. When you select this option, you can place all of your tall fields in the right panel, to make optimal use of the vertical real estate. To move a field between the panels, double-click the field. • **3 Column + Right Panel Layout**: Use this layout if the template contains one or more fields that are taller than the rest of the fields in the same row, like *Summary*, or *Resolution*. Having one tall field in a row where other fields are of average height causes those other fields in the same row to be pushed down, creating random gaps in the layout. When you select this option, you can place all of your tall fields in the right panel, to make optimal use of the vertical real estate. To move a field between the panels, double-click the field. • **4 Column Layout**: Use this layout if the template contains fields of average height in each row. You can switch between the two layouts, if needed.

4. Add one or more ticket fields to the ticket template. To break up your content into separate sections, use the separator field. This field comes with the same options as the data fields.

   NOTE: You can only add ticket fields that exist in the queue to which this ticket template belongs to.

   a. In the *Ticket Form Template* section, drag one or more fields from the area on the right.
   b. As you add the fields, you can arrange them in the way that makes most sense for the use of this template. You can arrange related fields together, or place a field close to an edge of template area, and create empty spaces in between, as needed.
   c. A field can be one-, two-, or three-column wide. To change the width of the field, click until it reaches the desired width.
   d. To delete a field, click .
   e. To configure the field property overrides or certain conditions determining whether a field appears, click . Then, in the dialog box that appears, configure the following options, as required.

Tab	Option	Description
Overrides		Use the options on this tab to configure any overrides for field parameters that are already specified in the queue to which this ticket template belongs to.
	Label	The field name.

Tab	Option	Description
	Required	Indicates if the field value must be provided or not. Select one of the following values: • **Not Required** • **Always Required** • **Required on Close** For more information about these values, see Define custom ticket fields.
	Permission	Specify which users have access to this field. Select one of the following values: • **Read Only** • **Owners Only - Hidden from Users** • **Owners Only - Visible to Users** • **User Create** • **User Create & Modify** For more information about these values, see Define custom ticket fields.
	Default Value	Configure the default value for this field. • If this field is associated with pre-defined values, those values appear in the list, and they are available for selection. For example, if you add an *Owner* field to the ticket template, the list displays all users associated with the queue. • If you selected a text field, you can type a desired value, as required.
Conditional Logic		Use the options on this tab to show or hide certain fields based on the previously selected values on the ticket page. For example, if you have a ticket template for printer issues, you can display different set of fields that are applicable to different kinds of printer issues. If the user indicates on the ticket that the printer is missing paper, the page displays a set of fields that allow the user to specify the paper format.
	Visibility	Indicate if you want the field to appear or not when the specified conditions are met.
	When	Specify the action on the field based on the outcome of conditional expressions. Select one of the following values: • **All conditions matched** • **One of the conditions matched**
	Required when visible	Select this option if you want the end user to populate this field when it appears in the ticket.
	Condition	Add up to 10 conditions to control the appearance of the selected field. Each condition can evaluate if the value of a field that appears on the page matches or does not match a certain value. You can only select those fields that have pre-defined values associated with them (and typically

Tab	Option	Description
		appear as multi-value lists on the ticket page), or check boxes. Simple text fields, such as *Title*, are not available for selection. For example, you can create a condition that evaluates whether a printer issue matches *Ink*, *Paper*, or *Other*, and display or hide the selected field, as required. **NOTE:** Conditional logic will not be saved if the conditional field is marked as **Always required** or **Required on Close** in the queue field configuration or ticket template overrides. To make a conditional field required, use the **Required when Visible** option.

When done, click Update.

The dialog box closes.

5. Click **Apply Changes**.

TIP: You can also make a copy of this template by clicking **Duplicate**.

Next, you can preview the ticket template. For more information, see Preview ticket layout.

Preview ticket layout

When you finish making changes to the way tickets are displayed on the *New Ticket* and *Ticket Detail* pages for a selected ticket template, you can preview the ticket page layout.

There are several preview options to choose from. The type of information on the ticket page depends on the permissions associated with the user accessing the page (User or Owner), and the action type (*New Ticket* or *Ticket Detail*). For example, a Ticket Owner typically has access to more information than a user associated with the ticket. Also, the *New Ticket* page can have some additional controls for providing comments or linking attachments, unlike the *Ticket Detail* page.

NOTE: Previewing a ticket template causes it to create and save a ticket. Any values that you make while previewing a ticket are saved by default.

1. Go to the Service Desk *Queue Detail* page:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the **Configuration** panel, click **Create and manage queues** in **Queue** section.
   c. To display the *Queue Detail* page, do one of the following:
   # Click the name of a queue.
   # Select **Choose Action** > **New**.
2. On the on the **Service Desk Configuration** page, under the *Layout* section, click *Create ticket templates* link and select existing template name.>

   The *Ticket Template Detail* **page appears.**
3. On the *Ticket Template Detail* page, make your customizations, as required.

For details, see Configure a ticket template.

4. At the bottom of the page, click **Save and Preview**.

   The *Ticket Details* **page appears.**
5. At the top of the *Ticket Details* page, click **Preview Form As**, and choose one of the following options, as required:

Option	Description
Input Form - User	*New Ticket* page, as a User
Input Form - Owner	*New Ticket* page, as a Ticket Owner
Edit Form - User	*Ticket Detail* page, as a User
Input Form - Owner	*Ticket Detail* page, as a Ticket Owner

The *New Ticket* page refreshes, showing the ticket page based on the selected ticket template and owner details.

Using parent-child ticket relationships

You can set up any Service Desk ticket as a **parent** ticket and assign child tickets to it.

There are two ways to use the parent-child relationship:

- **Prevent the parent from being closed unless all its child tickets are closed**. This strategy uses the parent ticket as a global to-do list and each child ticket as a separate task on the list. After all the tasks are completed and the child tickets are closed, the parent can be closed.
- **Close all child tickets when you close the parent ticket**. This strategy is useful for tickets that are duplicates of the same problem. For example, if a server crashes and users file duplicate tickets about the issue. When the server is restored, the ticket owner can close the parent and close all of the child tickets at the same time.

Regardless of the strategy you choose, child tickets cannot be orphaned. That is, you cannot close the parent ticket before closing the child tickets.

NOTE: You can create many levels of parent-child ticket relationships, but closing child tickets by closing their parent ticket works for only one parent-child level.

Enable parent-child ticket relationships for a queue

Parent-child ticket relationships are disabled by default. To enable them, you can configure queues to show the *PARENT_INFO* ticket field. If you have multiple queues, you enable parent-child ticket relationships in each queue separately.

1. Go to the Service Desk *Queue Detail* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Service Desk**, then click **Configuration**.
    c. On the **Configuration** panel, click **Create and manage queues** in **Queue** section.
    d. To display the *Queue Detail* page, do one of the following:
    # Click the name of a queue.
    # Select **Choose Action** > **New**.
2. On the Service Desk Configuration page, under the *Queue* section, click the **Customize fields** link.
3. Go to the *Related Ticket information* tab and select the **Edit** button for the *PARENT_INFO* field to make changes to that field's settings: .
4. Select one of the *Owners Only - Visible to Users* permission settings.
5. Click **Save** in the row.
6. Click **Save** at the bottom of the page.

When you save these changes, ticket owners and administrators (by default) are able to make any ticket in the queue a child or a parent ticket.

Enable parent tickets to close child tickets

You can configure queues to allow parent tickets to close child tickets. When this is configured, child tickets are closed automatically when parent tickets are closed.

Enable parent-child relationships for queues. See Enable parent-child ticket relationships for a queue.

1. Go to the Service Desk *Queue Detail* page:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Service Desk**, then click **Configuration**.
    c. On the **Configuration** panel, click **Create and manage queues** in **Queue** section.
    d. To display the *Queue Detail* page, do one of the following:
    # Click the name of a queue.
    # Select **Choose Action** > **New**.
2. On the **Service Desk Configuration** page, under the *Queues* section, click **Modify configurations and preferences** to display the *Queue Customization* page. Then go to the *Preference* tab.
3. At the bottom of the page, click **Save**.

The change is applied to the queue. When you close parent tickets, any child tickets are closed automatically.

Create child tickets for any ticket

Child tickets are Service Desk tickets that have other tickets as their parents. Creating child tickets is useful for organizing tickets and managing related tasks. You can create child tickets for any ticket in any queue that has parent-child ticket relationships enabled.

Parent-child ticket relationships are enabled for the queue. See Enable parent-child ticket relationships for a queue.

1. Go to the Service Desk *Tickets* list:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Service Desk**, then click **Tickets**.
2. To create a child ticket for an existing ticket:
    a. On the *Tickets* list, click a ticket title.
    b. On the *Ticket Detail* page, select **Choose Action** > **Save and Create Child**.

    NOTE: This option is available only if parent-child relationships are enabled for the queue.

    c. Provide the required information for the child ticket, then click **Save**.
3. To create a child for a new ticket:
    a. On the *Tickets* list, select **Choose Action** > **New**.
    b. On the *Ticket Detail* page, provide the required information for the parent ticket.
    c. Select **Choose Action** > **Save and Create Child.**

    NOTE: This option is available only if parent-child relationships are enabled for the queue.

    d. Provide the required information for the child ticket, then click **Save**.

You can use parent tickets to organize duplicate tickets, and you can enable parent tickets to close child tickets. See:

- Use parent tickets to organize duplicate tickets
- Enable parent tickets to close child tickets

Designate tickets as parents and add existing tickets as their children

You can designate tickets as parents, and then set up parent-child relationships among tickets. You need to designate tickets as parents before you can add existing tickets to them as children.

Enable parent-child relationships for a queue. See Enable parent-child ticket relationships for a queue.

1. Go to the Service Desk *Ticket Detail* page.
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Service Desk**, then click **Tickets**.
    c. To display the *Ticket Detail* page, do one of the following:
    # Click the name of a ticket.
    # Select **Choose Action** > **New Ticket From Queue** > **Queue name**.

    If you have a high number of queues, use the search box to quickly find a specific queue.
2. On the Service Desk Configuration page, under the **Queues** section, click **Customize fields**. Then go to the *Related Ticket Information* tab, and verify that the *Parent Ticket* section is visible. If it is not displayed, verify that parent-child relationships are enabled for the queue. See Enable parent-child ticket relationships for a queue.
3. Select the *Allow this ticket to be a parent* check box to make this ticket a parent.
4. Click **Save**.
5. To add existing tickets as child tickets:
    a. Click **Add Tickets** under the **Child Tickets** section.
    b. Enter the child ticket number(s), separated by a comma, or use the **Select ticket to add** drop-down list to find the ticket(s) to add.
6. Click **Save** to save any changes to the ticket.

Use a parent ticket as a to-do list

The Service Desk parent-child relationship can be used to group tasks that need to be performed by different users, such as tasks that need to be completed when you hire a new employee. This enables you to track the tickets as a group.

- Enable parent-child relationships. See Enable parent-child ticket relationships for a queue.
- Verify that the ticket queue allows parents to close child tickets. See Enable parent tickets to close child tickets.

TIP: If you expect a multi-phase task to be repeated regularly, consider making it a process ticket. See Using Service Desk processes.

1. Create a ticket to serve as a parent. See Designate tickets as parents and add existing tickets as their children.
2. From the parent ticket, add child tickets for each required task on the to-do list.
3. Close each child ticket as tasks are completed.
4. When prompted, close the parent ticket. This prompt appears when the last child task is closed.

NOTE: If the resolution for the parent ticket is empty, the resolution from the child ticket will be added to the parent resolution.

Use parent tickets to organize duplicate tickets

When multiple tickets are filed for the same issue, you can use parent tickets to organize and manage the duplicate tickets as groups.

Enable parent-child relationships for queues, and enable parents to close child tickets. See:

- Enable parent-child ticket relationships for a queue
- Enable parent tickets to close child tickets

1. Designate one of the duplicate tickets as the parent. See Designate tickets as parents and add existing tickets as their children.
2. Change the remaining duplicate tickets to child tickets:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. Click **Service Desk** > **Tickets** to display the *Tickets* page.
    c. Select all of the tickets that you want to change to child tickets.
    d. In the *Choose Action* menu, select **Add To Parent**.

    NOTE: **Add to Parent** appears only if you are viewing tickets in a single queue, and that queue has parent-child ticket relationships enabled. It is not available if you are in the *All Queues* view. See Enable parent-child ticket relationships for a queue.

    The selected tickets become child tickets of the parent.
3. When the issue is resolved, close the parent ticket.

    The child tickets are automatically closed.

Using ticket approvers

You can require that a particular user or group approve tickets before tickets are opened or closed. In addition, you can require that only users who are set up as approvers can close tickets. If you have multiple queues, you can configure approver settings for each queue separately.

Setting up ticket approvers involves the following workflow:

- Create a label to specify approvers.
- Add users (approvers) to the label. You choose approvers from the list of all users regardless of queue, so they are not limited to a single queue.
- Configure the *APPROVAL_INFO* ticket field in the queue to require this feature.

NOTE: Approvers only have access to the *Approval* and *Approval Note* fields on a ticket. The *Approval* field has the following options:

- Approved
- Rejected
- More Information Needed

NOTE: The *Approval* field must be set before the ticket can be opened or closed, depending on how the *Required* option is configured. The *Approval Note* field is optional. Approvers can see all of the tickets they need to approve by clicking **Service Desk** > **Tickets**, then clicking **View By** > **My Approvals**.

Configure ticket approvers

You can require that a particular user or group approve a ticket before it can be opened and closed in a queue.

1. Go to the *Users* list:
    a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
    b. On the left navigation bar, click **Settings**, then click **Users**.
2. Select the check box next to a user.
3. In the *Choose Action* menu, select **Add Label**.
4. In the *Add Label* window, enter a name for the label, for example, Ticket Approvers, then click **Add Label**.

    TIP: Avoid using backslashes (\) in label names. If you need to use a backslash in a label name, add a second backslash (\\) to escape it.

5. Click **Service Desk** > **Configuration** > **Queues** > **Create and manage queues** to display the *Queues* page.
6. Click the name of a queue to display the *Queue Detail* page.
7. In the *User Preferences* tab, clear the *Allow all users as approvers* check box, then click **Save**.
8. In the *Queues* section, click **Customize fields** to display the *Queue Customization* page.
9. In the *Default Field* section, click the **Edit** button for the *APPROVAL_INFO* row: .

    The editable *APPROVAL_INFO* row appears.
10. In the *Label* field, enter the name of the label you created for approvers in 4.
11. Select **Required on close** in the *Required* field.

    Selecting Required on close or Always Required enables the approval requirement for all tickets in this queue. When you select one of these settings, a ticket must have an approver specified before it can be worked on or closed, depending on the option you choose.
12. Click the **Save** button in the row, then click **Save** at the bottom of the page.

The Approval feature is enabled, and the approval options you selected are applied to tickets in the queue.

Approving tickets by email

After ticket approval is configured, the designated ticket approver can send an email message to approve a ticket, add an approval note, or designate a different approver.

For details on changing tickets by email, see Creating and managing tickets by email. For a list of the fields used to change the approval fields, see Changing ticket approval fields using email.

Configuring SMTP email servers

You can configure your Service Desk to use SMTP email servers.

For instructions on setting up a POP3 email server, see Configuring email settings.

Connect your email server to the appliance

You can connect your email server to the appliance so that the Service Desk can receive email from your email server. The process for connecting depends entirely upon your email configuration.

If you are using Microsoft Exchange Server, see the Microsoft documentation on transport rules.

1. Open the Exchange Server Manager.
2. **Optional**: Create a Virtual SMTP server. This is not necessary if you have an SMTP server.
3. Create a Virtual SMTP Connector called appliance_HelpDesk.
4. Select **Administrative Groups** > **Connectors** > **appliance_HelpDesk** to display the *appliance_HelpDesk Properties* page.
5. Click **General**.
6. Click **Use DNS to route each address space on this connector**.

   The *Local Bridgeheads* section becomes available.
7. Complete the *Local Bridgeheads* section:

Server	Virtual Server
your_exchange_servername	Default SMTP Virtual Server

8. Click the **Address Space** tab.
9. Click **Add** to add an address space for the appliance SMTP server. Use the following settings:
   - **Type**: SMTP
   - **Address**: Enter the fully qualified appliance server name. The syntax is k1000.**mydomain**.com.
   - **Cost**: Set this to one level above the other connectors. That way, appliance email is filtered first, and no appliance email inadvertently leaves the network.
10. Under *Connector scope*, click **Entire organization**.
11. Leave **Allow messages to be relayed to these domains** disabled.
12. Click **OK** to save and close the *appliance_HelpDesk Properties* page.

Your email server is now connected to the appliance.

Using internal and external SMTP servers

Depending on the needs of your environment, you can set up your email to go through the internal SMTP server or an external SMTP server.

The appliance includes an internal SMTP server. If most of the email traffic coming to the appliance is from and to your Service Desk staff, it might make sense to use this internal server. To set it up, see Use the internal SMTP server.

If all of your email must go through a specific external SMTP server, direct the appliance to use this server. See Use an external SMTP server or Secure SMTP server.

Use the internal SMTP server

You can configure the appliance network settings to use the internal SMTP email server.

1. Go to the appliance *Control Panel*:
   - **If the Organization component is not enabled on the appliance, log in to the appliance Administrator Console, `https://appliance_hostname/admin`, then select Settings > Control Panel.**
   - **If the Organization component is enabled on the appliance, log in to the appliance System Administration Console, `https://appliance_hostname/system`, or select System in the drop-down list in the top-right corner of the page, then select Settings > Control Panel.**
2. Click **Enable SMTP** in the **Network Settings** section to display the *Network Settings* page.
3. In the *SMTP* tab, clear the **Enable SMTP Remote Server (Outbound Relay)** check box. This setting refers to an external SMTP server.
4. Click **Save**.
5. If prompted, click **Yes** to restart the appliance and apply the changes.

The internal SMTP server is set to process outgoing email. For information about configuring SMTP settings for queues, see Create and configure POP3 email accounts.

Use an external SMTP server or Secure SMTP server

To use an external SMTP server, you need to set up an account for the SMTP server in the appliance network settings, and you need to set up an account on the SMTP server for each Service Desk queue.

To use secure SMTP (SSMTP), select the SSL setting in each queue. This is necessary because Microsoft does not allow aliasing from addresses in the Exchange 365 service.

1. Confirm that your external router and firewall allow the appliance to use port 25 to send email.
2. Go to the appliance *Control Panel*:
   - **If the Organization component is not enabled on the appliance, log in to the appliance Administrator Console, `https://appliance_hostname/admin`, then select Settings > Control Panel.**
   - **If the Organization component is enabled on the appliance, log in to the appliance System Administration Console, `https://appliance_hostname/system`, or select System in the drop-down list in the top-right corner of the page, then select Settings > Control Panel.**
3. Click **Enable SMTP** in the **Network Settings** section to display the *Network Settings* page.
4. To use an external SMTP server, select **Enable SMTP Remote Server (Outbound Relay)** in the *SMTP* tab, then specify SMTP server options:

Option	Description
Server	Specify the hostname or IP address of an external SMTP server, such as **smtp.gmail.com**. External SMTP servers must allow anonymous (non-authenticated) outbound email transport. Ensure that your network policies allow the appliance to contact the SMTP server directly. In addition, the mail server must be configured to allow the relaying of email from the appliance without authentication. If you specify an IP address, enclose the address in brackets. For example `[10.10.10.10]`.
Port	Enter the port number to use for the external SMTP server. For standard SMTP, use port 25. For secure SMTP, use port 587.
Login	Enter the username of an account that has access to the external SMTP server, such as **your_account_name**@gmail.com.

Option	Description
Password and Confirm Password	Enter the password of the specified server account.

5. Test the SMTP configuration.
    a. Click **Test Connection**.
    b. In the *Connection Test SMTP* dialog box that appears, type the email address to which you want to send a test email using the newly configured SMTP server, and click **Send Test Email**.

    The *Connection Test SMTP* dialog box refreshes, showing the test results. status of the email operation. If the test fails, verify your configuration, and try again.
6. **Optional**: To configure a different SMTP or POP3 server for each queue, go to the *Configure Queue Email Settings* page:
    a. On the left navigation bar, click **Service Desk**, then click **Configuration**.
    b. On the **Configuration** panel, in the *Email Configuration* section, click **Configure Queue Email Settings**.

    The *Service Desk Queue Email Settings* page appears.
7. If you want to use an external SMTP server for emails associated with this queue, use the settings in the *Outbound Email Setting* tab.
    a. Select the *Specify Queue specific SMTP Settings* check box.
    b. Specify the following options:

Option	Description
SMTP Server	Specify the hostname or IP address of an external SMTP server, such as **smtp.gmail.com**. External SMTP servers must allow anonymous (non-authenticated) outbound email transport. Ensure that your network policies allow the appliance to contact the SMTP server directly. In addition, the mail server must be configured to allow the relaying of email from the appliance without authentication.
SMTP Port	Enter the port number to use for the external SMTP server. For standard SMTP, use port 25. For secure SMTP, use port 587.
SMTP Username	Enter the username of an account that has access to the external SMTP server, such as **your_account_name**@gmail.com.
SMTP Password	Enter the password of the specified server account.

8. Click **Save**.

The appliance is configured to forward email to the designated SMTP server. If you have multiple queues, repeat the preceding steps for each queue.

TIP: By default, the appliance accepts Service Desk email only when the sender's email address matches a user account on the appliance. To change this setting, see the setting, *Accept email from unknown users* in the section Configuring Service Desk ticket queues.

Maintenance and troubleshooting

The appliance has automatic backup capabilities, logs, and troubleshooting tools that help administrators maintain and monitor system health.

Maintaining the appliance

Appliance maintenance includes establishing a backup schedule, verifying system health, and applying updates to appliance software.

Tracking changes to settings

If History subscriptions are configured to retain information, you can view the details of the changes made to settings, assets, and objects.

This information includes the date the change was made and the user who made the change, which can be useful during troubleshooting. See About history settings.

About appliance backups

Appliance backups are files that are used to restore your appliance in the event of a data loss or other disaster.

There are two kinds of appliance backup files:

- **Base**: A backup of the file system. Base backup files are generally created once a week.
- **Differential**: A backup of the Base (file system) files that have changed since the most recent Base backup and a backup of database files. Differential backups reference the most recent Base backup file available.

To restore files, you must have a matched pair of Differential and Base backup files. Paired backup files reference the same appliance version number and date, and only paired backup files can be used to restore the appliance.

NOTE: Backups are created while the appliance is running. The appliance is not taken offline during the backup process. Restoring the appliance to a backup and resetting the appliance to factory settings, however, continue to require that the appliance be taken offline.

In addition, there are three types of backup processes:

- **Scheduled daily backups**: In most cases, daily backups include only Differential backup files. If there is no Base backup, or if the most recent Base backup is more than seven days old, the daily backup includes both Base and Differential backup files. This backup is known as a full backup. By default, daily backups are scheduled to occur at 02:00, but you can change that schedule. See Set the daily backup schedule and the number of backups to retain.
- **Scheduled monthly backups**: Monthly backups occur on the last day of the month, and you cannot change the schedule of monthly backups. This backup includes the most recent Base backup and the latest Differential backup files collected after the Base backup.
- **Backups initiated using the Run Now command**: When you click **Run Now** on the *Backup Settings* page, the appliance generates a full backup, which includes both Base and Differential backup files.

You can disable backups, which schedules existing backup data for deletion and disables daily and monthly backups. See Disable or enable appliance backups.

TIP: Always back up appliance data before installing updates or upgrading appliance software.

Set the daily backup schedule and the number of backups to retain

You can configure the daily backup schedule and the number of backups to retain.

1. Go to the appliance *Control Panel*:
   - **If the Organization component is not enabled on the appliance, log in to the appliance Administrator Console, `https://appliance_hostname/admin`, then select Settings > Control Panel.**
   - **If the Organization component is enabled on the appliance, log in to the appliance System Administration Console, `https://appliance_hostname/system`, or select System in the drop-down list in the top-right corner of the page, then select Settings > Control Panel.**
2. On the *Control Panel*, in the *Backup Settings and Restore* section, click any of the links to go to the *Backup Settings* page.
3. In the *Onboard Retention and Schedule* tab, specify the following settings:

Option	Description
Number of Daily Backups to Retain	The number of daily backups to retain on the appliance. You can retain up to seven daily backups.
Number of Monthly Backups to Retain	The number of monthly backups to retain on the appliance. You can retain up to two monthly backups. Monthly backups occur on the last day of the month, and you cannot change the schedule of monthly backups.

4. In the *Onboard Retention and Schedule* section, specify the schedule for running **daily** backups.

   Times are listed in the 24-hour clock format, and you can select intervals of 5 minutes. For example, to schedule the daily backup for 5 minutes past midnight, select 0:05.

   TIP: To ensure that backup logs are not turned over during daily log maintenance, schedule daily backups to occur after midnight.

5. Click **Save**.

The settings are applied. When the next scheduled backup runs, older backup files are removed if the number of backups retained on the appliance exceeds the number specified in the *Retention* section.

Back up the appliance manually

You can back up appliance manually any time. In addition, you should manually back up the appliance before you install appliance updates or perform upgrades.

1. Go to the appliance *Control Panel*:
   - **If the Organization component is not enabled on the appliance, log in to the appliance Administrator Console, `https://appliance_hostname/admin`, then select Settings > Control Panel.**
   - **If the Organization component is enabled on the appliance, log in to the appliance System Administration Console, `https://appliance_hostname/system`, or select System in the drop-down list in the top-right corner of the page, then select Settings > Control Panel.**
2. On the *Control Panel*, in the *Backup Settings and Restore* section, click any of the links to go to the *Backup Settings* page.
3. At the bottom of the page, click **Run Now**, then click **Yes** to confirm.

   The system performs a full backup, which includes both Base and Differential backup files.

When the backup is complete, the *Logs* page appears.

If you are backing up an appliance because you want to migrate it to a different appliance, power off the old appliance. If the old appliance is kept on, it may cause conflicts when the same settings are uploaded to the new appliance.

Download backup files from the Administrator Console

For a greater level of recoverability, you can download backup files from the **Administrator Console** and save them to a different location.

You can also access backup files through FTP. See Access backup files through FTP.

NOTE: To restore files, you must have a matched pair of Differential and Base backup files. Paired backup files reference the same appliance version number and date, and only paired backup files can be used to restore the appliance.

1. Go to the appliance *Control Panel*:
   - **If the Organization component is not enabled on the appliance, log in to the appliance Administrator Console, `https://appliance_hostname/admin`, then select Settings > Control Panel.**
   - **If the Organization component is enabled on the appliance, log in to the appliance System Administration Console, `https://appliance_hostname/system`, or select System in the drop-down list in the top-right corner of the page, then select Settings > Control Panel.**
2. On the *Control Panel*, in the *Backup Settings and Restore* section, click the *Restore appliance to prior backup* link to go to the *Restore Backup* page.
3. In the *Onboard Backups* tab download a matched pair of Differential and Base backup files:
   a. Select the date associated with a pair of backup files.

      The Differential file has `incr` in the file name, while the Base file uses `base`. For example, `<date>_k1_incr_<version>.tgz` and `<date>_k1_base_<version>.tgz`.

      SHA256 checksums also appear for each backup file. The checksums are calculated at the time of backup creation. If the checksum of a downloaded backup file does not match the checksum displayed on this page, the transfer may have been interrupted (resulting in corrupt data,) or data on disk may have been manipulated.

   b. If prompted, select a download location for each file.

NOTE: The saved backup files reflect the appliance data from the most recent automatic backup time (2:00 AM by default) for a selected date. If you need a backup that reflects the current appliance state, you can perform a manual backup. For more information, see Back up the appliance manually.

Access backup files through FTP

You can use FTP to access appliance backup files. This is useful if you want to create a process on a different server to access the backup, or if your backup files are more than 1 GB and accessing them through the **Administrator Console** causes the browser to time out.

1. Verify that Security Settings enable FTP access to backup files.

   See Configure security settings for the appliance.

2. Do one of the following:

   - **On a Windows device, open a command prompt, then at the `C:\` prompt, enter: `ftp k1000`.**
   - **Using any FTP client, access `ftp k1000`.**

3. Enter the login credentials.

   The default credentials are:

   Username: kbftp

   Password: getbxf

   NOTE: To change the FTP password, see Configure security settings for the appliance. You cannot change the FTP username.

4. To access the backup files from a command prompt, enter the following commands:

```
> type binary
> get k1_base.tg
> get k1_base.tgz
> get k1_incr.tgz
>close
>quit
```

About deleting appliance backup data

You can delete appliance backup data by disabling appliance backups.

Disabling backups can be useful if you want to reduce the amount of data being stored by the appliance. For example, if your virtual appliance uses virtual machine snapshots to back up appliance data instead of using the appliance backup files, you can disable appliance backups to reduce the size of the virtual machine.

IMPORTANT: Disabling backups prevents you from restoring appliance settings and data from the Administrator Console in the event of a disaster. As a result, you should disable appliance backups only if you are using an alternative method of backing up data, such as virtual machine snapshots for the virtual appliance. Disabling backups is not recommended for physical appliances.

Disable or enable appliance backups

By default, appliance backups are enabled. You can disable and enable appliance backups as needed.

When you disable appliance backups, existing backup files are scheduled for deletion at the next scheduled backup time.

IMPORTANT: Disabling backups prevents you from restoring appliance settings and data from the Administrator Console in the event of a disaster. As a result, you should disable appliance backups only if you are using an alternative method of backing up data, such as virtual machine snapshots for the virtual appliance. Disabling backups is not recommended for physical versions of the appliance.

1. **Optional**: To preserve the ability to restore data and settings in the event of a disaster, download the latest backup files from the Administrator Console and save them to a different location before you disable backups. See Download backup files from the Administrator Console.
2. Go to the appliance *Control Panel*:
   - **If the Organization component is not enabled on the appliance, log in to the appliance Administrator Console, `https://appliance_hostname/admin`, then select Settings > Control Panel.**
   - **If the Organization component is enabled on the appliance, log in to the appliance System Administration Console, `https://appliance_hostname/system`, or select System in the drop-down list in the top-right corner of the page, then select Settings > Control Panel.**
3. On the *Control Panel*, in the *Backup Settings and Restore* section, click either of the links *Set backup schedule*, *Configure retention policy*, or *Configure offboard backup settings* link to go to the *Backup Settings* page.
4. On the *Backup Settings* page, select **Disable Backups**.
5. Click **Save**.

   The following actions are performed:

   # All backup options are disabled.
   # Backup retention settings are set to 1 for daily backups and 0 for monthly backups.
   # Existing backup files are scheduled for deletion from the appliance at the next scheduled backup time.
6. To enable appliance backups, clear the **Disable Backups** check box, then click **Save**.
7. **Optional**: Click **Run Now** to generate a full backup of the system, including both Base and Differential backup files.

Configure offboard backup transfer

Appliance backups allow you to restore your appliance in the event of a data loss or other disaster. When you run into a problem with the appliance OS or the database, and you are asked to re-image the appliance, if you do not copy the backup files to a safe location prior to re-imaging, the backups cannot be restored. The *Backup Settings* page allows you to configure the transfer of backup data to an external location automatically. When configured, the appliance copies nightly backup files to an external location each time it completes the backup process.

1. Go to the appliance *Control Panel*:
   - **If the Organization component is not enabled on the appliance, log in to the appliance Administrator Console, `https://appliance_hostname/admin`, then select Settings > Control Panel.**
   - **If the Organization component is enabled on the appliance, log in to the appliance System Administration Console, `https://appliance_hostname/system`, or select System in the drop-down list in the top-right corner of the page, then select Settings > Control Panel.**
2. On the *Control Panel*, in the *Backup Settings and Restore* section, click the *Configure offboard backup settings* link to go to the *Backup Settings* page.
3. In the *Offboard Backup Transfer Settings* tab, clear the **Disable Offboard Backup Transfer**.
4. Click **Offboard Backup Transfer Protocol**, and select the protocol that you want to use to transfer the backup files: **FTP**, **Secure FTP**, **Samba**, **Azure Commercial Blob Storage**, **Azure Goverment Blob Storage** or **Amazon S3**.

Option	Description
Disable Offboard Backup Transfer	Indicates if offboard backup transfer is disabled or enabled. Clear this check box to enable offboard backup transfer.

Option	Description
Offboard Backup Transfer Protocol	The protocol that you want to use to transfer the backup files: **FTP**, **Secure FTP**, **Samba**, **Azure Commercial Blob Storage**, **Azure Goverment Blob Storage** or **Amazon S3**. If you want to use an Azure Blob Storage or Amazon S3 you must have a storage account set up. For more details, see your MS Azure and Amazon documentation. **IMPORTANT: Secure FTP (SFTP), Azure Commercial Blob Storage, and Amazon S3 protocols are the best practice recommendation for secure transfers with built-in integrity checking. While FTP and Samba options are also available, they are not recommended due to inherent vulnerabilities in these protocols and unencrypted data transfer.**
Offboard Backup Transfer Server	The host name or the IP address of the machine to which you want to copy the backup files.
Path or Share Name	The path of the directory on the machine to which you want to copy the backup files.
User Name	The name of the user account that you want to use to access the destination machine.
User Password	The password associated with the user name.

5. To verify if you can access the destination machine using the provided address and credentials, click **Test**.

   A message appears, indicating the success of the operation. If access to the destination server fails, this is indicated in the message. Verify your configuration and make changes, as applicable.
6. Click **Save**.

Restoring the appliance

You can restore appliance data using backup files, provided that backups are enabled and a matching pair of Differential and Base backup files are available. In addition, you can restore the appliance to its factory settings at any time.

Restoring the appliance destroys the data currently configured in the appliance. Quest KACE recommends that you off-load any backup files or data that you want to keep before you restore the appliance. In addition, restoring the appliance requires that the appliance be taken offline. The **Administrator Console** and the **User Console** are unavailable during the restore process.

NOTE: To restore files, you must have a matched pair of Differential and Base backup files. Paired backup files reference the same appliance version number and date, and only paired backup files can be used to restore the appliance.

Restore the appliance using the most recent backup

The appliance has a built-in ability to restore settings from the most recent backup directly from the appliance backup drive.

Appliance backups are enabled and you have a matching pair of Differential and Base backup files available. See Disable or enable appliance backups.

1. Go to the appliance *Control Panel*:
   - **If the Organization component is not enabled on the appliance, log in to the appliance Administrator Console, `https://appliance_hostname/admin`, then select Settings > Control Panel.**
   - **If the Organization component is enabled on the appliance, log in to the appliance System Administration Console, `https://appliance_hostname/system`, or select System in the drop-down list in the top-right corner of the page, then select Settings > Control Panel.**
2. On the *Control Panel*, in the *Backup Settings and Restore* section, click the *Restore appliance to prior backup* to go to the *Restore Backup* page.
3. In the *Onboard Backups* tab, select the most recent backup files.
4. Click **Restore from Backup**, then click **Yes** to confirm.

   The appliance is restored and restarted. The Administrator Console and the User Console are unavailable during the restore process. Progress appears in the browser window.

Upload backup files to the appliance

If you have copied your backup files to an off-appliance location, you can upload those files to the appliance manually using the **Administrator Console**, FTP, or Client Drop location process. FTP and Client Drop location uploads are useful if your backup files are more than 1 GB and uploading them through the **Administrator Console** causes the browser to time out.

You have copied backup files to an off-appliance location.

NOTE: To restore files, you must have a matched pair of Differential and Base backup files. Paired backup files reference the same appliance version number and date, and only paired backup files can be used to restore the appliance.

- To upload files using the Administrator Console:

  1. Go to the appliance *Control Panel*:

  # If the Organization component is not enabled on the appliance, log in to the Administrator Console, `http://`**appliance_hostname**`/admin`, then click **Settings**.

  # If the Organization component is enabled on the appliance, log in to the System Administration Console, `http://`**appliance_hostname**`/system`, or select **System** in the drop-down list in the top-right corner of the page, then click **Settings**.

  2. On the *Control Panel*, in the *Backup Settings and Restore* section, click any of the links to go to the *Restore Backup* page

     Or

     Click the *Manually upload backup files* link to go directly to the *Uploads* tab on the *Restore Backup* page.

  3. In the *Uploads* tab, under the *Differential* heading, click **Choose File**, to locate the Differential file you want to upload.

     Users can upload files using FTP. For more information, see the procedure below. When files are uploaded through FTP, they appear available for download in the *Restore* section.

  4. In the *Uploads* tab, under the *Base* heading, click **Choose File**, to locate the matching Base file you want to upload.

     NOTE: To restore files, you must upload pairs of Differential and Base backup files. Paired backup files reference the same appliance version number and date, and only paired backup files can be used to restore the appliance.

  5. Click **Upload Files**.

The uploaded files appear in the *Backups* section of the *Backup Settings* page.

- To upload your backup files to the appliance using FTP:

  1. Verify that Security Settings enable FTP access to backup files.

     See Configure security settings for the appliance.

  2. Do one of the following:

  # On a Windows device, open a command prompt, then at the `C:\` prompt, enter: `ftp k1000`.

  # Using any FTP client, access `ftp k1000`.

  3. Enter FTP login credentials.

     The default credentials are:

  Username: kbftp

  Password: getbxf

  NOTE: To change the FTP password, see Configure security settings for the appliance. You cannot change the FTP username.

  The uploaded files appear in the *Backups* section of the *Backup Settings* page.

- To use the Client Drop location method for uploading backup files, place your backup files in the Client Drop location on the appliance.

  Files placed in the Client Drop location are automatically identified as backup files and they become available for selection on the *Backup Settings* page within five minutes. See Copy files to the appliance Client Drop location.

Restore the appliance using the uploaded backup files. See Restore the appliance from backups.

Restore the appliance from backups

You can restore the appliance from backup files as needed.

If you are restoring files from an off-appliance location, you have uploaded a matching pair of Differential and Base backup files to the appliance. See Upload backup files to the appliance.

If you are migrating an appliance to a new appliance, the two appliances must be the same version. If that is not the case, you must upgrade the old appliance to the version running on the new appliance.

1. Go to the appliance *Control Panel*:

   - **If the Organization component is not enabled on the appliance, log in to the appliance Administrator Console, `https://appliance_hostname/admin`, then select Settings > Control Panel.**
   - **If the Organization component is enabled on the appliance, log in to the appliance System Administration Console, `https://appliance_hostname/system`, or select System in the drop-down list in the top-right corner of the page, then select Settings > Control Panel.**

2. On the *Control Panel*, in the *Backup Settings and Restore* section, click any of the links to go to the *Restore Backup* page

   Or

   Click the *Restore appliance to prior backup* link to go directly to the *Onboard Backups* tab on the *Restore Backup* page.

3. In the *Onboard Backups* tab, select the pair of files you want to restore.
4. If you want to disregard the network configuration from the backup files, and specify a new configuration under *Restore Options*, select **Override Network Configuration**, and specify the applicable options.

A set of options appears on this page when you select this check box. They are identical to the appliance network settings that you need to set up during an initial configuration. For complete information, see Change appliance network settings.

5. Click **Restore from Backup**, then click **Yes** to confirm.

   The appliance is restored and restarted. The Administrator Console and the User Console are unavailable during the restore process. Progress appears in the browser window.

   This process can take up to one hour and the appliance will be unavailable during this time. The amount of time for a restore depends on the size of the backup files. Once the restore completes, the appliance reboots. After the reboot, the appliance will be in the same state as when the backup files were created. This includes the same authentication settings, network settings, and so on.

   If the IP settings are not set upon reboot, try rebooting one or two times, to properly set the IP settings. If not they are not set using that method, try using the Console login `netdiag/netdiag` utility, and update the IP address there.

The appliance is restored and restarted.

Restore the appliance to factory settings

The appliance has a built-in ability to restore factory settings. This is useful if you encounter problems and you need to remove all custom configurations.

1. Go to the appliance *Control Panel*:
   - **If the Organization component is not enabled on the appliance, log in to the appliance Administrator Console, `https://appliance_hostname/admin`, then select Settings > Control Panel.**
   - **If the Organization component is enabled on the appliance, log in to the appliance System Administration Console, `https://appliance_hostname/system`, or select System in the drop-down list in the top-right corner of the page, then select Settings > Control Panel.**
2. On the *Control Panel*, in the *Backup Settings and Restore* section, click any of the links to go to the *Restore Backup* page
3. At the bottom of the page, click **Reset to Factory Settings**, then click **Yes** to confirm.

   The appliance is restored and restarted.
4. Re-configure the appliance as needed.

   See Configuring the appliance.

Updating appliance software

You can check for and install appliance software updates. When you update the appliance, custom configurations, such as Service Desk and Asset customizations, are preserved.

Check for and apply advertised appliance updates

The appliance checks with the servers at Quest daily to determine whether appliance software updates are available. These updates are referred to as advertised updates.

If updates are available, an alert appears on the *Home* page the next time you log in with Administrator account privileges.

TIP: Always back up appliance data before installing updates or upgrading the appliance software. For instructions, see About appliance backups.

1. Go to the appliance *Control Panel*:
   - **If the Organization component is not enabled on the appliance, log in to the appliance Administrator Console, `https://appliance_hostname/admin`, then select Settings > Control Panel.**
   - **If the Organization component is enabled on the appliance, log in to the appliance System Administration Console, `https://appliance_hostname/system`, or select System in the drop-down list in the top-right corner of the page, then select Settings > Control Panel.**
2. On the left navigation bar, click **Appliance Updates** to display the *Appliance Updates* page.
3. In the *Server* section, click **Check for Update** to display the *Logs* page.

   Results of the check appear in the log.
4. When an update is available, back up your database and files.

   See About appliance backups.
5. Click **Update**.

The update is applied. The **Administrator Console** is unavailable until the update is complete. Progress appears in the browser window and in the **Administrator Console**.

Upload an update file to the appliance manually

If you have an update file from Quest, you can upload it to the appliance manually.

Before you update the appliance manually, verify that your appliance meets the minimum server version requirements as specified in the release notes for the update. If your appliance does not meet these requirements, you must upgrade to the minimum version before you update the appliance software. See View the appliance version, model, and license information.

1. Back up your database and files. See About appliance backups.
2. Download the `k1000_upgrade_server_`**XXXX**`.kbin` file, and save it locally.
3. Go to the appliance *Control Panel*:
   - **If the Organization component is not enabled on the appliance, log in to the appliance Administrator Console, `https://appliance_hostname/admin`, then select Settings > Control Panel.**
   - **If the Organization component is enabled on the appliance, log in to the appliance System Administration Console, `https://appliance_hostname/system`, or select System in the drop-down list in the top-right corner of the page, then select Settings > Control Panel.**
4. On the left navigation bar, click **Appliance Updates** to display the *Appliance Updates* page.
5. In the *Manually Update* section:
   a. Click **Browse** or **Choose File**, and locate the update file.
   b. Click **Update**, then click **Yes** to confirm.

The update is applied. The **Administrator Console** is unavailable until the update is complete. Progress appears in the browser window and in the **Administrator Console**.

Verify updates

After applying an update, you can verify successful completion by reviewing the update log.

1. Go to the appliance *Control Panel*:
   - **If the Organization component is not enabled on the appliance, log in to the appliance Administrator Console, `https://appliance_hostname/admin`, then select Settings > Control Panel.**
   - **If the Organization component is enabled on the appliance, log in to the appliance System Administration Console, `https://appliance_hostname/system`, or select System in the drop-down list in the top-right corner of the page, then select Settings > Control Panel.**
2. Click **Logs** to display the *Logs* page.
3. In the *Log* drop-down list, select **Updates**.
4. Review the log for error messages and warnings.
5. Click **Need Help** in the top-right corner of the page, then click **About** at the bottom of the *Help* panel to verify the current version. See View the appliance version, model, and license information.

Update the appliance license key

You might need to update the appliance license key if you expand your license capabilities or purchase additional components, such as the Organization component.

1. Go to the appliance *Control Panel*:
   - **If the Organization component is not enabled on the appliance, log in to the appliance Administrator Console, `https://appliance_hostname/admin`, then select Settings > Control Panel.**
   - **If the Organization component is enabled on the appliance, log in to the appliance System Administration Console, `https://appliance_hostname/system`, or select System in the drop-down list in the top-right corner of the page, then select Settings > Control Panel.**
2. On the left navigation bar, click **Appliance Updates** to display the *Appliance Updates* page.
3. In the *License Information* section, enter your license key.
4. Click **Update**.

Reboot or shut down the appliance

You might need to reboot or shut down the appliance from time to time when troubleshooting or performing maintenance tasks.

In addition, you need to shut down the appliance before you unplug it.

TIP: To shut down the physical appliance any time, press the power button once, quickly.

1. Go to the appliance *Control Panel*:
   - **If the Organization component is not enabled on the appliance, log in to the appliance Administrator Console, `https://appliance_hostname/admin`, then select Settings > Control Panel.**
   - **If the Organization component is enabled on the appliance, log in to the appliance System Administration Console, `https://appliance_hostname/system`, or select System in the drop-down list in the top-right corner of the page, then select Settings > Control Panel.**
2. On the left navigation bar, click **Appliance Updates** to display the *Appliance Updates* page.
3. In the *Appliance Controls* section, do one of the following:
   - **Click Reboot. The appliance restarts.**
   - **Click Reboot and Check Database to open the Confirm dialog.**

     To confirm reboot, enter the phrase **understood** in the text box, and click **Yes**.
     The appliance restarts and then verifies the database.
   - **Click Shutdown. The appliance shuts down, and it is safe to power-down the appliance hardware.**

Understanding the daily run output

The appliance **daily run output** is a report that shows appliance status information, such as disk status, network interface status, and appliance up-time averages.

The report is automatically emailed to the system administrator every day at 02:00. To change the system administrator email address, see Configure appliance General Settings with the Organization component enabled or Configure appliance General Settings without the Organization component.

Disk status

The *daily run output* report, which is automatically emailed to the system administrator every day, includes a *Disk status* table.

Filesystem	Size	Used	Avail	Capacity	Mounted on
/dev/twed0s1a	38G	3.6G	32G	10%	/
devfs	1.0K	1.0K	0B	100%	/dev
fdescfs	1.0K	1.0K	0B	100%	/dev/fd
procfs	4.0K	4.0K	0B	100%	/proc

The following columns appear in the *Disk status* table.

Column heading	Description
Filesystem	The name of the file system.
Size	The amount of disk space allocated to the specified file system.
Used	The amount of disk space in use by the specified file system.

Column heading	Description
Avail	The amount of free disk space available to the specified file system.
Capacity	The percentage of disk space available to the specified file system.
Mounted on	The disk partition on which the specified file system is located.

Appliance network interface status

The *daily run output* report, which is automatically emailed to the system administrator every day, includes a *Network interface status* table.

Make sure the *Ierrs/Oerrs* are zero. Other values indicate network failures.

If you notice consistent errors, contact **Quest Support** at https://support.quest.com/contact-support.

```
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     -     -
```

Appliance up-time and load averages

The *daily run output* report, which is automatically emailed to the system administrator every day, shows the appliance up-time and load averages.

The load averages vary depending on the appliance load when the report runs.

The following indicates the amount of time the appliance has been up since the last time it was powered off. In this example, no users are logged on to the appliance.

```
Local system status:
 2:01AM up 7 days, 4:12, 0 users, load averages: 0.05, 0.20, 0.15
```

Email system health

The *daily run output* report, which is automatically emailed to the system administrator every day, shows the health of the email system.

The following messages are the standard FreeBSD messages regarding the health of email systems.

There should be no email messages in the queues. If messages appear in the queues, see Verify SMTP settings.

```
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
```

Verify SMTP settings

If email messages appear in the queues, verify your SMTP settings.

1. Go to the appliance *Control Panel*:
   - **If the Organization component is not enabled on the appliance, log in to the appliance Administrator Console, `https://appliance_hostname/admin`, then select Settings > Control Panel.**
   - **If the Organization component is enabled on the appliance, log in to the appliance System Administration Console, `https://appliance_hostname/system`, or select System in the drop-down list in the top-right corner of the page, then select Settings > Control Panel.**
2. Click **Network Settings** to display the *Network Settings* page.

Appliance backup status

The *daily run output* report, which is automatically emailed to the system administrator every day, shows the appliance backup status.

The following appliance-specific message shows that the backups have been successfully completed and are on the /kbackup disk, available through FTP.

See Access backup files through FTP.

```
[2015-06-21 02:01:24 -0700] Backup: Complete.
```

Status of RAID drives

For physical KACE SMAs, the status of RAID drives is displayed in the server logs. This status is available for physical KACE SMAs only.

The following log message indicates that RAID drives are functioning properly:

```
Logical Drive 0 (RAID 5) Information
RAID Array Status: Logical Drive 0 is not rebuilding: status is Optimal.
Status: Online. Spun Up
```

If RAID drives are degraded or not rebuilding properly, contact **Quest Support** at https://support.quest.com/contact-support.

Troubleshooting the appliance

The appliance includes tools, logs, and reports to help you monitor system health and resolve issues.

Using Troubleshooting Tools

You can use troubleshooting tools to identify and resolve issues.

Verify the status of devices on the network

To verify the status of devices on the network, you can use the ping troubleshooting utility.

1. Go to the appliance *Control Panel*:
   - **If the Organization component is not enabled on the appliance, log in to the appliance Administrator Console, `https://appliance_hostname/admin`, then select Settings > Control Panel.**
   - **If the Organization component is enabled on the appliance, log in to the appliance System Administration Console, `https://appliance_hostname/system`, or select System in the drop-down list in the top-right corner of the page, then select Settings > Control Panel.**
2. On the left navigation bar, click **Support** to display the *Support* page.
3. In the *Troubleshooting Tools* section, click **Run diagnostic utilities** to display the *Diagnostic Utilities* page.
4. In the text box, enter the IP address of a device.
5. Select **ping** in the drop-down list.
6. Click **Run Now**.

   Results are displayed.
7. To use other utilities, select them in the drop-down list, then click **Run Now**.

Identify device issues

Use the *Device Issues* list to see if any of your managed devices have issues connecting to the agent, or other issues.

The appliance relies on the KACE Agent to collect information from agent-managed devices in your organization. If a device encounters issues connecting to the agent, or other issues related to their environment, this prevents the appliance from obtaining inventory information for that device.

The *Device Issues* list page identifies any agent-managed devices whose information does not appear in the inventory due to any of the following issues:

- WMI (Windows Management Instrumentation) corruption.
- Desktop heap exhaustion.

  TIP: In most cases, this problem can be cleared by simply restarting the device.
- Failure to write to `amp.conf`.

For more information about these issues, visit https://support.quest.com/kace-systems-management-appliance/kb.

1. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
2. Select **Settings** > **Support** to display the *Support* page.
3. In the *Troubleshooting Tools* section, click **Device Issues** to display the *Device Issues* page.
4. Review the list of faulty devices on the *Device Issues*, and take any steps to resolve these issues, as required.

Enable a tether to Quest KACE Support

You can access the Quest Support Portal to request a tether to your appliance to enable Quest KACE Technical Support to troubleshoot issues.

Obtain a tethering key by contacting **Quest Support** at https://support.quest.com/contact-support.

To ensure security, enable remote access to the appliance after the Support team authorizes you to do so.

1. Go to the appliance *Control Panel*:
   - **If the Organization component is not enabled on the appliance, log in to the appliance Administrator Console, `https://appliance_hostname/admin`, then select Settings > Control Panel.**
   - **If the Organization component is enabled on the appliance, log in to the appliance System Administration Console, `https://appliance_hostname/system`, or select System in the drop-down list in the top-right corner of the page, then select Settings > Control Panel.**
2. Click **Security Settings** on the appliance *Control Panel* to display the *Security Settings* page.
3. Ensure the **Enable SSH** check box is selected.
4. Click **Save and Restart Services**.
5. On the left navigation bar, click **Support** to display the *Support* page.
6. In the *Troubleshooting Tools* section, click **Enter a Tether Key** to display the *Support Tether Key* page.
7. On the *Support Tether Key* page, in the text field, type the description of the problem, and complete one of the following steps.
   - **To obtain the tether key automatically and send the message to Technical Support, click Enable Tether.**

     If the process fails, select **Enable Tether** and type the tether key, as prompted. Click **Save**.
   - **To use a tether key provided by Technical Support, click I already have a tether key, then select Enable Tether and type the tether key, as prompted. Click Save.**

Troubleshooting appliance issues

The appliance server logs can help you and **Quest Support** detect and resolve errors.

The logs contain the last seven days of activity, and they are copied and compressed every day. Compressed logs are deleted when they are seven days old.

Log maintenance checks are performed daily, and no additional administrative log maintenance procedures are required.

View appliance logs

You can view appliance logs in the **Administrator Console**. Appliance logs provide information related to appliance processes and errors the system encounters.

If the appliance is configured to share detailed usage data with Quest KACE, appliance and Agent exceptions or errors are reported to Quest every day. See:

- Configure appliance General Settings with the Organization component enabled
- Configure appliance General Settings without the Organization component

1. Go to the appliance *Control Panel*:
   - **If the Organization component is not enabled on the appliance, log in to the appliance Administrator Console, `https://appliance_hostname/admin`, then select Settings > Control Panel.**
   - **If the Organization component is enabled on the appliance, log in to the appliance System Administration Console, `https://appliance_hostname/system`, or select System in the drop-down list in the top-right corner of the page, then select Settings > Control Panel.**
2. On the left navigation bar, click **Logs** to display the *Logs* page.
3. Select a log in the *Log* drop-down list.

Log Type	Log Name	Description
Hardware	**Disk Status**	The status of the physical appliance disk array (not available for virtual appliances).
Server	**K1000 Log**	The errors generated on the appliance.
	Access	The HTTP server's access information.
	Server Errors	Errors or server warnings related to appliance server processes.
	Stats	The number of connections the appliance is processing over time.
	Updates	Details of appliance patches or upgrades applied to the appliance.
	Reporting Log	Details of reports that have been run.
	Reporting Errors	Errors related to reports that have been run.
	Konductor Log	Konductor-related logs. Konductor is an internal appliance component that regulates communications between the appliance and managed devices to keep the system running smoothly. The number of tasks Konductor is running appears on the *Tasks in Progress* widget. In addition, task throughput information appears on the appliance *General Settings* page (on appliances with the Organization component enabled) or on the *Communication Settings* page (on appliances without the Organization component enabled). See: • Configure appliance General Settings with the Organization component enabled • Configure Agent communication and log settings
	Patch Download Log	Information about patches that have been downloaded to the appliance.
	Dell Updates Log	Information about Dell hardware updates that have been downloaded to the appliance.
	Backup Log	Details of daily and monthly appliance backups.
	Backup Restore Log	Details about restoring information from appliance backups.
	Discovery Log	Information related to the discovery process.
	Provisioning Log	Information related to the KACE Agent provisioning.
	Agentless Log	Information related to Agentless device connections to the appliance.
	Monitoring Log	Information related to monitored servers and their connections to the appliance.

Log Type	Log Name	Description
	Software Inventory	Information related to Software Catalog inventory processing.
	Software Inventory Errors	Processing errors related to appliance Software Catalog inventory processing.
	Asset Import Log	Information related to importing assets.
	Dell Warranty Log	Information related to Dell Warranty updates.
	User Authentication Log	Information related to user authentication. Each entry in the log includes the following information: • The name of the user account that attempts to log in. • The IP address of the device from which the login attempt originated. • The console to which the user attempts to log in: `userui` (**User Console**), `systemui` (**System Administration Console**), `adminui` (**Administrator Console**), or a Linked Appliance. • The name of the organization the user is authenticated against. • The type of authentication used: `Local Authentication`, `Single Sign On`, `systemui Local Authentication`, or `LDAP`. • The result of the login attempt: `success` or `failed`. For example: `[2018-04-26 07:27:06 -0700] AUTH [info] admin - 10.1.243.172 - adminui - Default - systemui Local Authentication - success`
Mail	**Service Desk Incoming Mail Log**	Information related to problems encountered by the Exim Server (Mail Transfer agent) while processing email for Service Desk queues. For example, invalid email addresses and Service Desk licensing issues.
	Service Desk Incoming Mail Error Log	PHP errors encountered when inbound email messages are processed.
	Service Desk Outgoing Mail Log	Errors encountered by the Mail Daemon while sending outgoing email messages. For example, invalid email addresses.
	Service Desk Outgoing Mail Error Log	PHP errors encountered when outgoing email notifications are processed.
	KMailServices Log	Information related to the `KMailServices` process.
EXIM	**Exim Main Log**	Information related to the arrival end delivery of each message.
	Exim Reject Log	Information related to rejected messages.

Log Type	Log Name	Description
Device	**Client Access**	KACE Agent access logs.
	Client Errors	KACE Agent exception logs.
	Agent Messaging Protocol Server	Server-related Agent Messaging Protocol log entries.
	Agent Messaging Protocol Server Errors	Server-related Agent Messaging Protocol log errors.
	Agent Messaging Protocol Queue	Queue-related Agent Messaging Protocol log entries.
	Agent Messaging Protocol Queue Errors	Queue-related Agent Messaging Protocol log errors.

If the Organization component is enabled on your system, you can change the number of days logs are retained. This setting appears in the *Log Retention* section of the appliance *General Settings*. See Configure appliance General Settings with the Organization component enabled.

Download appliance activity logs

You can download appliance activity logs from the **Administrator Console**. These logs can be useful during troubleshooting.

1. Go to the appliance *Control Panel*:
   - **If the Organization component is not enabled on the appliance, log in to the appliance Administrator Console, `https://appliance_hostname/admin`, then select Settings > Control Panel.**
   - **If the Organization component is enabled on the appliance, log in to the appliance System Administration Console, `https://appliance_hostname/system`, or select System in the drop-down list in the top-right corner of the page, then select Settings > Control Panel.**
2. On the left navigation bar, click **Support** to display the *Support* page.
3. Click **Retrieve appliance activity logs**.

   The logs are downloaded in the `k1000_logs.tgz` file.

   For information about logs used in debugging, see:

   # Managing provisioning schedules
   # Troubleshooting and debugging the KACE Agent
   # View appliance logs

If the Organization component is enabled on your system, you can change the number of days logs are retained. This setting appears in the *Log Retention* section of the appliance *General Settings*. See Configure appliance General Settings with the Organization component enabled.

Viewing the daily run output

The daily run output is a report that shows appliance information such as the disk status, network interface status, uptime and load averages, mail system health, and database status. Use this report to verify system status and identify issues that need to be resolved.

This report runs on a daily basis and is sent by email to the system administrator. See Understanding the daily run output and .

Troubleshooting and debugging the KACE Agent

Use the Agent's debugging features to troubleshoot Agent-related issues.

If devices do not show up in Inventory, ensure the **Agent Debug Trace** option is enabled on the *Communication Settings* page. For more information, see Configure Agent communication and log settings.

For additional assistance, go to the **Quest Support** website, https://support.quest.com/contact-support. This website contains a Knowledge Base you can use for troubleshooting.

Resolve Windows security issues that prevent Agent provisioning

If Windows security settings prevent the appliance from provisioning the Agent to Windows devices, you can reconfigure settings through a command prompt.

To allow provisioning, you must open the firewall and configure security settings.

1. Open a command prompt on the device.
2. Open the firewall and configure security settings:

```
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
```

Testing and troubleshooting email communication

You can take steps to ensure that your Service Desk email communication is working correctly. You can verify email system configuration by testing your outgoing and incoming email. In addition, you can use Telnet to test email. Log files are available to provide error information.

The testing and troubleshooting information assumes that you are using a POP3 email server to communicate with the appliance as described in Configuring email settings.

Test outgoing email

You can test outgoing email to verify system configuration.

1. Go to the appliance *Control Panel*:
   - **If the Organization component is not enabled on the appliance, log in to the appliance Administrator Console, `https://appliance_hostname/admin`, then select Settings > Control Panel.**
   - **If the Organization component is enabled on the appliance, log in to the appliance System Administration Console, `https://appliance_hostname/system`, or select System in the drop-down list in the top-right corner of the page, then select Settings > Control Panel.**
2. On the left navigation bar, click **Support** to display the *Support* page.
3. In the *Troubleshooting Tools* section, click **Run diagnostic utilities** to display the *Diagnostic Utilities* page.
4. In the Test drop-down list, select **email sending**.
5. In the text box, enter a valid email address.
6. Click **Run Now** to display a log of the email's path.
7. Check the log file for errors.
   - **If no errors are reported, the outgoing email was successfully sent.**
   - **In the event of an error:**
     # Check your email and spam filters.
     # Check your appliance network settings. If you are using your own SMTP server, the appliance relays email through it. Many SMTP servers require specific permission to do this. Add your appliance IP address to the list of acceptable servers.
     # Check your router settings. Make sure the appliance can use the SMTP port (25).
     # Check your firewall settings. Make sure the appliance can use the SMTP port (25).
     # If you cannot resolve the issue, contact **Quest Support** at https://support.quest.com/contact-support.

Test incoming email

You can test incoming email to verify system configuration.

1. Log on to your SMTP server, and create a Service Desk ticket by sending an email message to the Support email address for your appliance.
2. Go to the Service Desk *Tickets* page:
   a. Log in to the appliance Administrator Console, `https://`**appliance_hostname**`/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
   b. On the left navigation bar, click **Service Desk**, then click **Tickets**.
3. Confirm that a ticket appears.

   If you send email from a valid account on the appliance, a ticket is created automatically.

Use Telnet to test incoming email

You can use Telnet to communicate with the appliance SMTP server and send a test email.

1. Use the following commands:

```
>telnet k1000.mydomain.com 25
>EHLO mydomain.com
>MAIL FROM:<admin@mydomain.com>
>RCPT TO:<servicedesk@k1000.mydomain.com
```

```
>DATA
>Test data here
>QUIT
.
```

These commands start communication, tell the server who the message is from, tell the server who the message is to, prepare to send data, and quit Telnet.

2. Check the Service Desk email box to confirm that you have received email from admin@**mydomain**.com.

Access appliance logs to view Microsoft Exchange Server errors

Information about Microsoft Exchange Server errors is available in appliance log files when logging is enabled on the Exchange Server.

1. In Microsoft Exchange Server, open the *SMTP Virtual Server Properties* window.
2. On the *General* tab, make sure that the *Enable Logging* check box is selected. If it is not selected, select it, then send a test email to the appliance.
3. Go to the appliance *Control Panel*:
   - **If the Organization component is not enabled on the appliance, log in to the appliance Administrator Console, `https://appliance_hostname/admin`, then select Settings > Control Panel.**
   - **If the Organization component is enabled on the appliance, log in to the appliance System Administration Console, `https://appliance_hostname/system`, or select System in the drop-down list in the top-right corner of the page, then select Settings > Control Panel.**
4. On the left navigation bar, click **Logs** to display the *Logs* page.
5. Select a log from the *Log* drop-down list.
6. Examine the `exim_mainlog_*` and `exim_paniclog_*` files for problems.

   Problem could include:

   # Errors and unsuccessful steps
   # Hostnames and other variables not fully resolved
7. Examine the `Debug_*` log for any other Exim problems such as runaway Exim processes.

   These other logs might also provide clues to the problem:

   # `khelpdeskmailhandler_output`
   # `khelpdeskmailnotifier_error`
   # `khelpdeskmailnotifier_output`
8. Examine the Microsoft Exchange SMTP service logs in `C:\windows\system32\ologFiles\*SMTP` for problems.

Troubleshooting email errors

Solutions exist for some typical email errors.

Email error	Solution
550 Unknown user	• Make sure the address is correct. • Verify that the address matches the address used by Service Desk. • Try disabling the external SMTP server and removing the address from the network settings. Reboot and restore the address. Reboot once more.
451 error - unable to verify sender	Check DNS settings.

About Diagnostic Console Two-Factor Authentication

Diagnostic Console Two-Factor Authentication (2FA) allows you to control access to the appliance back-end. When you enable SSH access to the appliance and create a tether, the **Quest Support** team can log in to the back-end of the appliance using the appliance root password together with an access token. Tokens are provided in the *Initial Setup Wizard*. They can be viewed and regenerated using the *Diagnostic Console Two-Factor Authentication* page in the appliance System Console. Each token can only be used once and must be given to the **Quest Support** contact before they can log in to the appliance through the tether or the console.

To navigate to this page, log in to the appliance System Console. On the left navigation bar, under *Settings*, click **Support**, and on the *Support* page, under *Troubleshooting Tools*, click **Diagnostic Console Two-Factor Authentication**.

The security key and offline tokens that are provided with the appliance during the initial setup should be recorded and stored in secure location, not on the appliance machine. You may be required to provide this information to Support, when needed.

After upgrading from an earlier version, if a message appears indicating that Diagnostic Console Two-Factor Authentication is disabled, and you want to enable it for enhanced security, follow the instructions in the message to enable it.

- To replace the secret key and regenerate the offline tokens, click **Replace Secret Key**.
- To regenerate offline tokens, click **Regenerate Offline Tokens**.

Appendixes

Database table names

Database table names can be used in reports and other database queries.

The following tables list the current database table names and the table names that have changed between the 6.3 and 6.4 versions of the appliance:

- Organization-level (ORG1) database tables
- System-level (KBSYS) database tables

Organization-level (ORG1) database tables

The following table lists organization-level (ORG1) database table names. Reference these table names when creating custom reports using SQL queries. See Create reports using SQL queries.

Table 36. ORG1 database tables and components

Table	Component
ADVISORY	Service Desk: Knowledge Base
ADVISORY_LABEL_JT	Service Desk: Knowledge Base
ADVISORY_RATINGS	Service Desk: Knowledge Base
AGENTLESS_TASK_LOG	Appliance Administration: Discovery
ASSET	Asset Management
ASSET_ASSOCIATION	Asset Management
ASSET_CATALOG_ASSOCIATION	Asset Management
ASSET_CLASS	Asset Management: Asset Subtypes
ASSET_DATA_1	Asset Management: Import Assets
ASSET_DATA_2	Asset Management: Import Assets
ASSET_DATA_3	Asset Management: Import Assets
ASSET_DATA_4	Asset Management: Import Assets
ASSET_DATA_5	Asset Management: Import Assets
ASSET_DATA_6	Asset Management: Import Assets

Table	Component
ASSET_DATA_7	Asset Management: Import Assets
ASSET_FIELD_DEFINITION	Settings: Asset History
ASSET_FILTER	Asset Management: Labeling
ASSET_HIERARCHY	Asset Management
ASSET_HISTORY	Settings: Asset History
ASSET_TYPE	Asset Management: Asset Types
AUTHENTICATION	Appliance Administration
CLIENTDIST_LABEL_JT	Appliance Administration: KACE Agent
CLIENT_DISTRIBUTION	Appliance Administration: KACE Agent
CREDENTIAL	Settings: Credentials
CUSTOM_FIELD_DEFINITION	Appliance Administration
CUSTOM_VIEW	Appliance Administration: Service Desk Configuration
DASHBOARD	Dashboard
DASHBOARD_CACHE	Dashboard
DELL_ASSET	Security: Dell Updates
DELL_INVENTORY	Security: Dell Updates
DELL_INVENTORY_APPLICATION_DEVICE_JT	Security: Dell Updates
DELL_INVENTORY_DEVICE_JT	Security: Dell Updates
DELL_INVENTORY_LOG	Security: Dell Updates
DELL_MACHINE_PKG_UPDATE_STATUS	Security: Dell Updates
DELL_MACHINE_STATUS	Security: Dell Updates
DELL_PKG_LABEL_JT	Security: Dell Updates
DELL_PKG_STATUS	Security: Dell Updates
DELL_PKG_UPDATE_HISTORY	Security: Dell Updates

Table	Component
DELL_SCHEDULE	Security: Dell Updates
DELL_SCHEDULE_LABEL_JT	Security: Dell Updates
DELL_SCHEDULE_MACHINE_STATUS	Security: Dell Updates
DELL_SCHEDULE_OS_JT	Security: Dell Updates
DELL_SCHEDULE_UPDATE_LABEL_JT	Security: Dell Updates
DELL_WARRANTY	Security: Dell Updates
DEVICE_DETAIL_FIELD	Inventory: Devices
DEVICE_DETAIL_GROUP	Inventory: Devices
DEVICE_DETAIL_GROUP_ASSET_CLASS_JT	Inventory: Devices
DEVICE_DETAIL_SECTION	Inventory: Devices
DEVICE_DETAIL_SECTION_ASSET_CLASS_JT	Inventory: Devices
FILTER	Labels
FS	File Synchronization
FS_LABEL_JT	File Synchronization
FS_MACHINE_JT	File Synchronization
GLOBAL_OPTIONS	Appliance Administration
GRID_COLUMNS_OVERRIDES	Appliance Administration
HD_ANNOUNCEMENT	Service Desk: Announcements
HD_ANNOUNCEMENT_LABEL_JT	Service Desk: Announcements
HD_ARCHIVE_ATTACHMENT	Service Desk: Ticket Archive
HD_ARCHIVE_TICKET	Service Desk: Ticket Archive
HD_ARCHIVE_TICKET_CHANGE	Service Desk: Ticket Archive
HD_ARCHIVE_TICKET_CHANGE_FIELD	Service Desk: Ticket Archive
HD_ARCHIVE_WORK	Service Desk: Ticket Archive

Table	Component
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: User Console Home Page
HD_IMPACT	Service Desk: Tickets
HD_LINK	Service Desk: User Console Home Page
HD_MAILTEMPLATE	Service Desk: Tickets
HD_PRIORITY	Service Desk: Tickets
HD_QUEUE	Service Desk: Queues
HD_QUEUE_APPROVER_LABEL_JT	Service Desk: Queues
HD_QUEUE_OWNER_LABEL_JT	Service Desk: Queues
HD_QUEUE_SUBMITTER_LABEL_JT	Service Desk: Queue
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 Agreement
HD_SLA_HOLIDAYS	Service Desk: Service Level Agreement
HD_STATUS	Service Desk: Tickets
HD_TICKET	Service Desk: Tickets
HD_TICKET_CHANGE	Service Desk: Tickets
HD_TICKET_CHANGE_FIELD	Service Desk: Tickets
HD_TICKET_FILTER	Service Desk: Tickets

Table	Component
HD_TICKET_RELATED	Service Desk: Tickets
HD_TICKET_RULE	Service Desk: Tickets
HD_WORK	Service Desk: Tickets
IM_CRON	Appliance Administration
KBOT	Scripting
KBOT_CRON_SCHEDULE	Scripting
KBOT_DEPENDENCY	Scripting
KBOT_EVENT_SCHEDULE	Scripting
KBOT_FORM	Scripting
KBOT_FORM_DATA	Scripting
KBOT_LABEL_JT	Scripting
KBOT_LOG	Scripting
KBOT_LOG_DETAIL	Scripting
KBOT_LOG_LATEST	Scripting
KBOT_OS_FAMILY_JT	Scripting
KBOT_OS_JT	Scripting
KBOT_RUN	Scripting
KBOT_RUN_MACHINE	Scripting
KBOT_RUN_TOKEN	Scripting
KBOT_SHELL_SCRIPT	Scripting
KBOT_UPLOAD	Scripting
KBOT_VERIFY	Scripting
KBOT_VERIFY_STEPS	Scripting
KMON_ALERT	Monitoring

Table	Component
KMON_CONDITION	Monitoring
KMON_CONFIG	Monitoring
KMON_CONFIG_DEFAULT	Monitoring
KMON_CONFIG_DETAIL	Monitoring
KMON_CONFIG_DEVICE_JT	Monitoring
KMON_INSTALL_LEP_DEVICE_JT	Monitoring: Log Enablement Packages
KMON_LEP	Monitoring: Log Enablement Package
KMON_LEP_INSTALL	Monitoring: Log Enablement Package
KMON_LOG_CONFIG	Monitoring
KMON_MAINT_CONFIG	Monitoring
KMON_MONITORED_DEVICE	Monitoring
LABEL	Labels
LABEL_LABEL_JT	Labels
LDAP_FILTER	Labels: LDAP
LDAP_IMPORT_USER	Labels: LDAP
MACHINE	Inventory: Devices
MACHINE_ACTIONS	Inventory: Devices
MACHINE_BITLOCKER_VOLUME	Inventory: Devices
MACHINE_CHROMEOS_DETAILS	Inventory: Devices
MACHINE_CUSTOM_INVENTORY	Inventory: Devices
MACHINE_DAILY_UPTIME	Inventory: Devices
MACHINE_DCM_AMT_SETTINGS	Inventory: Devices
MACHINE_DCM_BATTERY	Inventory: Devices
MACHINE_DCM_DESKTOP_MONITOR	Inventory: Devices

Table	Component
MACHINE_DCM_FLAT_PANEL	Inventory: Devices
MACHINE_DCM_LOG_ENTRY	Inventory: Devices
MACHINE_DCM_PHYSICAL_MEMORY	Inventory: Devices
MACHINE_DCM_PROCESSOR	Inventory: Devices
MACHINE_DCM_VPRO_SETTINGS	Inventory: Devices
MACHINE_DDPE	Inventory: Devices
MACHINE_DDPE_VOLUME	Inventory: Devices
MACHINE_DISKS	Inventory: Devices
MACHINE_DRIVE_ENCRYPTION_SUMMARY	Inventory: Devices
MACHINE_FIELD_DEFINITION	Inventory: Devices
MACHINE_FILEVAULT_VOLUME	Inventory: Devices
MACHINE_INTEL_AMT	Inventory: Devices
MACHINE_LABEL_JT	Inventory: Devices
MACHINE_LOCATION	Inventory: Devices
MACHINE_MOBILE	Inventory: Devices
MACHINE_NICS	Inventory: Devices
MACHINE_NTSERVICE_JT	Inventory: Devices
MACHINE_PROCESS_JT	Inventory: Devices
MACHINE_REPLITEM	Inventory: Devices
MACHINE_SNMP_DATA	Inventory: Devices
MACHINE_SOFTWARE_JT	Inventory: Devices
MACHINE_STARTUPPROGRAM_JT	Inventory: Devices
MACHINE_TPM	Inventory: Devices
MESSAGE	Distribution: Alerts

Table	Component
MESSAGE_LABEL_JT	Distribution: Alerts
MI	Distribution: Managed Installations
MI_ATTEMPT	Distribution: Managed Installations
MI_LABEL_JT	Distribution: Managed Installations
NODE	Inventory: Discovery
NODE_LABEL_JT	Inventory: Discovery
NODE_PORTS	Inventory: Discovery
NODE_SNMP_IF	Inventory: Discovery
NODE_SNMP_SYSTEM	Inventory: Discovery
NOTIFICATION	Reporting: Notifications
NOTIFICATION_USER_JT	Reporting: Notifications
NTSERVICE	Inventory: Services
NTSERVICE_LABEL_JT	Inventory: Services
OBJECT_FIELD_DEFINITION	Settings: History
OBJECT_HISTORY	Settings: History
OBJECT_HISTORY_CONFIGURATION	Settings: History
OPERATING_SYSTEMS	Inventory: Devices
PATCH_FILTER	Security: Patch Management
PATCH_LABEL_JT	Security: Patch Management
PATCH_MACHINE_REMEDIATION_STATUS	Security: Patch Management
PATCH_MACHINE_STATUS	Security: Patch Management
PATCH_PATCH_COUNT	Security: Patch Management
PATCH_SCHEDULE	Security: Patch Scheduling
PATCH_SCHEDULE_DEPLOY_LABEL_JT	Security: Patch Scheduling

Table	Component
PATCH_SCHEDULE_DETECT_LABEL_JT	Security: Patch Scheduling
PATCH_SCHEDULE_LABEL_JT	Security: Patch Scheduling
PATCH_SCHEDULE_MACHINE_STATUS	Security: Patch Scheduling
PATCH_SCHEDULE_OS_JT	Security: Patch Scheduling
PATCH_SCHEDULE_ROLLBACK_LABEL_JT	Security: Patch Scheduling
PATCH_SCHEDULE_RUN	Security: Patch Scheduling
PATCH_SCHEDULE_RUN_COUNTS	Security: Patch Scheduling
PATCH_SCHEDULE_RUN_LOG	Security: Patch Scheduling
PATCH_SCHEDULE_RUN_MACHINE	Security: Patch Scheduling
PATCH_SETTINGS	Security: Subscriptions
PATCH_STATUS	Security: Patch Management
PORTAL	Service Desk: **User Console**
PORTAL_LABEL_JT	Service Desk: **User Console**
PROCESS	Inventory: Processes
PROCESS_LABEL_JT	Inventory: Process
PROVISION_CONFIG	Settings: Agent Provisioning
PROVISION_NODE	Settings: Agent Provisioning
REMOTE_CHROMEOS_HOST	Settings: Agentless Provisioning
REMOTE_DMM_HOST	Settings: Agentless: Dell Mobility Manager
REMOTE_HOST	Settings: Agentless Provisioning
REMOTE_HOST_KUID	Settings: Agentless Provisioning
REMOTE_SHELL_HOST	Settings: Agentless Provisioning
REMOTE_SNMP_HOST	Settings: Agentless Provisioning
REMOTE_WSMAN_HOST	Settings: Agentless Provisioning

Table	Component
REPLICATION_LANGUAGE	Distribution: Replication
REPLICATION_PLATFORM	Distribution: Replication
REPLICATION_SCHEDULE	Distribution: Replication
REPLICATION_SHARE	Distribution: Replication
REPORT_FIELD	Reporting
REPORT_FIELD_GROUP	Reporting
REPORT_JOIN	Reporting
REPORT_OBJECT	Reporting
REPORT_OBJECT_JOIN	Reporting
REPORT_SCHEDULE	Reporting
SAM_CATALOG_FILTER	Inventory: Software Catalog
SAM_CATALOG_LABEL_JT	Inventory: Software Catalog
SAM_COMPLIANCE_DETAIL	Asset Management: License Compliance
SAM_COMPLIANCE_SUMMARY	Asset Management: License Compliance
SAM_COUNT	Inventory: Software Catalog
SAM_MACHINE_JT	Inventory: Software Catalog
SAM_MACHINE_TERMINATED_APPS	Inventory: Software Catalog
SAM_METER	Inventory: Software Catalog
SAM_METER_DATA	Inventory: Software Catalog
SAM_METER_TITLED_APPLICATION	Inventory: Software Catalog
SAM_NOT_ALLOWED	Inventory: Software Catalog
SAVED_SEARCH	Appliance Administration
SCAN_FILTER	Inventory: Discovery
SCAN_SETTINGS	Inventory: Discovery

Table	Component
SETTINGS	Settings
SETTINGS_HISTORY	Settings: History
SETTINGS_HISTORY_CONFIGURATION	Settings: History
SETTINGS_HISTORY_FIELD_DEFINITION	Settings: History
SMARTY_REPORT	Reporting
SNMP_INVENTORY_OIDS	Inventory: SNMP
SNMP_INVENTORY_SETTINGS	Inventory: SNMP
SNMP_INVENTORY_SETTINGS_JT	Inventory: SNMP
SNOOZE_ALERT	Patch Schedules
SOFTWARE	Inventory: Software
SOFTWARE_LABEL_JT	Inventory: Software
SOFTWARE_OS_JT	Inventory: Software
STARTUPPROGRAM	Inventory: Startup Programs
STARTUPPROGRAM_LABEL_JT	Inventory: Startup Programs
THROTTLE	Appliance Administration
USER	Settings: Users
USERIMPORT_SCHEDULE	Settings: User Authentication
USER_AUTO_REFRESH	Settings: Users
USER_HISTORY	Settings: Users
USER_KEYS	Settings: Users
USER_LABEL_JT	Settings: Users
USER_ROLE	Settings: Users
USER_ROLE_PERMISSION_VALUE	Settings: Users

System-level (KBSYS) database tables

The following table shows the System-level (KBSYS) database table names. Reference these table names when creating custom reports using SQL queries. See Create reports using SQL queries.

Table 37. KBSYS database tables and components

Table	Component
ACCESS_STATS	Appliance Administration (used to track page views)
AGENTLESS_TASK	Inventory
APPLE_MODEL	Inventory: Devices
AUTHENTICATION	Settings: Users
CLIENT_CRASH	Appliance Administration
COUNTRYCODE_MAPPING	Inventory: Devices(used for Dell devices)
CREDENTIAL_CONSUMER	Settings: Credentials
DASHBOARD	Dashboard
DASHBOARD_BASE_WIDGETS	Dashboard
DASHBOARD_CACHE	Dashboard
DASHBOARD_CUSTOM_WIDGETS	Dashboard
DASHBOARD_DATASOURCES	Dashboard
DASHBOARD_WIDGET_TYPES	Dashboard
DELL_CATALOG	Security: Dell Updates
DELL_CRITICALITY	Security: Dell Updates
DELL_ERROR_CODE	Security: Dell Updates
DELL_PKG	Security: Dell Updates
DELL_PKG_DEVICE	Security: Dell Updates
DELL_PKG_DEVICE_DEPENDENCY	Security: Dell Updates
DELL_PKG_DEVICE_PCI	Security: Dell Updates
DELL_PKG_DEVICE_PNP	Security: Dell Updates
DELL_PKG_DEVICE_VERSION	Security: Dell Updates

Table	Component
DELL_PKG_OS	Security: Dell Updates
DELL_PKG_OS_LANG	Security: Dell Updates
DELL_PKG_SYSTEM	Security: Dell Updates
DELL_RESOURCE	Security: Dell Updates
DELL_SUPPORTED_MODELS	Security: Dell Updates
DELL_UPDATE_STATUS	Security: Dell Updates
GLOBAL_OPTIONS	Appliance Administration
GRID_COLUMNS_BASE	Appliance Administration
GRID_COLUMNS_OVERRIDES	Appliance Administration
HD_EMAIL_EXCLUSION	Service Desk: Email Exclusion List
HISTORY_FIELD_VALUE_LABEL_MAP	Settings: History
IM_CRON	Appliance Administration (used for scheduled processes)
INVENTORY	Inventory
INVENTORY_FAILURES	Inventory
KBOT_GRAMMAR	Scripting
KBOT_GRAMMAR_ATTRIBUTE	Scripting
KBOT_UPLOAD_TOKENS	Scripting
KBOX	Scripting
KBOX_VERSION	Scripting
KONDUCTOR_TASK	Appliance Administration
KUID_MACHINE	Appliance Administration
KUID_ORGANIZATION	Appliance Administration
LICENSE_MODE	Appliance Administration
LINKED_APPLIANCE	Settings: Appliance Linking

Table	Component
LINKED_USER_TOKEN	Settings: Appliance Linking
LOCALE_BROWSER	Appliance Administration
LOCALE_COLLATION_RULES	Appliance Administration
LOCALE_SERVER	Appliance Administration
LOCALE_TIME_FORMAT	Appliance Administration
MSI_ERROR_CODES	Distribution
NETWORK_SETTINGS	Appliance Administration
ORGANIZATION	Organizations
ORGANIZATION_FILTER	Organizations: Filters
ORGANIZATION_FILTER_CRITERIA	Organizations: Filters
ORGANIZATION_FILTER_CRITERIA_LDAP	Organizations: Filters
ORG_ROLE	Organizations: Roles
ORG_ROLE_PERMISSION_VALUE	Organizations: Roles
OS_FAMILY	Inventory: Devices
PATCH_ATTRIBUTE	Security: Patch Management
PATCH_CATALOG_RUN_STATUS	Security: Patch Management
PATCH_CATALOG_UPDATE_STATUS	Security: Patch Management
PATCH_ERROR_CODE	Security: Patch Management
PATCH_LANGUAGE	Security: Patch Management
PATCH_OS	Security: Patch Management
PATCH_PACKAGE	Security: Patch Management
PATCH_PAYLOAD_DOWNLOAD_STATUS	Security: Patch Management
PATCH_PRODUCT	Security: Patch Management
PATCH_PRODUCT_JT	Security: Patch Management

Table	Component
PATCH_PRODUCT_OS_JT	Security: Patch Management
PATCH_PRODUCT_TITLED_APPLICATION_JT	Security: Patch Management
PATCH_PRODUCT_TITLED_SUITE_JT	Security: Patch Management
PATCH_RESOURCE	Security: Patch Management
PATCH_SUPERCEDES_JT	Security: Patch Management
PERMISSION_DEFINITION	Settings: Roles
PORT_SERVICES	Inventory: Discovery
PROVISIONING_ERRORS	Settings: Provisioning
REPORT_FIELD	Reporting
REPORT_FIELD_GROUP	Reporting
REPORT_JOIN	Reporting
REPORT_OBJECT	Reporting
REPORT_OBJECT_JOIN	Reporting
REPORT_SCHEDULE	Reporting
RESOURCE_EXPORTED	Settings: Resources
RESOURCE_QUEUE	Settings: Resources
SAM_APPLICATION	Software Catalog
SAM_HARDWARE	Software Catalog
SAM_LINUX_APPLICATION	Software Catalog
SAM_MUI_CACHE_DATA	Software Catalog
SAM_PUBLISHER	Software Catalog
SAM_SOFTWARE_TAG	Software Catalog
SAM_TITLE_REQUEST	Software Catalog
SAM_VIEW_ALL_SOFTWARE	Software Catalog

Table	Component
SAM_VIEW_DISCOVERED_APPLICATIONS	Software Catalog
SAM_VIEW_DISCOVERED_SOFTWARE	Software Catalog
SAM_VIEW_DISCOVERED_SUITES	Software Catalog
SAM_VIEW_INVENTORY_ADD_REMOVE_PROGRAMS	Software Catalog
SAM_VIEW_INVENTORY_MOBILE_APPS	Software Catalog
SAM_VIEW_MACHINE_DISCOVERED_SOFTWARE	Software Catalog
SAM_VIEW_TITLED_SOFTWARE	Software Catalog
SERVER_CRASH	Appliance Administration (used to track internal errors)
SERVICE_LEVEL_MAPPING	Inventory: Devices (used for Dell devices)
SETTINGS	Settings
SETTINGS_HISTORY	Settings: History
SETTINGS_HISTORY_CONFIGURATION	Settings: History
SETTINGS_HISTORY_FIELD_DEFINITION	Settings: History
SHAPING_METADATA	Inventory: API
SMARTY_REPORT	Reporting
SMMP_CONNECTION	Discovery
SMMP_CONNECTION_PLUGIN_JT	Discovery
SMMP_MSG_Q	Discovery
SMMP_NIC	Discovery
SMMP_PLUGIN	Discovery
SOFTWARE_INVENTORY	Inventory
SOFTWARE_INVENTORY_FAILURES	Inventory
SSL_CERT	Settings: Security Settings

Table	Component
SSL_CSR	Settings: Security Settings
SSL_PRIVATEKEY	Settings: Security Settings
SYSTEM_DEFINED_ROLES	Organizations: Roles
TIME_SETTINGS	Settings: Date and Time Settings
USER	Settings: Authentication
USER_AUTH	Settings: Authentication
USER_AUTO_REFRESH	Settings: Authentication

Adding steps to task sections of scripts

You can add steps to scripts in the Scripting component.

The following tables detail the steps that can be added to the task sections of scripts. Task sections are available on the *Script Detail* page when you add a task. See Adding and editing scripts.

The column headings *V*, *OS*, *R*, *ORS*, and *ORF* indicate whether a particular step is available in the corresponding task sections: *Verify*, *On Success*, *Remediation*, *On Remediation Success*, and *On Remediation Failure*.

- Steps for Windows devices
- Steps for Mac OS X devices
- Steps for Red Hat Enterprise Linux devices

Steps for Windows devices

NOTE: For the syntax to use when specifying registry paths, see Specifying Windows registry paths.

Table 38. Adding steps to scripts used on Windows devices

Step	Description	V	OS	R	ORS	ORF
Always fail		X		X		
Call a custom DLL function	Call function "%{procName}" from "%{path}\%{file}".	X	X	X		
Create a custom DLL object	Create object "%{className}" from "%{path}\%{file}".	X	X	X		
Create a message window	Create a message window named "%{name}" with title "%{title}", message	X	X	X	X	X

Step	Description	V	OS	R	ORS	ORF
	"%{message}" and timeout "%{timeout}" seconds.					
Delete a registry key	Delete "%{key}" from the registry. See Specifying Windows registry paths.		X	X		
Delete a registry value	Delete "%{key}!%{name}" from the registry. See Specifying Windows registry paths.		X	X		
Destroy a message window	Destroy the message window named "%{name}".	X	X	X	X	X
Install an application package	Install "%{name}" with arguments "%{install_cmd}". **NOTE:** This step requires you to choose from a list of application packages already uploaded using the functionality in the *Inventory* > *Software* page. See Adding and deleting applications in Software page inventory.		X	X		
Stop a process	Stop the process "%{name}".	X	X	X	X	X
Launch a program	Launch "%{path}\%{program}" with params "%{parms}".	X	X	X	X	X
Log a registry value	Log "%{key}!%{name}".			X		
Log file information	Log "%{attrib}" from ""%{path}\%{file}".			X	X	X
Log message	Log "%{message}" to "%{type}".			X		
Restart a service	Restart service "%{name}"			X		
Run a batch file	Run the batch file "%{_fake_name}" with params "%{parms}". **NOTE:** In this step, you do not need to upload the batch file. You create the batch file by pasting the script in the space provided.	X	X	X		
Set a registry key	Set "%{key}".	X	X			
Set a registry value	Set "%{key}!%{name}" to "%{newValue}".	X	X			
Start a service	Restart service "%{name}".			X		
Stop a service	Stop service "%{name}"			X		
Unzip a file	Unzip "%{path}\%{file}" to "%{target}".	X		X	X	X

Step	Description	V	OS	R	ORS	ORF
Update message window text	Set the text in the message window named "%{name}" to "%{text}".	X		X	X	X
Update policy and job schedule	Update policy and job schedule from the appliance.	X				
Upload a file	Upload "%{path}\%{file}" to the server.		X	X		
Verify a directory exists	Verify that the directory "%{path}" exists.	X				
Verify a file exists	Verify that the file "%{path}\%{file}" exists.	X				
Verify a file version is exactly	Verify that the file "%{path}\%{file}" has version "%{expectedValue}".	X				
Verify a file version is greater than	Verify that the file "%{path}\%{file}" has version greater than "%{expectedValue}".	X				
Verify a file version is greater than or equal to	Verify that the file "%{path}\%{file}" has version greater than or equal to "%{expectedValue}".	X				
Verify a file version is less than	Verify that the file "%{path}\%{file}" has version less than "%{expectedValue}".	X				
Verify a file version is less than or equal to	Verify that the file "%{path}\%{file}" has version less than or equal to "%{expectedValue}.	X				
Verify a file version is not	Verify that the file "%{path}\%{file}" does not have version "%{expectedValue}".	X				
Verify a file was modified since	Verify that the file "%{path}\%{file}" was modified since "%{expectedValue}".	X				
Verify a process is not running	Verify the process "%{name}" is not running.	X				
Verify a process is running	Verify the process "%{name}" is running.	X				
Verify a product version is exactly	Verify that the product "%{path}\%{file}" has version "%{expectedValue}".	X				
Verify a product version is greater than	Verify that the product "%{path}\ %{file}" has version greater than "%{expectedValue}".	X				

Step	Description	V	OS	R	ORS	ORF
Verify a product version is greater than or equal to	Verify that the product "%{path}\%{file}" has version greater than or equal to "%{expected-Value}".	X				
Verify a product version is less than	Verify that the product "%{path}\%{file}" has version less than "%{expectedValue}".	X				
Verify a product version is less than or equal to	Verify that the product "%{path}\%{file}" has version less than or equal to "%{expectedValue}".	X				
Verify a product version is not	Verify that the product "%{path}\%{file}" does not have version "%{expectedValue}".	X				
NOTE: For the syntax to use when specifying registry paths, see Specifying Windows registry paths.						
Verify a registry key does not exist	Verify that "%{key}" does not exist.	X				
Verify a registry key exists	Verify that "%{key}" exists.	X				
Verify a registry key's subkey count is exactly	Verify that "%{key}" has exactly "%{expectedValue}" subkeys.	X				
Verify a registry key's subkey count is greater than	Verify that "%{key}" has greater than "%{expectedValue}" subkeys.	X				
Verify a registry key's subkey count is greater than or equal to	Verify that "%{key}" has greater than or equal to "%{expectedValue}" subkeys.	X				
Verify a registry key's subkey count is less than	Verify that "%{key}" has less than "%{expectedValue}" subkeys.	X				
Verify a registry key's subkey count is less than or equal to	Verify that "%{key}" has less than or equal to "%{expectedValue}" subkeys.	X				
Verify a registry key's subkey count is not	Verify that "%{key}" does not have exactly "%{expectedValue}" subkeys.	X				
Verify a registry key's value count is exactly	Verify that "%{key}" has exactly "%{expectedValue}" values.	X				

Step	Description	V	OS	R	ORS	ORF
Verify a registry key's value count is greater than	Verify that "%{key}" has greater than "%{expectedValue}" values.	X				
Verify a registry key's value count is greater than or equal to	Verify that "%{key}" has greater than or equal to "%{expectedValue}" values.	X				
Verify a registry key's value count is less than	Verify that "%{key}" has less than "%{expectedValue}" values.	X				
Verify a registry key's value count is less than or equal to	Verify that "%{key}" has less than or equal to "%{expectedValue}" values.	X				
Verify a registry key's value count is not	Verify that "%{key}" does not have exactly "%{expectedValue}" values.	X				
Verify a registry pattern doesn't match	Verify that "%{key}!%{name}= %{expectedValue}" doesn't match.	X				
Verify a registry pattern match	Verify that "%{key}!%{name}= %{expectedValue}" matches.	X				
Verify a registry value does not exist	Verify that "%{key}!%{name}" does not exist.	X				
Verify a registry value exists	Verify that "%{key}!%{name}" exists.	X				
Verify a registry value is exactly	Verify that "%{key}!%{name}" is equal to "%{expectedValue}".	X				
Verify a registry value is greater than	Verify that "%{key}!%{name}" is greater than "%{expectedValue}".	X				
Verify a registry value is greater than or equal to	Verify that "%{key}!%{name}" is greater than or equal to "%{expectedValue}" .	X				
Verify a registry value is less than	Verify that "%{key}!%{name}" is less than "%{expectedValue}".	X				
Verify a registry value is less than or equal to	Verify that "%{key}!%{name}" is less than or equal to "%{expectedValue}".	X				

Step	Description	V	OS	R	ORS	ORF
Verify a registry value is not	Verify that "%{key}!%{name}" is not equal to "%{expectedValue}".	X				
Verify a service exists	Verify the service "%{name}" exists.	X				
Verify a service is running	Verify the service "%{name}" is running.	X				

Specifying Windows registry paths

When specifying Windows registry paths, use the base key and specify whether the registry is on a device with 32-bit or 64-bit operating system and hardware.

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

For example, specify the path for HKEY_LOCAL_MACHINE for 32- and 64-bit Windows devices as follows:

- `HKLM\Software\32BitProgramA\installDate`
- `HKLM64\Software\64BitProgramB\installDate`

Steps for Mac OS X devices

Table 39. Adding steps to scripts used on Mac OS X devices

Step	Description	V	OS	R	ORS	ORF
Always fail		X		X		
Create a message window	Create a message window named "%{name}" with title "%{title}", message "%{message}" and timeout "%{timeout}" seconds.	X	X	X	X	X
Destroy a message window	Destroy the message window named "%{name}".	X	X	X	X	X

Step	Description	V	OS	R	ORS	ORF
Stop a process	Stop the process "%{name}".	X	X	X	X	X
Launch a program	Launch "%{path}\%{program}" with params "%{parms}".	X	X	X	X	X
Log a plist value	Log "%{key}!%{name};"			X		
Log message	Log "%{message}" to "%{type}".			X		
Search file system	Search for "%{name}" in "%{startingDirectory}" on "%{drives}" and "%{action}".	X				
Unzip a file	Unzip "%{path}\%{file}" to "%{target}".	X		X	X	X
Update message window text	Set the text in the message window named "%{name}" to "%{text}".	X		X	X	X
Update policy and job schedule	Update policy and job schedule from the appliance.	X				
Upload a file	Upload "%{path}\%{file}" to the server.		X	X		
Verify a directory exists	Verify that the directory "%{path}" exists.	X				
Verify a file exists	Verify that the file "%{path}\%{file}" exists.	X				
Verify a file was modified since	Verify that the file "%{path}\%{file}" was modified since "%{expectedValue}".	X				
Verify a process is not running	Verify the process "%{name}" is not running.	X				
Verify a process is running	Verify the process "%{name}" is running.	X				
Verify a plist value equals		X				
Verify a plist value exists	Verify that "%{key}" exists.	X				
Verify a plist value greater than		X				
Verify a plist value less than		X				

Step	Description	V	OS	R	ORS	ORF
Verify an environment variable equals		X				
Verify an environment variable exists		X				
Verify an environment variable greater than		X				
Verify an environment variable less than		X				
Verify at least one file matching regex exists		X				
Verify count of filenames matching regex is greater than		X				
Verify count of filenames matching regex is less than		X				
Verify count of filenames matching regex		X				
Verify file info equals		X				
Verify file info greater than		X				
Verify file info less than		X				

Steps for Red Hat Enterprise Linux devices

Table 40. Adding steps to scripts for RHEL

Step	Description	V	OS	R	ORS	ORF
Always fail		X		X		
Stop a process	Stop the process "%{name}".	X	X	X	X	X
Launch a program	Launch "%{path}\%{program}" with params "%{parms}".	X	X	X	X	X

Step	Description	V	OS	R	ORS	ORF
Log message	Log "%{message}" to "%{type}".			X		
Search file system	Search for "%{name}" in "%{startingDirectory}" on "%{drives}" and "%{action}".	X				
Unzip a file	Unzip "%{path}\%{file}" to "%{target}".	X		X	X	X
Update policy and job schedule	Update policy and job schedule from the appliance.	X				
Upload a file	Upload "%{path}\%{file}" to the server.		X	X		
Verify a directory exists	Verify that the directory "%{path}" exists.	X				
Verify a file exists	Verify that the file "%{path}\%{file}" exists.	X				
Verify a file was modified since	Verify that the file "%{path}\%{file}" was modified since "%{expectedValue}".	X				
Verify a process is not running	Verify the process "%{name}" is not running.	X				
Verify a process is running	Verify the process "%{name}" is running.	X				
Verify an environment variable less than		X				
Verify at least one file matching regex exists		X				
Verify count of filenames matching regex is greater than		X				
Verify count of filenames matching regex is less than		X				
Verify count of filenames matching regex		X				
Verify file info equals		X				
Verify file info greater than		X				

Step	Description	V	OS	R	ORS	ORF
Verify file info less than		X				

LDAP variables

The appliance supports variables for use in LDAP Labels and database queries.

Device or machine variables

Device or machine variables can be used in LDAP Labels and queries to automatically group devices by name, description, and other LDAP criteria. During LDAP Label processing, the appliance replaces all `KBOX_` defined variables with their respective runtime values. The following table shows supported device or machine variables and their mapping to columns in the MACHINE database table and LDAP attributes.

Table 41. Device or machine variables and mappings

Appliance variable	Appliance MACHINE database table column	LDAP attribute mapping
KBOX_COMPUTER_NAME	NAME	cn | name
KBOX_COMPUTER_DESCRIPTION	SYSTEM_DESCRIPTION	description
KBOX_COMPUTER_MAC	MAC	macAddress
KBOX_COMPUTER_IP	IP	ipHostNumber
KBOX_USER	USER_NAME	
KBOX_USER_DOMAIN	USER_DOMAIN	
KBOX_DOMAINUSER	USER	
KBOX_CUSTOM_INVENTORY_*	CUSTOM_INVENTORY	

The KBOX_CUSTOM_INVENTORY_* variable can be used to check a custom inventory value. The * is replaced with the Display Name of the custom inventory rule. Allowed characters are [a-z0-9.-]. Any other characters are replaced with an underscore (_).

User variables

User variables can be used in LDAP Labels and queries to automatically group users by domain, location, budget code, or other LDAP criteria. During LDAP Label processing, the appliance replaces all `KBOX_` defined variables with their respective runtime values. The following table shows supported user variables and their mapping to columns in the USER database table and LDAP attributes.

Table 42. User variables and mappings

Appliance variable	Appliance USER database table column	LDAP attribute mapping
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	
KBOX_CUSTOM_3	CUSTOM_3	
KBOX_CUSTOM_4	CUSTOM_4	
KBOX_ROLE_ID	ROLE_ID	
KBOX_API_ENABLED	API_ENABLED	• No value: Disable user access to the KACE GO app
KBOX_AMS_ID	AMS_ID	No value. This variable is not used.
KBOX_LOCALE_BROWSER_ID	LOCALE_BROWSER_ID	
KBOX_HD_DEFAULT_QUEUE_ID	HD_DEFAULT_QUEUE_ID	
KBOX_LDAP_UID	LDAP_UID	objectGUID

List of Countries

The following is the list of countries.

NOTE: To ensure proper display on the World Geo Map widget chart, the country name must exactly match the one from the list below.

Table 43. ORG1 database tables and components

Country Name	Country Name
Zimbabwe	El Salvador
Zambia	Egypt
Yemen	Ecuador
Vietnam	Dominican Rep.
Venezuela	Dominica
Vatican	Djibouti
Vanuatu	Greenland
Uzbekistan	Faeroe Is.
Uruguay	Denmark
Micronesia	Czechia
Marshall Is.	N. Cyprus
N. Mariana Is.	Cyprus
U.S. Virgin Is.	Cuba
Guam	Croatia
American Samoa	Côte d'Ivoire
Puerto Rico	Costa Rica
United States of America	Dem. Rep. Congo
S. Geo. and the Is.	Congo
Br. Indian Ocean Ter.	Comoros

Country Name	Country Name
Saint Helena	Colombia
Pitcairn Is.	China
Anguilla	Macao
Falkland Is.	Hong Kong
Cayman Is.	Chile
Bermuda	Chad
British Virgin Is.	Central African Rep.
Turks and Caicos Is.	Cabo Verde
Montserrat	Canada
Jersey	Cameroon
Guernsey	Cambodia
Isle of Man	Myanmar
United Kingdom	Burundi
United Arab Emirates	Burkina Faso
Ukraine	Bulgaria
Uganda	Brunei
Turkmenistan	Brazil
Turkey	Botswana
Tunisia	Bosnia and Herz.
Trinidad and Tobago	Bolivia
Tonga	Bhutan
Togo	Benin
Timor-Leste	Belize
Thailand	Belgium

Country Name	Country Name
Tanzania	Belarus
Tajikistan	Barbados
Taiwan	Bangladesh
Syria	Bahrain
Switzerland	Bahamas
Sweden	Azerbaijan
eSwatini	Austria
Suriname	Australia
S. Sudan	Indian Ocean Ter.
Sudan	Heard I. and McDonald Is.
Sri Lanka	Norfolk Island
Spain	Ashmore and Cartier Is.
South Korea	Armenia
South Africa	Argentina
Somalia	Antigua and Barb.
Somaliland	Angola
Solomon Is.	Andorra
Slovakia	Algeria
Slovenia	Albania
Singapore	Afghanistan
Sierra Leone	Siachen Glacier
Seychelles	Antarctica
Serbia	Sint Maarten
Senegal	Palestine

Country Name	Country Name
Saudi Arabia	Ireland
São Tomé and Principe	Iraq
San Marino	Iran
Samoa	Indonesia
St. Vin. and Gren.	India
Saint Lucia	Iceland
St. Kitts and Nevis	Hungary
Rwanda	Honduras
Russia	Haiti
Romania	Guyana
Qatar	Guinea-Bissau
Portugal	Guinea
Poland	Guatemala
Philippines	Grenada
Peru	Greece
Paraguay	Ghana
Papua New Guinea	Germany
Panama	Georgia
Palau	Gambia
Pakistan	Gabon
Oman	France
Norway	St. Pierre and Miquelon
North Korea	Wallis and Futuna Is.
Nigeria	St-Martin

Country Name	Country Name
Niger	St-Barthélemy
Nicaragua	Fr. Polynesia
New Zealand	New Caledonia
Niue	Fr. S. Antarctic Lands
Cook Is.	Åland
Netherlands	Finland
Aruba	Fiji
Curaçao	Ethiopia
Nepal	Estonia
Nauru	Eritrea
Namibia	Eq. Guinea
Mozambique	Lithuania
Morocco	Liechtenstein
W. Sahara	Libya
Montenegro	Liberia
Mongolia	Lesotho
Moldova	Lebanon
Monaco	Latvia
Mexico	Laos
Mauritius	Kyrgyzstan
Mauritania	Kuwait
Malta	Kosovo
Mali	Kiribati
Maldives	Kenya

Country Name	Country Name
Malaysia	Kazakhstan
Malawi	Jordan
Madagascar	Japan
Macedonia	Jamaica
Luxembourg	Italy
Israel	

Glossary

A

Acceptable Use Policy

A statement or policy that is displayed to users when they log in to the **Administrator Console**, **Command Line Console**, or **User Console**. See Enable or disable the Acceptable Use Policy.

add to catalog request

A cataloging request is a form you can submit to request that an application that is not included in the Software Catalog (Uncataloged) be added to the public Software Catalog. When Quest receives a cataloging request, that request is evaluated to determine whether or not the application should become part of the public Software Catalog. In addition, applications are automatically added to the local version of the Software Catalog on the appliance when cataloging requests are submitted. See Adding applications to the Software Catalog.

Administrator Console

The **Administrator Console** is the web-based interface used to control the appliance. To access the **Administrator Console**, go to `http://<appliance_hostname>/admin` where `<appliance_hostname>` is the hostname of your appliance. If the Organization component is enabled, you can access the System-level settings of the **Administrator Console** at `http://<appliance_hostname>/system`. To view the full path of URLs in the **Administrator Console**, which can be useful when searching the database or sharing links, add ui to the URL you use to log in. For example: `http://<appliance_hostname>/admin`.

Agent

The KACE Agent is an application that can be installed on devices to enable device management through the appliance. Agents that are installed on managed devices communicate with the appliance through the agent messaging protocol. Agents perform scheduled tasks, such as collecting inventory information from, and distributing software to, managed devices. Agentless management is available for devices that cannot have Agent software installed, such as printers and devices with operating systems that are not supported by the Agent. See Provisioning the KACE Agent.

Agentless management

Agentless device management is a method of managing devices without the need to deploy and maintain the KACE Agent software on those devices. Agentless management uses SSH, SNMP, and other methods to connect to Agent-intolerant devices, such as printers, network devices, and storage devices, and report inventory in the appliance **Administrator Console**. This is useful for operating system versions and distributions that are not supported by the KACE Agent, and where Agentless management is preferred over installing the Agent. See Managing Agentless devices.

alerts

Broadcast alerts are messages, such as pop-ups, that can be broadcast from the appliance to be displayed on Agent-managed devices. Displaying alerts is useful when you need to communicate urgent information, or notify users before running actions or scripts on their devices. See Broadcasting alerts to managed devices.

Monitoring alerts are messages that are generated on supported server devices and sent to the appliance to alert staff about errors and issues being reported in the event and system logs of the devices. See Monitoring devices.

alternate download location

An alternate download location can be any network location that has all the files required to install a particular application. You can distribute packages from alternate download locations including a UNC address or DFS source. The CIFS and SMB protocols, Samba servers, and file server appliances are

supported. You specify the location when you create a Managed Installation. See Using Managed Installations.

app

See KACE GO .

appliance linking

Appliance linking enables you to log in to one appliance and access all linked appliances from the drop-down list in the top-right corner of the **Administrator Console**, without having to log in to each appliance separately. You can link all of the Quest K-Series appliances you manage. See Linking Quest KACE appliances.

appliance or virtual appliance

The appliance is available as a physical or hardware-based appliance, and as a virtual appliance. The virtual appliance uses a VMware infrastructure. The same system management features are available on both the physical and virtual appliances. See About the appliance components.

Application Control

Application Control enables you to mark applications as Not Allowed and block them or prevent them from running on Agent-managed Windows and Mac devices. This is useful if you want to restrict specific applications from running in your environment. See Apply the Application Control label to devices.

Asset Management

Support for complex license compliance reporting, building on the framework of data collected through the appliance Inventory process. Asset Management also enables you to track additional data about managed devices, including purchase dates, support contracts, asset tags, and so on. See About the Asset Management component.

assets, Asset Types, and Asset Subtypes used in the Asset Management component

Assets and Asset Types used in the Asset Management component include physical and logical items, such as devices, applications, printers, licenses, departments, locations, and vendors. The Asset Management component enables you to build relationships between assets, track inventory data, view records of changes, and report on changes to assets. Assets are based on Asset Types. You can modify default Asset Types, create custom Asset Types, and import asset information as needed. See About Asset Types. Asset Subtypes are subcategories of assets that you can add to any Asset Type, including custom Asset Types. This enables you to identify and manage subtypes of assets, such as Device assets that are computers, printers, or routers, and Software assets that run on Windows, Mac, or Linux systems in the appliance inventory. See About Asset Subtypes, custom fields, and device detail preferences.

Chromebooks & Network Devices that count toward your appliance license limit

Your appliance license agreement entitles you to manage a specified number of endpoints that are categorized as Chromebooks & Network Devices, and these endpoints differ from assets used in the Asset Management component. Endpoints that count toward your license limit include devices that 1) have been added to the appliance inventory but do not meet the definition of Managed Computers or Monitored Computers and 2) were not added to inventory manually, through the WSAPI, or through mobile management. Examples of Assets include printers, projectors, network gear, and storage devices.

NOTE: The assets you create and manage using the Asset Management component do not count toward the license limit.

See View product licensing information.

AUP

See Acceptable Use Policy .

automatic labels

Labels that are applied automatically, such as Smart Labels. See Setting up and using labels to manage groups of items.

B

blocking

See Application Control .

C

Cataloged applications

Cataloged applications are executables that are in the official Software Catalog database. This includes both applications that appear in the appliance inventory (Discovered applications) and applications that do not appear in appliance inventory (Not Discovered applications). See About cataloged applications.

catalog request

See add to catalog request .

category

See software category .

change management

The ability to track changes made to items in the **Administrator Console**, such as scripts, reports, assets, and settings. See Configuring history settings.

Charlie Root

The email address used for communication from the appliance.

NOTE: Notifications and daily reports come from the default address, Charlie Root, (`root@<appliance_hostname>`) and you cannot modify this address.

Classic Metering

Classic Metering is the metering system that was available on the appliance prior to version 5.5. If you upgraded to version 5.5 from version 5.4 or lower, and you enabled metering prior to the upgrade, you can continue to access Classic Metering in the appliance 5.5 release. However, the Software Catalog metering system, which provides more detailed information than Classic Metering, replaced Classic Metering in the 6.0 release. Classic Metering is no longer available in version 6.0 and higher. See metering .

Classic Reports

The reporting feature available on the appliance version 5.2 and lower. Classic Reports are no longer available in version 5.5 and higher.

Client Drop location

The Client Drop location is a file share used for uploading large files, such as application installers and appliance backup files, to the appliance. Uploading files to the Client Drop location is an alternative to uploading files through the **Administrator Console** using the default HTTP mechanism, which can result in browser timeouts for large files. See Copy files to the appliance Client Drop location.

clients

See devices .

Command Line Console

The **Command Line Console** is a terminal window interface to the appliance. The interface is designed primarily to configure the appliance and enforce policies if the **Administrator Console** is not accessible. See Power-on the appliance and log in to the Administrator Console.

Computers

Computers is a category of devices that can be managed by the appliance. Examples of Computers include personal computers, servers, laptops, tablets, and smart phones. Your appliance license agreement entitles you to manage a specified number of Computers. See Managed Computers .

Credentials Management

Credentials Management enables you to organize the usernames and passwords required for logging in to other systems, such as managed computers and servers, and the information required for Google or SNMP authentication. This streamlines the process of entering and managing credentials and authentication information. See Managing credentials.

D

data retention

The options for saving data for metering, device uptime, uncataloged applications, and backups on the appliance. See Configure Admin-level or organization-specific General Settings and Set the daily backup schedule and the number of backups to retain.

data sharing

The options for sharing appliance information with Quest KACE. See Configure data sharing preferences.

Dell Command | Monitor

Dell Command | Monitor is the monitoring tool of the Dell Command Suite. It enables remote management applications, such as the appliance, to access management information, monitor status, and change the state of enterprise client systems. If Dell Command | Monitor is detected on a managed device, the appliance uses the WMI (Windows Management Instrumentation) interface to collect detailed hardware inventory and health status. See .

Device Actions

A feature that enables you to run commands on managed devices from the *Devices* list. For information about setting up Device Actions, see Configure appliance General Settings without the Organization component.

devices

Devices are machines, or endpoints, that are managed by the appliance. Your product license agreement entitles you to manage a specified number of devices, which are classified as Managed Computers, Assets, and Monitored Computers. Managed devices report data, such as software, hardware, and networking information, to the appliance. See View product licensing information.

Discovered applications

Discovered applications are executables in the appliance inventory that match the definitions of applications in the Software Catalog. You can enable metering for Discovered applications and suites, mark them as Not Allowed, and add license information for them. In addition, the Discovered software list can be exported in CSV format. You can export the Discovered software list, the Uncataloged list, and the Locally Cataloged list; you cannot export the entire Software Catalog.

Compare to Not Discovered applications . See Discovered applications.

Discovery

Discovery is the process of identifying devices that are connected to the network and retrieving information about those devices. Devices that can be discovered include laptops, desktops, servers, mobile devices, virtual devices, printers, network devices, wireless access points, routers, switches and more. These devices can be scanned and identified even if they do not have the KACE Agent installed on them. You can run Discovery scans on-demand or schedule scans to run at specific times. See About Device Discovery and device management.

E

email alerts

See alerts .

F

fast switching for organizations and linked appliances

Fast switching makes it possible to switch from one organization to another using a drop-down list in the top-right corner of the **Administrator Console** instead of logging in to each organization separately. Also, it makes it possible to switch between linked K-Series appliances without logging in to each appliance separately. See Enable fast switching for organizations and linked appliances.

File Synchronizations

File Synchronizations enable you to distribute files to managed devices. Unlike Managed Installations, however, File Synchronizations do not install files; they simply distribute files. Use File Synchronizations to copy files of any type to managed devices. See Create and use File Synchronization.

filters

See labels and organization filters .

I

Inventory

Inventory includes information about the devices, applications, processes, startup programs, and services on managed devices on your network. Inventory is collected by the KACE Agent, which is installed on managed devices, uploaded using the inventory API, or obtained through connections to Agentless devices. You can view detailed data about individual managed devices, as well as aggregated data collected across all managed devices. In addition, you can use inventory information in reports, and in decisions about upgrades, troubleshooting, purchasing, policies, and so on. See Provisioning the KACE Agent.

IP Scans

See Discovery .

K

KACE GO

KACE GO is an app that enables administrators to access Service Desk tickets, inventory information, monitoring alerts, and application deployment features from their smart phones or tablets. The app also allows non-admin users to submit Service Desk tickets, view the status of submitted tickets, and read Knowledge Base articles from their mobile devices. You can download KACE GO from the Apple App Store for iOS devices, or from the Google Play Store for Android devices. See Configuring Mobile Device Access.

KACE SDA series appliances

The K2000 series includes system deployment appliances designed to fully automate the deployment of operating systems (OS). For more information about the KACE SDA series, go to the Quest website, https://quest.com/products/kace-systems-deployment-appliance/.

appliance series appliances

The appliance series includes system management appliances designed to fully automate system management tasks such as system management, application deployment, and asset management. For more information about the appliance series, go to the Quest website, https://quest.com/products/kace-systems-management-appliance/.

Knowledge Base

Quest has a Knowledge Base of articles about the appliance, which you can access at https://support.quest.com/kace-systems-management-appliance/kb. The Knowledge Base is continually updated with solutions to real-world issues that administrators encounter.

Konductor

Konductor is an internal appliance component that regulates communications between the appliance and managed devices to keep the system running smoothly. The number of tasks Konductor is running appears on the *Tasks in Progress* widget. In addition, task throughput information appears in the General Settings (on appliances with the Organization component enabled) or in the Agent Settings (on appliances without the Organization component enabled).

See:

- About Dashboard widgets
- Configuring System-level and Admin-level General Settings

KScripts

See Offline KScripts , and Online KScripts .

L

labels

Labels are containers that organize and categorize items, such as devices, so that you can manage them as a group. For example, you can use labels to identify devices that have the same operating system or that are in the same geographic location. You can then initiate actions, such as distributing software or deploying patches, on all of the devices that in that label. Labels can either be manually assigned to specific items or automatically assigned to items when they are associated with criteria, such as SQL or LDAP queries. See Setting up and using labels to manage groups of items.

label groups

Label groups enable you to organize labels so you can manage them as a group. Label groups share their types with the labels they contain. Not only can a label group include multiple labels, but a label can be associated with more than one label group. See Add, view, or edit label groups.

LDAP Browser

The LDAP Browser is a wizard that enables you to browse and search data located on an LDAP server, such as an Active Directory server. See Use the LDAP Browser.

LDAP Labels

LDAP labels are labels that interact with the Active Directory or LDAP (Lightweight Directory Access Protocol) server. You can use LDAP Labels to automatically label device records and user records based on LDAP or Active Directory queries or search filters. LDAP Labels are applied to devices that match the search criteria. See Managing LDAP Labels.

linking

See appliance linking .

Localization component

A appliance component that enables you to choose the language to use for the **Command Line Console**, **Administrator Console**, and **User Console**. See Configuring locale settings.

Locally Cataloged applications

Applications that are not in the official version of the Software Catalog, but that have been added to the local version on the appliance, are referred to as Locally Cataloged applications. Locally Cataloged applications can be metered, marked as Not Allowed, and associated with License assets. See About Locally Cataloged applications.

Log Enablement Package

Log Enablement Packages (LEPs) enable performance threshold monitoring and monitoring for applications such as Exchange, Internet Information Services (IIS), and so on, for servers. In the *Log Enablement Packages* list page, Quest publishes a base set of Windows Reliability and Performance Monitor (PerfMon) templates and non-Windows open-source Perl scripts, so that users can extend their monitoring capability and identify system and application performance issues. Monitoring on the appliance works without these additional templates and scripts, but the profiles that are created from the templates and scripts are helpful if users want to do performance threshold monitoring. See Configuring application and threshold monitoring with Log Enablement Packages.

logs

See Search the scripting logs.

M

machines

See devices .

Managed Computers

Your product license agreement entitles you to manage a specified number of devices that are categorized as Managed Computers. Managed Computers are devices in appliance inventory that: 1) have Windows, Mac, Linux, or UNIX operating systems, 2) are categorized as PCs or servers, and 3) were not added to inventory manually, through the WSAPI, or through mobile device management. See View product licensing information.

Managed Installations

Managed Installations (MI) are the primary mechanism for deploying or removing applications from appliance managed devices. Each Managed Installation describes a specific application title and version to be installed or removed, including installation commands, installation files, and target devices (by label). Managed Installations always take place at the same time that managed devices upload inventory data to the appliance. In this way, the appliance confirms that the installation is actually needed before it performs the installation. Installation packages can be configured to run silently or with user interaction. Managed Installations can include installation, uninstallation, and command-line parameters. See Using Managed Installations.

manual labels

See labels .

metering

Software metering enables you to collect information about how applications are installed and used on the Windows and Mac devices that you manage. This includes Windows Store applications, such as Bing Travel. Metering is not available for applications installed other operating systems, such as Linux. In the Software Catalog, metering can be enabled for applications that are listed as Discovered and Not Discovered and for applications that are Locally Cataloged. Metering cannot be enabled for operating system software, applications installed on unsupported operating systems, such as Linux, or for applications that are listed as Uncataloged in the Software Catalog. See About software metering.

MIA

Missing in action. Devices that are being managed by the appliance, but that have not been inventoried on schedule are referred to as MIA devices. See Managing MIA devices.

Mobile Device Access

Mobile Device Access enables you to interact with the appliance using KACE GO.

KACE GO is an app that enables administrators to access Service Desk tickets, inventory information, and application deployment features from their smart phones or tablets. The app also allows non-admin users to submit Service Desk tickets, view the status of submitted tickets, and read Knowledge Base articles from their mobile devices. You can download KACE GO from the Apple App Store for iOS devices, or from the Google Play Store for Android devices.

See Configuring Mobile Device Access.

Monitored Computers

Your product license agreement entitles you to manage a specified number of devices that are categorized as Monitored Computers. Monitored Computers are servers that 1) meet the requirements for Managed Computers and 2) have Monitoring enabled. You can monitor 5 servers with your appliance license. If you want to be able to monitor up to 200 servers, you must obtain a license for the Monitoring Module. See View product licensing information and Managing monitoring for devices.

MSI Installer template

This template enables you to create a script that sets the basic command line arguments for running MSI-based installers. For command-line options, go to the Microsoft MSI Command-Line documentation at http://msdn.microsoft.com. See .

N

nodes

See devices .

non-computer devices

Non-computer devices are assets such as printers, routers, network gear, and other devices that do not meet the definition of Computers. Administrators can create Asset Subtypes to track information related to specific non-computer devices. See About Asset Subtypes, custom fields, and device detail preferences.

Not Allowed applications

Not Allowed applications are applications that have been marked as Not Allowed on the *Software Catalog* page. Windows and Mac applications can be marked as Not Allowed only if they are classified as Discovered, Not Discovered, or Locally Cataloged applications. Applications that are Uncataloged cannot be marked as Not Allowed until they are added to the Software Catalog. Applications that are marked as Not Allowed can be blocked from running on managed devices if those devices have an Application Control-enabled label applied to them. See Using Application Control.

Not Discovered applications

Applications that do not exist in the inventory, but that do exist in the Quest KACE Software Catalog, are referred to as Not Discovered applications. You can enable metering for Not Discovered applications, mark them as Not Allowed, and add license information for them. However, because the applications have not been found in the local appliance inventory, the Not Discovered software list cannot be exported in CSV format. Compare to Discovered applications . See Not Discovered applications.

notifications

Notifications are email messages the appliance sends to administrators when devices, scan results, and assets meet specified criteria. For example, if you want to notify administrators when devices approach disk space limits, you can set up alerts based on disk usage. Notifications are sent when devices meet the specified criteria.

The appliance checks inventory against the criteria in the notification schedules at the specified frequency. When an item meets the criteria, the appliance sends email to the specified recipients.

Messages that are sent through email based on selected criteria and at scheduled intervals. See Scheduling notifications.

O

Offline KScripts

Scripts that run at a scheduled time, based on the target device's clock. Offline KScripts can run even when target devices are not connected to the appliance, such as when devices start up or when users log in. You can create these scripts using the scripting templates. See Adding and editing scripts.

Online KScripts

Scripts that run only when a target device is connected to the appliance. Online KScripts run at scheduled times based on the appliance clock. You can create these scripts using the scripting templates. See Adding and editing scripts.

Online shell scripts

Scripts that run at scheduled times based on the appliance clock, but that run only when the target device is connected to the appliance. Online shell scripts are created using simple text-based scripts, such as Bash, Perl, batch, and so on, that are supported by the target device's operating system. Batch files are supported on Windows, along with the different shell script formats supported by the specific operating system of the target devices. See Adding and editing scripts.

Organization component

An appliance component that enables you to create and manage organizations within the appliance. This makes it possible to assign devices to separate organizations and to create User Roles within each organization to control administrator and user access. For example, you can configure organizations so that administrators can only view and perform actions on devices in their organization; they cannot view devices that belong to other organizations.

See Creating and managing organizations.

organization filters

Organization filters are similar to labels, but they serve a specific purpose: Organization filters automatically assign devices to organizations when devices are inventoried.

There are two types of organization filters:

- **Data Filter**: Assigns devices to organizations automatically, based on search criteria. When devices are inventoried, they are assigned to the organization if they meet the criteria. This filter is similar to Smart Labels in that it assigns devices to organizations automatically if they match specified criteria.
- **LDAP Filter**: Assigns devices to organizations automatically based on LDAP or Active Directory interaction. When devices are inventoried, the query runs against the LDAP server. If devices meet the criteria, they are automatically assigned to the organization.

  See Managing organization filters.

organizations

Organizations are logical instances of an appliance that run on a single appliance. You can create organizations if the Organization component is enabled on your appliance, each organization is supported by its own database, and you manage each organization's inventory and other components separately. See Creating and managing organizations.

P

patching

Patching is a mechanism for deploying security-related and other important patches from Microsoft, Apple, and other third-party vendors such as Adobe. This includes patches for operating systems as well as applications. When deploying patches in a production environment, you can select which operating systems you want to patch and define schedules for patching by using labels. See About patch management.

provisioning schedules

Provisioning schedules specify how and when to install the KACE Agent on devices you want to manage using Agent software. See Managing provisioning schedules.

provisioning

The process of installing the KACE Agent on managed devices. See Provisioning the KACE Agent.

R

Replication Shares

Replication Shares are devices that keep copies of files for distribution, and they are especially useful if your managed devices are deployed across multiple geographic locations. For example, using a Replication Share, a device in New York could download files from another device at the same office, rather than downloading those files from an appliance in Los Angeles. A Replication Share is a full replication of all digital assets and is managed automatically by the appliance. Whenever a Replication Share is specified for a label, devices in that label go to the Replication Share to get files. See Using Replication Shares.

reporting

The ability to gather information about hardware, software, and license compliance on a per-device basis. You can run standard reports, or create custom reports using a step-by-step report wizard. In addition, you can schedule reports to run and be delivered through email. Advanced users can also write reports against the appliance database using any ODBC (Open DataBase Connectivity) -compliant reporting engine. See Using reports and scheduling notifications.

resources

Items such as scripts, reports, Managed Installations, and software that can be imported or exported among organizations and appliances. See Importing and exporting appliance resources.

role

The permissions related to user accounts and organizations. See:

- Managing System-level user accounts
- Managing organization user accounts
- Managing Organization Roles and User Roles
- Create and assign monitoring-specific roles

S

SAM

SAM is short for Software Asset Management, a method of managing applications in inventory. See Managing Software Catalog inventory.

Samba share

The built-in file sharing system on the appliance. See Enable file sharing at the System level.

scripting

The ability to create and run a set of actions on managed devices. Scripts can be designed to do many different things, from installing or removing applications to verifying and changing settings, such as firewall settings, on managed devices. Scripts are deployed and run based on labels and schedules that you define, operating independently of the inventory process that is central to Managed Installations. See Adding and editing scripts.

scripts

See Offline KScripts , Online KScripts , and Online shell scripts .

Server monitoring

The appliance offers a module with which to perform basic performance monitoring for servers in inventory. The monitoring feature targets server-class operating systems, and provides default monitoring profiles that define criteria for performance alerts for each operating system. You can define additional, custom profiles that point to alternative event logs or OS level logs, with similar or different criteria.

Service Desk

Service Desk is the default name for the end-user trouble-ticket tracking system that is part of the appliance **User Console**. The Service Desk enables end users to submit trouble tickets through email or through the **User Console**, `http://<appliance_hostname>/user`, where `<appliance_hostname>` is the hostname of your appliance. Your help desk team manages these tickets through email, the **Administrator Console**, `http://<appliance_hostname>/admin`, or the KACE GO app. You can customize the categories and fields associated with tickets as needed. See About Service Desk.

Share With Quest

The options for sharing appliance information with Quest. See Configure data sharing preferences.

single sign on for appliances

See appliance linking .

single sign on for the Administrator Console and User Console

Single sign on enables users who are logged on to the domain to access the appliance **Administrator Console** and **User Console** without having to re-enter their credentials on the appliance login page. See About single sign on (SSO).

Smart Labels

Smart Labels are labels that are applied and removed automatically based on criteria you specify. For example, to track laptops in a specific office, you could create a label called “San Francisco Office,” and create a Smart Label based on the IP address range or subnet for devices located in the San Francisco office. Whenever a device that falls within the IP address range is inventoried, the Smart Label “San Francisco” is automatically applied. When the device leaves the IP address range, and is inventoried again, the label is automatically removed.

Smart Labels are applied to and removed from managed devices when the appliance processes device inventory. So if you create a Smart Label that enables metering on devices, it might take time for the Smart Label to be applied to devices and for devices to report metering information. Metering is enabled for devices that match the Smart Label criteria only after devices are inventoried and the Smart Label is applied.

See Managing Smart Labels.

Software Catalog

The Software Catalog is a database that contains standardized information about more than 57,000 Windows and Mac applications and software suites. Information in the catalog includes the name,

version, publisher, and category of each application or suite as well as the operating system on which the application or suite runs. See Managing Software Catalog inventory.

software category

Software categories classify software as belonging to a specified group, such as software drivers or security applications. For applications listed on the Software page, categories are assigned manually. For applications listed on the Software Catalog page, software categories are assigned to applications automatically. See Using software threat levels and categories.

T

tether

The connection to **Quest Support**. The tether enables Quest representatives to connect to your system for troubleshooting. See Enable a tether to Quest KACE Support.

task throughput

The task load on the appliance. See Konductor .

third-party applications

Applications created by third-parties and licensed for use in Quest KACE products.

threat levels

Threat levels can be used to indicate the relative safety of items and the number of devices on which those items are located. This information is for tracking purposes only. The appliance does not enforce policies based on threat levels. See Using software threat levels and categories.

U

Uncataloged applications

Uncataloged applications are executables that are in the inventory but that do not appear in the Software Catalog. You can view applications that are listed as Uncataloged on the *Software Catalog* page. However, you cannot enable metering for Uncataloged applications, mark them as Not Allowed, or add license information for them. Uncataloged applications must be added to the local or public Software Catalog before they can be metered, marked as Not Allowed, or associated with license information. See Uncataloged applications.

User Console

The **User Console** is the web-based interface that makes software, scripts, and other downloadable items available to users on a self-service basis. It also enables users to access Knowledge Base articles and to file Service Desk support tickets to request help or report issues. To access the **User Console**, go to `http://<appliance_hostname>/user` where `<appliance_hostname>` is the hostname of your appliance. See About Service Desk.

User Downloads

User Downloads are software installation packages, such as printer drivers and other applications, that are distributed to users through the **User Console**. See Managing User Downloads.

V

virtual appliance

See appliance or virtual appliance .

W

Wake-on-LAN

Wake-on-LAN enables you to power-on devices remotely from the appliance regardless of whether the devices have the KACE Agent installed. See Using Wake-on-LAN.

About us

Quest Software creates technology and solutions that build the foundation for enterprise AI. Focused on data management and governance, cybersecurity and platform modernization, Quest helps organizations address their most pressing challenges and make the promise of AI a reality. Around the globe, more than 45,000 companies including over 90% of the Fortune 500 count on Quest Software. For more information, visit www.quest.com or follow Quest Software on X (formerly Twitter) and LinkedIn.

Technical support resources

Technical support is available to Quest customers with a valid maintenance contract and customers who have trial versions. You can access the Quest Support Portal at https://support.quest.com.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to-videos
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product.

Legal notices

© 2025 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.

Patents

Quest Software is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at 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.

Legend

CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

IMPORTANT, NOTE, TIP, MOBILE, or VIDEO: An information icon indicates supporting information.

KACE Systems Management Appliance Administrator Guide

Updated - December 2025

Software Version - 15.0

Index

Numerics

2FA, configuring 92
2FA, configuring for organizations 295
2FA, enabling for the appliance 100

A

Acceptable Use Policy 120
action buttons on User Console 779
Active Directory
  single sign on access with 180
  single sign on configuration 110, 178
adding 494
  announcements to User Console 781
  applications to Software page inventory 468, 539
  applications to the Software Catalog 486
  Asset Types 213
  Contracts 235, 236
  Custom Views 63
  devices to inventory manually 439
  File Synchronization 554
  LDAP Labels 153
  License assets for Software Catalog inventory 248, 489
  License assets for Software page inventory 252
  Licenses 238, 239
  Locations 231, 232
  Managed Installations 539
  manual labels 136
  notification schedules 719
  Purchases 242, 243
  scripts 565
  Service Desk ticket queues 842
  Smart Labels 139
  Software assets in Assets section 470
  Software assets in Inventory section 470
adding Agent tokens 396
Admin level 28
  Dashboard 40
  General Settings 72
administration
  backing up data 878
  Daily Run Output 897
  email notifications for administrators 159
  logs, downloading 896
  logs, viewing 893
  restarting the appliance 888
  restoring appliance settings 883
  restoring factory settings 886
  restoring most recent backup 883
  troubleshooting 893
  updating appliance software 886
  updating the license key 888
Administrator Console 28, 28
  about 27
  components
    with the Organization component 36
    without the Organization component 32
  locale settings for 78, 83
Advanced Search
  and Custom Views 63
  for organizations 300
  for Software page inventory 474
Advanced Search{Filter}
  and Smart Labels 63
Agent
  about 27, 186, 398
  add Windows registry key for access to DDP|E information 388
  communication settings for 410
  deploying manually 186, 418
  enabling file sharing for 399
  enabling organization-level file sharing for 400, 400
  features available to managed devices 342
  GPO Provisioning Tool for Windows 401
  history 186, 398
  installing on multiple devices 404
  Konea 415
  log settings for 410
  messages, deleting 416
  messages, viewing 415
  methods for provisioning 186, 398
  obtaining installation files 419
  preparing to install with onboard provisioning 403
  provisioning 399, 400, 400, 401
  provisioning results 409
  provisioning schedules
    deleting 408
    duplicating 407
    editing 407
    running 407
    viewing 407
  provisioning using Discovery results 340
  quarantined
    approve 397
    block 397
    delete 397
    review 397
  registering with the appliance 395
  starting and stopping on Linux 424
  starting and stopping on Mac OS X 427
  system requirements for installation 403
  task status 414
  tokens
    adding 396

editing 396
updates 416, 416
configuring automatic 416
uploading manually 417
Agent debugging 897
Agent deploy
Linux devices 423
startup/login 423
updating 424
verifying the version 424
viewing the version on Linux 425
Linux devices, removing 424
Mac OS X devices
deploy/upgrade 425
remove 427
using shell scripts 426
using terminal window 426
verify 427
verifying the version 428
Windows devices 419
Agent Provisioning Assistant
provision Windows devices with GPO Provisioning Tool 402
using to deploy Agent on devices 404
Agentless management 429
add Windows registry key for access to DDP|E information 390
delete device details 436
device details 436
enable manually 431
enable using Discovery information 430
features available to managed devices 342
supported operating systems 429
alerts 560
automatic deletion of 737
automatic dismissal of 737
creating for broadcast 560
creating Service Desk tickets from 744, 802
deleting 753
dismissing 752
filter unwanted 748, 748, 749, 750
for device configuration changes 738
Konea connection required for 560
retrieve dismissed 753
searching for 748
stopping for maintenance 738
allow access to hosts 99
alternate download locations
about 538
distributing packages from 538
for scripts 563
Android 121
announcements
adding and editing on User Console home page 781
prioritizing on User Console home page 782
Apache
graphs 893
log paths 732
webserver diagnostic graphs 100
API
access to the appliance 100
Apple iOS 121
appliance
configuration
session timeout 114
SSL certificate 113
configuring network settings 69
domain access 95
hardware specifications 69
Inventory Dashboard widgets 203
labels 59
license information 722
local routing tables 98
NTP service, verifying status of 94
patch download settings 599
port settings 93
security settings 100
software updates 59
software version 56
task schedules 56
Windows Feature Update download settings 599
appliance backups 881, 881
about 878
daily backup schedule 879
deleting 881
downloading files 880
FTP access to 881
manual 880
status of 891
appliance linking
about 125
adding names and keys 126
disabling 128, 128
enabling 126, 126
enabling access to Federation API settings 127, 127
appliance network interface status 890
appliance resources
about importing and exporting 302
exporting from appliance 302
exporting from organizations 304
importing to appliances 303
importing to organizations 304
appliance settings
advertised updates 886
general 72
license key updates 888
manual updates 887
restore to factory settings 886
restoring 883
restoring from backup 883, 885
security 100
uploading backup files 884
verify updates 888
appliance up-time and load averages 890
appliance version 56
application classifications 476

Application Control
applying labels for 505
editions sharing executables 505
limitations of 505
marking as Not Allowed 505
messages that appear 505
removing designation 507
reporting on 506
requirements 504
using 504
viewing Not Allowed applications 506
application patches, viewing 602
applications
cataloged 476
finding using Advanced Search 474
Locally Cataloged 477
Not Allowed 477
viewing Discovered 480
viewing Locally Cataloged applications 482
viewing Not Discovered 480
viewing Uncataloged applications 481
APPROVAL_INFO field 874
approvals, requiring for tickets 873
approving tickets by email 874
archival
deleting tickets from 840
enabling for tickets 837
restoring tickets from 840
ticket queue settings for 839
Asset Management
about 202, 218
adding and deleting asset fields 212
adding barcodes 209
adding Software assets 470
asset administrator role 231
Asset Subtypes 218, 219
adding 219
deleting 225
editing 222
setting as default 222
Asset Types
about 212
adding 213
adding custom fields for devices 216
adding fields for locations 217
customizing 213
deleting 218
parent relationships for locations 217
renaming 212
assigning assets to subtypes 223, 224
classic metering 494
comparing assets to inventory 207
contracts
about 235
Contracts
adding 235, 236
customizing 236
editing 235
data format 257
device assets
archiving 230
identifying assets to track 208
importing license data 257
about 256
preparation 257
License Asset Type, customizing 247
License Compliance 261
customizing the warning threshold 264
setting up 245
viewing configuration information 265
licenses
about 238
Licenses
adding 238, 239
customizing 239
editing 238
locations
about 231
Locations
adding 231, 232
customizing 232
editing 231
maintaining assets manually 231
managing 261
physical assets
about 228
adding 228
purchases
about 242
Purchases
adding 242, 243
customizing 243
editing 242
relationships between asset fields 216
reporting on assets 231
searching for assets 208, 210
Software assets 225, 225
adding from Assets section 226
adding from Inventory section 226
customizing Asset Types 225
software metering
about 494
about enabling 495
configuring options 499
device selection for 495
disabling 502
disabling for devices with manual labels 502
disabling for devices with Smart Labels 502
enabling for applications 498
enabling for devices with Smart Labels 497
enabling with manual device labels 496
information collected 494
scheduling inventory collection intervals 503
scripts that collect informaiton 495
software suites 495
viewing device details 501

viewing metering details 500, 500
updating assets manually 224
viewing asset lifecycle settings 211
viewing Asset Subtypes on the Assets page 223
viewing assets 208, 210
viewing available Asset Subtypes 223
workflow for SNMP devices 219
Asset Management Dashboard
about 203
customizing 205
Asset Management Dashboard, Administrator Console 203
assigning user roles 269
attachments to tickets 787, 815
authentication
Google Workspace credentials 194
managing credentials 190
Office 365 credentials 199
SNMP credentials 197
viewing credential usage 200
authentication and user accounts 157
authentication credentials for Chrome 324
auto-refresh settings 114

B

backup files
downloading 880
restoring 885
uploading 884
backups
about 878
configure offboard transfer 882, 882
deleting backup data 881
disabling 881
enabling 881
manual 880
scheduling and retention of 879
settings for backups 100
bandwidth for Replication Shares 187
best practices for patching 593
blocking applications
about 504
applying Application Control labels 505
limitations of 505
marking as Not Allowed 505
messages that appear 505
removing designation from apps 507
reporting on 506
requirements 504
viewing Not Allowed apps 506
broadcasting alerts 560, 560
Business Hours for Service Desk 758
buying licenses 58

C

Cataloged applications 476
cataloging requests
canceling 488
how custom names are resolved 487
submitting 487
certificate, for SSL 100
certification, DIACAP 120
change history
deleting 133
for assets 130
for objects 131
for settings 129
organization-level settings history 129, 129
viewing, searching, and exporting 132, 132, 133
changing custom ticket fields using email 808
changing ticket approval fields by email 808
changing ticket fields using email 807
checking patch details for a device 629
child tickets, creating for any ticket 871
Chrome
authentication credentials 324
Discovery Schedule for device 327
classic metering 494
clearing ticket fields using email 807
Client Drop File Size Filter 83
Client Drop Location
copying files to 472
filter settings for organizations 289
Client ID
used in Chrome authentication credentials 324
Client Secret
used in Chrome authentication credentials 324
code attributions 56
Command Line Console
about 27
accessing 71
command-line deployment
Mac OS X Agent 426
Windows Agent 419, 420
commands that must be run as root 425
Comment Field Options 862
comments 815
comments, adding to tickets 813
compliance
DIACAP 120
for software licensing 245
components
enabled on the appliance 58
overview of 27
computers
searching for in inventory 392
conditional rules
writing in Custom Inventory 519
configuration
allow access to hosts 99
API Access for the appliance
disabling for the appliance 121
date and time 89
General Settings, Admin level 78
local routing tables 98
local web server 99
locale settings 115
Mobile Device Access 121
disabling for the appliance 124
disabling for users 124
enabling for the appliance 122

enabling for users 122
network settings 95
POP3 email accounts 272
security settings 100
Service Desk
import tickets from another system 755
Service Desk setup tasks 755
Service Desk ticket settings 772
session timeout 114, 114
SSL certificate 113
theme settings 118
default appliance theme 118
default user theme 118
user notifications 90, 91
with the Organization component 72
without the Organization component 83
configuring 882
configuring 2FA 92
conflict warning dialog
enabling and disabling 770
creating
POP3 email accounts 272
tickets by email 806
creating a custom ticket layout 864
creating a ticket template 865, 866
credentials
adding Google Workspace 194
adding LDAP User/Password 193
adding Office 365 199
adding Secret Key 191
adding SNMP 197
adding User/Password 192
creating reports of 201
deleting 202
exporting 201
identifying the use of 200
managing 190
CSV format for License data 257
custom data fields
adding 349
custom fields
for Asset Subtypes 218
Custom Inventory rules
about 516
checking for conditions 519
creating 516
defining rule arguments 530
getting values from a device 525
how implemented 517
regular expressions for matching filenames 528, 530
syntax 518
testing 534
types 516
custom ticket fields
changing through email 808
defining 862
custom ticket layouts 859, 864, 865, 866
custom Ticket Rules
creating 833
deleting 836
duplicating 835
Custom Views
creating from Advanced Search criteria 63
for Service Desk tickets 812
CustomerResponded Ticket Rule 833
customize ticket detail 862, 869
customizing
Asset Types 213
Contracts 236
Licenses 239
Locations 232
Purchases 243
ticket details 772
User Console action buttons and widgets 779
User Console logo 775, 777
User Console welcome message 775, 777

D

daily run output 889
Dashboard
about 40
Admin level 40
customizing 51
System level 41
data retention settings 78, 83
data sharing preferences 119
database access to reports 100
database tables
Organization-level 901
System-level 901
date and time settings 89
debugging Agent software 897
default organization, about 286
default queue 844
default roles 266
default theme settings 118
default ticket
categories, status, and priorities 772
setting a view as the default 813
views, using 810
DefaultTicketOwners
email notifications for 270

deleting
Agent messages from command queue 416
alerts 753
alerts automatically 737
appliance backup data 881
Asset Subtypes 225
Asset Types 218
credentials 202
Discovery schedules 342
label groups 152
LDAP Labels 155
manual labels 138
MIA devices 464
notification schedules 720
organization filters 300
organizations 296
provisioning schedules 408
Service Desk ticket queues 843
Smart Labels 150
Software page inventory 470
user downloads 851
Dell
device warranty information 466
obtaining warranty information 466
renewing warranties 467
warranty reports 467
Dell Command | Monitor
information on Device Detail page 353
Dell Data Protection | Encryption
enabling inventory collection on Agentless-managed Windows clients 390
enabling inventory collection on Agent-managed Windows clients 388
information viewed in device details 382
inventory collection on Windows clients 388
Dell Updates
configuring Dell Updates 642
configuring schedules 649
patching, compared 641
viewing available updates 651
viewing schedules 648
viewing update details 652
Dell Updates, viewing 651
denying access to applications
editions sharing executables 505
dependencies, for scripts 563
deployment status, of device patches 629
deployments
compared with updates 641
detection, inventory term used instead 641
Detect-only patch schedules
error codes 615
device
add monitoring profile to 733
adding manually using Administrator Console 440
adding manually using API 444
alert on configuration change 738
apply SNMP configuration to 439
detail page for organizations 301
Discovery Schedule for Chrome 327
Discovery Schedule for ESXi hosts or vCenter Servers 332
Discovery Schedule for Hyper-V or SCVMM devices 334
Discovery Schedule for KACE Cloud Mobile Device Manager 325
Discovery Schedule for SNMP-enabled 336
Discovery Schedule for Workspace ONE 330
enabling monitoring for 723, 723, 724
finding in inventory 392
patching status for one 624
reassigning to organizations 301
running Device Actions 394
SCVMM credentials 336
SCVMM devices 336
viewing DDP|E information 382, 388
viewing status 892
Device Actions 78, 83
running 394
running from Ticket Detail page 817
device issues
identifying 892
device management 342, 348, 440
DIACAP compliance 120, 120
Diagnostic Utilities 892, 892
digital assets for distribution 537
digital assets, attaching to applications 471
disabling 881
Acceptable Use Policy 120
API Access for the appliance
for the appliance 121
appliance linking 128
Mobile Device Access
for the appliance 124
for users 124
secure attachments for tickets 787
Service Desk satisfaction survey 786
single sign on 177, 180
SSH for the appliance 100
Discovery 311
about 311
adding schedules for Chrome devices 327
adding schedules for ESXi hosts or vCenter Servers 332
adding schedules for Hyper-V or SCVMM devices 334
adding schedules for KACE Cloud Mobile Device Manager devices 325
adding schedules for non-computer devices 336
adding schedules for quick scans 312
adding schedules for thorough scans 320
adding schedules for Workspace ONE devices 330
Agentless management

enable 430
delete schedules 342
Nmap 319
results 340
results and Agent provisioning 340
SCVMM credentials 336
stop a running schedule 341
using Smart Labels with 145
viewing and searching results 340
disk status 889
dismissing alerts automatically 737
distributing
software 535
distribution packages
about 537
about attaching digital assets 537
for Mac OS X 538
inventory requirement for 537
using alternate download locations 538, 538
DMM
device detail 353
DNS Service Discovery (DNS-SD) requests 100
documentation
for MySQL 668
searching the appliance Help system 64
domains
joining the appliance server to 110, 178
unjoining appliance server from 180
domains that must be accessible for patching 596
download locations, alternate 538, 538
downloading
appliance backup files 880
KACE GO 123
patches 599
Windows Feature Updates 599
duplicating
Agent provisioning schedules 407
organization roles 288
reports 711
scripts 576
Service Desk ticket queues 843
Smart Labels 141

E

editing
Contracts 235
Licenses 238
Locations 231
Purchases 242
editing Agent tokens 396
email
approving tickets using 874
authentication using POP3 272
automatically adding addresses to tickets 283
changing approval fields using 808
changing custom ticket fields 808
changing ticket fields using 807, 807
clear text using POP3 272
clearing ticket fields using 807
configuring external SMTP email servers 876
configuring internal SMTP servers 876
configuring secure SMTP email servers 876
customizing email templates 276
event triggers 274
modifying ticket attributes using 807
notifications for Service Desk 271, 271, 765
notifications, recommended 275
open ticket notification 275
POP3 server, using 272
preferences 273
Service Desk exclusions for 284
setting an approval field value using 808
testing and troubleshooting 897
testing incoming email 898
testing outgoing email 898
ticket closure notification 275
email floods
Service Desk prevention of 284
email notifications for administrators 159
Email on Events, configuring 275
email system health 890
EmailOnClose Ticket Rule 833
enabling 881
2FA for the appliance 100
Acceptable Use Policy 120
appliance linking 126
fast switching for organizations 124
file sharing
organization-level 400, 400
System level 399
without the Organization component 400
file sharing for Windows devices 403
LDAP Labels 155
Mobile Device Access
enabling for users 122
for the appliance 122
for users 122
parent-child ticket relationships 870
secure attachments for tickets 787
single sign on 177
SSH for the appliance 100
switching between organizations 124
tether to Quest 892
ticket creation by email 806
enabling access to Federation API settings
appliance linking 127
encryption
device detail 353
error codes
patches 615
scripts 615

error logs
for email 899, 900
escalating tickets 819, 820, 821
time limit 820
examples
importing asset license data 257
Managed Installation, EXE 544
Managed Installation, MSI 544
Managed Installation, TAR.GZ 550
Perl script for inventory uploads 445
XML schema for Windows devices 448
exporting
credentials 201
Managed Installations 560
resources from appliances 302
resources from organizations 304

F

factory settings, restoring 886
fast switching, enabling for organizations 124
file sharing
enabling at the System level 399
with the Organization component 400
File Synchronization
creating 554
File Synchronizations
about 537
files supported by Managed Installations 539
files, attaching to tickets 815
filters
about Data Filters 136
adding Data Filters 297
data and LDAP, for organizations 296
devices by organization 392
redirecting devices to organizations 301
Firefox settings for single sign on 180
Fixed Ticket Fields 860
FTP
access to appliance backups 881
security settings for 100

G

General Settings 72
Google Play 121
Google Workspace credentials, adding and editing 194
GPO Provisioning Tool
deploy Agents with 401, 402
preparing system to use 401

H

hardware specifications for appliance 69
Help Desk 754
Help system and PDF 64
history settings
about 128
and the Organization component 129
asset subscriptions 130
assets, viewing 131
object subscriptions 131
objects, viewing 132
subscriptions for organizations 129, 129
viewing 130
Holidays for Service Desk 759
Home page, Administrator Console 40
Hours of Operation for Service Desk 758

I

identifying credential use 200
identifying device issues 892
importing
appliance resources, about 302
License asset data 257
resources to appliances 303
resources to organizations 304
users from LDAP servers 170
inactive patches 631
increasing license capacity 58
install Agent using provisioning schedule 404
installation files for Agent 419
installer files
identify parameters supported by 540
Intel AMT
information displayed in Device Details 391
Inventory
adding
devices manually using API 444
devices manually, about 439
devices manually, Administrator Console 440
Software assets 470
software manually 468
change history 349, 440
custom fields, adding 349
data collection schedule 350
delete devices 395
Dell warranty information 466
device detail 352, 353, 353, 382
device notifications 392
devices, searching for 392
force update 452
appliance 453
Linux devices 454
Mac OS X devices 453
Windows devices 453
labels for devices 393
managing devices 342, 440
manual inventory information 452
metering schedules for 503
MIA devices
applying labels to 464
configuring 463
deleting 464
overview 348
Processes
about 509

adding labels for 509
applying and removing labels for 510
assigning threat levels to 510
categorizing 510
deleting 511
viewing and editing 509
running Device Actions 394
searching for devices 392
Services
about 513
adding labels for 514
applying and removing labels 514
assigning threat levels to 515
categorizing 515
deleting 515
viewing and editing 513
Smart Labels for 393
software
adding labels for 474
applying and removing labels 474
categories 473
deleting 470
digital assets 471
Smart Labels 474
threat level 473
Software Catalog
adding labels for 474
applying and removing labels 474
Software page
about 467
viewing items on 468
startup programs
about 511
adding labels for 512
applying and removing labels 512
assigning threat levels for 513
categorizing 512
deleting 513
viewing and editing 511
submitting information using API 445
troubleshooting MIA devices 464
upload XML 452
view devices 395
Inventory Dashboard
about 306
customizing 308
Inventory Dashboard, Administrator Console 306
inventory, detection term used instead 641
iOS 121
IP scan
about 311
overview 311

K

KACE Agent
access through Mac menu bar 428
access through Windows system tray 422
provisioning with GPO Tool 401, 402
system requirements for installation 403
updating automatically 416
updating manually 417
KACE Cloud Mobile Device Manager
Discovery Schedule for device 325
KACE GO 121
about 27
downloading 123
enabling Mobile Device Access 122
KBSYS database table 901
Knowledge Base
about 851
links to articles in User Console 780
KScripts
about 562
default 564
obtaining dependencies 563
token replacement variables for 566

L

label groups
about 136
adding and editing 151
assigning labels to 152
deleting 152
removing labels from 152
labels
about 59, 135
adding and editing label groups 151
adding and editing LDAP Labels 153
adding and editing manual labels 136
adding Smart Labels 139
assigning to label groups 152
deleting 138
deleting LDAP 155
editing Smart Labels 141
enabling LDAP Labels 155
for application control 505
for Service Desk staff 270
label groups, about 136
LDAP Labels, about 135
manual 393
organization filters 136
searching with LDAP Browser 155
Service Desk All Ticket Owners 142
Smart Labels, about 135
viewing manual label details 138
laptops, critical patches for 605
Layout Ticket fields 860
LDAP Browser 155
LDAP Labels 135
about 59
adding and editing 153
deleting 155
enabling 155
searching with LDAP Browser 155
variables used in 926
LDAP server authentication 167
LDAP server user import 170
LDAP User/Password credentials
adding and editing 193
LEP Installation Log
viewing 734

License assets
adding for Software Catalog 248, 489
adding for Software page inventory 252
managing for Software Catalog 489
License Compliance
about 246
reclaiming unused software licenses 263
setting up 248, 489
updating 264
viewing compliance information 261
license expiration 56
license information 58
license key
monitoring counting toward limit 722
obtain for expanded server monitoring 724
updating appliance with expanded monitoring 725
license usage warning threshold 264
linking KACE SMAs
about 125
adding names and keys 126
disabling 128
enabling 126
enabling access to Federation API settings 127
links on User Console home page 783
Linux
SELinux and server monitoring 721
starting and stopping the Agent on 424
Linux package upgrades
about 652
configuring schedules 653, 656
viewing history 658
viewing schedules 652
local authentication for the appliance 157
local web server 99
locale settings 78, 83, 116
about 115
configuring Administrator Console 115
configuring Command Line Console 115
configuring User Console 116
for organizations 117
for users 117
Locally Cataloged applications
about 477
change to cataloged 486
viewing 482
log date format
nonstandard in monitoring 733
Log Enablement Package
editing on Windows Server 2008 or higher device 734
for application and threshold monitoring 733
installing 734
LEP Installation Log 734
log paths
Apache 732
MySQL 732
logging in 67
login credentials, managing 190
login requirements, for organizations 72
logos 72, 78, 83, 296, 775, 777
logs
daily run output 897
downloading for the appliance 896
for email errors 900
for patching 631
for Scripting 579
viewing for the appliance 893

M

Mac devices
manage KACE Agent 428
Mac OS X
distribution 538
manual deployment of Agents on 425
patching 632
starting and stopping Agents on 427
Machine Actions (see Device Actions) 78
macOS X
Managed Installations for 551
maintenance windows
scheduling for alert cessation 738
Malware scanning
manage 659
Managed Installations
about 537, 539
about creating 539
adding for Software Catalog 494
creating for Windows 540
EXE example 544
exporting 560
installer file parameters 540
macOS X platform 551
MSI example 544
parameters for 540
RPM example 545
TAR.GZ example 550
ZIP example 545
managing credentials 190
managing devices 342, 348, 440
managing processes inventory 509
managing service inventory 513
managing startup program inventory 511
manual appliance backups 880
manual deployment of Agents
Command line for Windows 420
installation wizard for Windows 419
Linux devices 423, 423
remove 424
logon script 186, 418
Mac OS X installer 425
Mac OS X terminal window 426
using email 186, 418
viewing the version 425
Windows devices 419
manual labels 136
merge
enabling for tickets 818

metering
about enabling 495
data retention settings for 78
enabling for applications 498
enabling for devices with manual labels 496
enabling for devices with Smart Labels 497
scheduling inventory collection 503
MIA devices
about 463
configuring settings 463
Microsoft Edge
single sign on settings for 180
migrating software License assets 493
missing patches 630
Mobile Device Access
about 121
disabling for the appliance 121, 124
disabling for users 124
downloading KACE GO 123
enabling for the appliance 122
enabling for users 122
model number of appliance 56
monitoring
about server 721
add profile to device 733
create user role for 739
creating a new profile 730
creating Service Desk tickets from alerts 744, 802
disable 742
disabling on a device 742
download profile 732
edit a Windows Log Enablement Package 734
edit profile 726, 748, 748, 750
SNMP traps 728
enabling on a device 742
enabling on eligible device 723, 723, 724
filter unwanted alerts 748, 748, 750
nonstandard log date format 733
pausing for a device 736
pausing for multiple devices 736
resuming for multiple devices 736
return default profile to factory settings 726
upload profile 732
working with profile 725
moving resources to network locations 305
multicast Domain Name System (mDNS) requests 100
MySQL
documentation link 665, 668
log paths 732
reporting password for 72

N

network settings 69
Network Utilities 892
new patches
using Smart Labels to view 143
New Ticket
customize 869
Nmap discovery
considerations 319
non-computer devices
adding Asset Subtypes for 219
assigning devices to Asset Subtypes 223, 224
viewing available Asset Subtypes of 223
Not Allowed applications
about 477
Application Control 505
removing designation from apps 507
viewing 506
notification schedules
adding from list pages 719
adding from Reporting section 717
deleting 720
editing 719
notifications
about 660
for administrators 159
server monitoring alerts 743
NTLMv2 400
NTP service
requirement for patching 595
verifying status of 94

O

object identifiers (OIDs)
obtained with appliance 437
used in inventory 437, 438
objects, configuring history subscriptions for 131
offboard backup transfer 882, 882
Office 365 credentials, adding and editing 199
offline KScripts
about 562
obtaining dependencies 563
OID
obtained with appliance 437
used in inventory 437, 438
online KScripts
about 562
default 564
obtaining dependencies 563
token replacement variables for 566
online shell scripts
about 562, 567
operating systems
supported by Agentless management 429
ORG database tables 901
Organization component 28, 286
appliance General Settings for 72
fast switching between organizations 72
organization filters
about 136
Data Filters 136
LDAP Filters 136
organization mode 28

organizations
about 286
about filtering devices 296
adding and editing 289
adding Data Filters 297
adding LDAP Filters 298
Advanced Search for devices 300
configuring 2FA 295
customizing logos for 296
default organization 286
deleting 296
deleting filters 300
Device Details page 301
filtering devices 300
locale settings for 117
managing 286
redirecting devices 301
require selection at login 72
roles, about 286
roles, adding and editing 287
roles, deleting 289
roles, duplicating 288
switching between 124
testing filters 299
user accounts for 296
OverdueClose Ticket Rule 833
owner-only comments for tickets 814

P

packages, for Patch Management 591
parameters for Managed Installations 540
parent tickets
adding existing tickets to 872
enabling parents to close child tickets 871
using as to-do lists 872
passwords, managing 191, 192, 193
Patch Management 591
about 589
about critical patches for laptops 605
about packages 591
about signature files 591
about subscriptions 595
assessment testing 591
best practices 593
configuring schedules 606, 614, 619, 622
Dell Updates, compared 641
Dell Updates, scheduling 642, 644
deployment testing 591
details by device 629
Detect-only schedules
error codes 615
download options 591
download settings for 599
download status 602
for Mac OS X devices 632
gather information about managed devices 596
marking patches as inactive 631
patch catalog 626
Quest Software Inc. 592
reports for 624
resetting patch deploy attempts 629, 629
rollback 625
Rollback options for patches 625
schedule field descriptions 606
scheduling non-critical patching 605
Smart Labels for critical OS patches 143
Smart Labels for desktops 146
Smart Labels for laptops 149
Smart Labels for new patches 144
Smart Labels for servers 148
speeding up with Replication Shares 593
subscribing to patches 597
testing environment 591
undo the last patch deployment 625
using Replication Shares for 187
using Smart Labels with 143
view missing patches 630
viewing available patches 602
viewing downloaded patches 626
viewing files within patches 624
viewing logs 631
viewing patch details 628
viewing patch status 624
viewing patch status for devices 624
viewing schedules 616
viewing statistics 631
warning users first, importance of 593
websites that must be accessible 596
workflow for critical OS patches 605
workflow for desktops and servers 605
workflow for first-time patching 596
workflow for patching 589
patches 591
error codes 615
PDF of Help system 64
Perl script
sample 445
permissions for Service Desk staff role 267
ping probe
disable 737
POP server settings 95
POP3 email accounts
DefaultTicketOwners@mydomain.com 272
supprt@mydomain.com 272
POP3 email server 272
port 443 100
port 80 100
port settings for the appliance
firewall exceptions for the appliance 93
preferences for data sharing 119
Preview ticket layout 869
Primary Keys for imported license data 257

printer
apply SNMP configuration to 439
Processes
adding labels for 509
applying and removing labels for 510
assigning threat levels to 510
categorizing 510
deleting 511
inventory, about 509
viewing details of 509
profiles
about 725
default monitoring 725
edit 748, 748, 750
monitoring
about 725
add to a device 733
create new 730, 732
download 732
edit 726, 728
edit a Windows Log Enablement Package 734
SNMP traps 728
upload 732
provisioning
schedules for Agent 407
viewing results 409
proxy server settings 95

Q

quarantined Agents
approve 397
block 397
delete 397
review 397
Quest Software Inc. 592
queues
about 841
adding 842
bulk edit tickets 847
configuring 761
configuring response templates 771
customizing ticket details for 772
default fields for All Queues list 845
deleting 843
enabling conflict warnings 770
moving tickets between 847
setting system default 844
setting user default 845
transferring Ticket Rules between 836
quick scans, for Discovery 312

R

RAID drive status 891
rebooting the appliance 888
redirecting devices 301
reinstalling the Software Catalog 508
Related Ticket Fields 860
removing
Agents from Linux devices 424
Agents from Mac OS X devices 427
Application Control designation 507
labels from label groups 152
renaming Service Desk 769
ReopenTicket Ticket Rule 833
Replication Shares
about 186, 538
adding 187
for locale patches 187
viewing details of 190
weekly schedules of 187
reports
about 660
adding schedules 715
creating and running 661
creating by entering SQL 665
creating from list pages 668
creating using report wizard 661
custom logos for 72, 713
deleting custom reports 713
deleting notification schedules 720
deleting schedules 717
Dell warranty 467
duplicating existing 711
editing 712
editing SQL statements 712
enabling database access to 100
for a single organization 714
for blocked applications 506
for credentials 201
for multiple organizations 714
for Service Desk 837
layout 713
notification schedules 717
patching-related 624
running 660, 713
requesting Local Cataloging for applications 487
required fields setting on Service Desk tickets 860
requiring ticket approvals 873
resetting patch deploy attempts
from patch Catalog page 629
from Patch Detail page 629
resources
about transferring 302
deleting status of exports 305
exporting from appliance 302
exporting from organizations 304
importing to appliances 303
importing to organizations 304
moving from local to network locations 305
viewing exported or imported 305
viewing status of exports 305
response templates
configuring 771
restoring appliance settings 883
retention of data 78

roles
about 266
adding and editing for organizations 287
adding and editing, user 160
assigning user roles 269
default 287
for Organizations 286
for Service Desk staff 267
monitoring-specific 739
root commands 425
rules
Custom Inventory 516, 516, 525
for Service Desk tickets 832
Run Now command
about 576
monitoring status of 578
using to run scripts 577
run order
of organization filters 297
of Smart Labels 150
running Device Actions 817
running reports 660

S

Samba share
Admin-level settings for organizations 78
Admin-level settings without organizations 83
and Client Drop Location for organizations 289
appliance settings 100
transferring resources between appliances 302
SAML
single sign on configuration 181
using AD in Azure as IdP 182
satisfaction survey
modifying the label for 786
preventing distribution of 786
using 785
scheduled task status 629
scheduling
daily backups 879
Dell Update deployment 649
Dell Updates 644
Discovery scans 312
inventory collection for Software Catalog 503
inventory collection, devices 350
LDAP user imports 170
Linux package upgrade 653
Linux package upgrades 656
metering for Software Catalog applications 503
patch deployment 606, 614, 619, 622
reports 715
Wake-on-LAN requests 558
Windows Feature Update deployment 633, 637
screen shots, attaching to tickets 815
Scripting
edit policies and scripts 579
Run Now status 578
searching logs 579
scripts
adding 567
adding steps to 917
default 564
deleting 574, 575
duplicating 576
editing 574
error codes 615
exporting 580
importing 575, 576
Kscripts 567
log files for 579
obtaining dependencies 563
online shell scripts 567
reusing 576
run from Script Detail page 577
run from Scripts page 577
Run Now 576, 577
tasks you can automate 562
token replacement variables for 566
workflow 565
search
Admin level 60
advanced
notifications 62
Smart Labels 62
documentation 64
online Help 64
page level 60, 61
searching for devices in Inventory 392
Secret Key credentials
adding and editing 191
security
for Service Desk attachments 787
settings for the appliance 100
SSL certificates 113
Security Dashboard
about 584
customizing 586
Security Dashboard widgets 584
Dell Updates 584
Overall Compliance By Machine 584
Overall Compliance By Patch 584
Patch Installation Progress 584
Patches Deployed 584
Patches Failed 584
Patches Released 584
Patching Tasks Completed 584
Reports 584
Views 584
Windows 10 Releases 584
Security Dashboard, Administrator Console 584
SELinux
server monitoring with 721
serial number of appliance 56

server monitoring
about 721
application 733
dismissing alerts 752
enable 742
enabling on device 723, 723, 724
filter alerts 748, 748, 749, 750
number of servers that can be monitored 721
obtaining license key for expanded 724
pause monitoring 736, 736
resume monitoring 736
searching for alerts 748
threshold 733
updating license key to increase limit 725
working with alerts 743
working with profile 725
Server-Enhanced Linux
effect on server monitoring 721
Service Desk 815
child tickets 870, 870
configuring
email exclusions 284
email settings 283
external SMTP email servers 876
internal SMTP email servers 876
terms used for tickets 769
title of Service Desk 769
widget data cache 285
creating child tickets 871
customizing
ticket categories 772
ticket fields 862
ticket impacts 772, 859
ticket layout 864
ticket layouts 772, 859
ticket priorities 772, 858
ticket settings 854
ticket statuses 772, 857
default user roles for 266
designating parent tickets 872
editing 822
email
configuring settings 271, 765
connecting servers to the appliance 874
error logs 899
errors 900
event triggers 274
notification strategy 271
preferences 273
testing incoming email 898
testing outgoing email 898
troubleshooting 897
troubleshooting incoming email 898
troubleshooting outgoing email 898
email testing
using Telnet 898
import tickets from another system 755
Knowledge Base
adding articles 852
attachments, adding 852
deleting articles 853
external inks for 852
user ratings and views 854
using markdown 852
labels and roles for staff members 270
managing
ticket templates 865, 866
organizing duplicate tickets 873
overview 754
parent tickets as to-do lists 872
parent tickets, enabling 870
parent-child tickets 870, 871
preventing
unnecessary email traffic 284
processes
adding 822
converting to regular tickets 831
deleting 831
types 828
using 822, 829, 829, 830, 830
queues
about 841
adding 842
bulk edit tickets 847
configuring 761
configuring response templates 771
default fields for All Queues 845
deleting 843
duplicating 843
enabling conflict warnings 770
moving tickets between 847
setting system default 844
setting user default 845
viewing tickets in all queues 844
running reports 837
Satisfaction Survey 785
securing attachments 100, 787
setup tasks for 755
staff role 267
system requirements for 754
ticket approvers, configuring 874
ticket approvers, using 873
tickets
categories and subcategories, creating 855
converting to process tickets 832
lifecycle of 792
links in User Console 784
owner-only comments 814
quick-action links on User Console 785
viewing in queues 843
Service Desk Dashboard
about 787
customizing 789
Service Desk Dashboard, Administrator Console 787
service inventory, managing 513
session timeout
about 72, 83, 114
extending 785
losing unsaved changes 785
resetting 72, 83, 114
Setting
Home Dashboard 52
setting up License Compliance 248, 489
setting up the appliance server 69

settings
history 128, 129
locale 78, 83
POP server 95
User Console 72
sharing data 119
shell scripts 567
shell support
SSH 436
shut down the appliance 888
signature files, for patching 591
single sign on
about 176
access with Active Directory 180
Active Directory method 110, 178
disabling 177, 180
enabling 177
SAML method 181
using AD in Azure as IdP 182
using Active Directory for 177
web browser settings
Firefox 180
Microsoft Edge 180
size restrictions for attachments to tickets 805
SLA
configuring 759
configuring Business Hours 758
enabling 759
Holidays for Service Desk 759
Smart Labels 135
adding 139
assigning the run order of 150
combining 140
deleting 150
editing 141
for critical OS patches 143
for desktops 146
for device inventory 393
for Discovery Results 145
for laptops 149
for new patches 144
for patching 143
for servers 148
for Service Desk 142
managing 139
SMTP server
connecting to appliance 874
using instead of POP3 272
verify settings of 891
SNMP
adding and editing credentials 197
Discovery Schedule for device 336
enabling for the appliance 100
full walk 336
Inventory Configurations 437, 437, 438, 439
printer templates 439
software
deploying from User Console 848
removing User Downloads 851
Smart Labels 474
Software assets 225, 470
adding from Assets section 226, 470
adding from inventory 226
customizing 225
for License Compliance 470
Software Catalog 478
about 475
about cataloged applications 476
about data collection 477
about Not Allowed applications 477
adding applications 486
and Application Control 505
application categories 477
canceling cataloging requests 488
change Locally Cataloged to Cataloged 486
classifications 476
configuring metering options for 499
custom names 487
data sharing for 478
feature comparison with Software page 478
for organizations 477
License Compliance for 246
license information 248, 489
localization of 477
Locally Cataloged applications 477, 482
Managed Installations 494
migrate License assets 493
reclaiming unused software licenses 263
removing local cataloging 488
scheduling inventory collection 503
scheduling metering 503
Smart Label restrictions for 139
software licenses for 489
submitting cataloging requests 486, 487
updating and reinstalling 508
updating License Compliance for 264
viewing Discovered applications 480
viewing License Compliance for 261
viewing Not Allowed applications 506
viewing Not Discovered applications 480
viewing software details 483
viewing Uncataloged 481
Software distribution
about 535
adding applications for 539
testing 536
software License Compliance
about 246
reclaiming unused software licenses 263
updating 264
viewing 261
software metering
about 494
configuring options 499
disabling for devices with manual labels 502
disabling for devices with Smart Labels 502
disabling for Software Catalog apps 502
enabling for applications 498
enabling for devices with Smart Labels 497
enabling with manual device labels 496
viewing device details 501
viewing metering details 500, 500

Software page
feature comparison with Software Catalog 478
license information 252
software version, of appliance 56
special characters
escaping in monitoring profiles 750
specifications, for the appliance 69
speeding up patching with Replication Shares 593
SQL queries
and Smart Labels 141
database table names for 901
documentation 668
for reports 665
SSH, enabling for the appliance 100
SSL certificate wizard 113
SSL certificates, uploading 100
SSLv3 (legacy version of SSL) 100
SSO 176
staff role, creating 267
starting and stopping the Agent on Linux 424
starting and stopping the Agent on Mac 427
startup program inventory
adding labels for 512
applying and removing labels 512
assigning threat levels for 513
categorizing 512
deleting 513
managing 511
viewing and editing 511
status of patch downloads 602
status of RAID drives 891
steps for Task sections of scripts 917
submitting cataloging requests 486, 487
subscribing to patches 595, 597
subscribing to Windows Feature Updates 632
subtypes for assets
about 218
adding 219
assigning or changing 223, 224
deleting 225
editing 222
setting as default 222
viewing available subtypes 223
viewing on the Assets page 223
workflow for SNMP devices 219
synchronizing files 554
syntax
Custom Inventory rules 518
for changing custom ticket fields using email 808
for clearing ticket fields using email 807
for task sections of scripts 917
System Administration Console 28
System level 28, 72
Dashboard 41
user accounts 157
with the Organization component 38
system requirements
for Agent installation 403
for Service Desk 754
for the appliance 69

T

task chains
add 581
edit 581
Task Chains
about 580
task schedules
about 56
technical specifications, appliance 27
technical support tether 892
Telnet, using to test incoming email 898
templates
for Service Desk email 276
terminal window interface 71
testing
assement, for Patch Management 591
Custom Inventory rules 534
deployment, for Patch Management 591
incoming email 898
LDAP Labels 153
LDAP server configuration 167
organization filters 299
tether to Quest 892
theme settings
default appliance theme 118
default user theme 118
third-party code attributions 56
threat levels 473
Ticket Detail
customize 862, 869
Ticket Rules 832
creating 833
customizing system rules 833
defaults for system rules 833
deleting 836
duplicating 835
moving between queues 836
transferring between queues 836
using system rules 833
tickets
about custom layouts 859
approval fields you can change by email 808
approvals, configuring 874
approvals, requiring 873
approving by email 874
archival
about 837
deleting tickets from 840
enabling 837
of selected tickets 840
queue settings for 839

restoring tickets from 840
attachment size restrictions 805
attachments to 815
attachments, adding 815
categories and subcategories, creating 855
categories, CC List values for 283
change field order 864
changing approval fields through email 808
changing custom fields through email 808
changing fields through email 807
clearing fields using email 807
closure notification 275
comments, adding 813
comments, viewing 815
configuring settings for 772
create by email 806
creating
from server monitoring alerts 744, 802
from the Administrator Console 794
from the Asset Detail page 801
from the Device Detail page 800
from the User Console 793
creating statuses for 772
custom fields you can change using email 808
custom fields, defining 862
custom layouts for 864
Custom Views for 812
customizing
impact values 859
priority values 858
status values 857
ticket settings 854
default status of 772
default views, using 810
deleting from queues 841
deletion settings for 841
due dates and SLAs 758, 759, 759
duplicates, organizing 873
enabling creation by email 806
escalation 819
about 820
email message for 821
email recipients 821
time limit, about 820
time limit, changing 821
escalation notification 275
fields you can change by email 807
history, viewing 817
import from another system 755
lifecycle of 792
links on User Console home page 784
merge
enabling 818
merging 818
from the Ticket Details page 819
from the Tickets list page 819
modifying by email 807
navigating among related items 809
opening notification 275
owner-only comments, adding 814
parent-child relationships, enabling 870
parent-child relationships, using 870
parents
using as to-do lists 872
using to organize duplicates 873
quick-action links on User Console 785
screen shots, adding 815
sending information by email 817
setting fields to Required on form 860
setting the default view for 813
SLA settings for 759
states 820
templates for 865, 866
work information for 809
time and date settings 89
time limit on open inactive user sessions 72, 83, 114
timeout period for user sessions 785
timing of email from Service Desk 274
token replacement
for Service Desk email 276
variables for scripts 566
transferring resources between appliances 302
troubleshooting 892, 893
Agent provisioning to Windows devices 897
Agent software 897
appliance issues 893
email communications 897
Wake-on-LAN requests 559
types
Service Desk processes 828

U

unjoin domain 180
unpacking the appliance 69
updates
checking for appliance updates 886
compared with deployments 641
Dell Updates and patching 641
viewing KACE Agent updates 416
updating
appliance Agents automatically 416
appliance software 59
KACE Agents automatically 416
KACE Agents on Linux, manual 424
KACE Agents on Mac OS X, manual 425
Software Catalog 508
software License Compliance 264
the appliance license key 888
uploading
appliance backup files 884
SSL certificates for the appliance 100
uploading files to the appliance server 472
usage data sharing 119

user accounts 167
assigning roles to 269
authentication with LDAP 167
DefaultTicketOwners 270
editing profiles 165
labels for 142
LDAP authentication 167
LDAP import, manual 170
LDAP import, scheduled 172
organization-level 157
adding 161
editing 161
managing 160, 296
Organization-level
adding 164
archiving 164, 164
editing 164
Service Desk All Ticket Owners label for 142
System-level 157
adding 157
deleting 160
editing 157
managing 157
time limit on sessions 72, 83, 114
viewing profiles 165
user authentication 167
LDAP 167
LDAP configuration 167
local accounts on the server 157
single sign on using LDAP 176
User Console
about 27
action buttons and widgets 779
adding announcements on home page 781
adding ticket links to home page 784
creating tickets from 793
custom links on home page 783
customizing 775, 777
distribution packages 537
links to KB articles from home page 780
locale settings for 78, 83
logo 777
prioritizing announcements on home page 782
quick-action ticket links on home page 785
settings 72
welcome message 777
User Downloads
about 848
applying labels to 851
creating packages for 848
removing labels from 851
removing packages 851
user notification settings 90, 91
user notifications 90, 90, 91
user roles
adding 160
assigning 269
deleting 161
editing 160
user sessions
reviewing 184, 185
locations 184
User/Password credentials
adding and editing 192

V

variables
for Service Desk email 276
used in LDAP Labels 926
used in scripts 566
verify the Agent is running on Linux 424
verify the Agent is running on Mac 427
version of appliance software 56
version of the Agent on Linux devices 425
version of the Agent on Mac devices 428
viewing history
Linux package upgrade 658
viewing Linux package upgrade schedules 652
viewing patch schedules 616
viewing Windows Feature Update schedules 637, 648

W

WaitingOverdue Ticket Rule 833
Wake-on-LAN
about 557
issuing requests 557
scheduling requests 558
troubleshooting 559
warning threshold for software licenses 264
warranty information for Dell devices 466
websites that must be accessible to the appliance 95
welcome message, user console 775
widget data cache
Service Desk configuration of 285
widgets
Assets by Location 203
Assets By Status 203
Assets By Type 203
Cost ($) of Unused Licenses By Product 203
Expired Contracts 203
Expired Software License Maintenance 203
Expiring Contracts 203
Expiring Software License Maintenance 203
for User Console 779
Home Dashboard widgets 42, 42
Active Tickets 42
Active Tickets By Category 42
Active Tickets By Owner 42
Active Tickets By Priority 42
Assets by Location 42
Assets By Status 42
Assets By Type 42
Average Ticket Resolution Time 42
Closed Tickets 42
Connections 42
Cost of Unused Licenses By Product 42
Critical Patch Compliance 42
Current Scripts 42
Dell Updates 42
Device Check-In Rate 42
Devices by Disk Capacity 42
Devices By Manufacturer 42, 42
Devices By Memory 42

Devices By Model 42, 42
Devices By Processor 42
Devices By Subtype 42
Disk Capacity 42
Expired Contracts 42
Expired Software License Maintenance 42
Expiring Contracts 42
Expiring Dell Warranties 42
Expiring Software License Maintenance 42
File Synchronizations 42
Latest News Articles 42
License Compliance 42
Managed Installations 42
Managed Operating Systems 42, 42
Monitored Devices 42
Monitoring Alert Summary 42
Monitoring Alerts 42
Overall Compliance By Machine 42
Overall Compliance By Patch 42
Overdue Tickets 42
Overdue Tickets By Owner 42
Overdue Tickets Count 42
Patch Installation Progress 42
Patch Tasks Completed 42
Patches Deployed 42
Patches Failed 42
Patches Released 42
Provision Platforms 42
Provisioning 42
Reopened Tickets 42
Reports 42
Shortcuts 42
Software Installed But Not Used in 60 Days 42
Software License Configuration 42
Software Publishers 42
Software Titles 42
Tasks in Progress 42
Tickets Due Today 42, 42
Tickets Opened Today 42
Tickets Today 42
Top Knowledge Base Articles 42
Views 42
VMware Device Counts 42
VMware Device Reports 42
VMware ESXi Device By Status 42
VMware ESXi Version Counts 42
Windows 10 Releases 42
Inventory Dashboard widgets 306
Agent Version Counts 306
Connections 306
Device Check-In Rate 306
Device Reports 306
Devices By Disk Capacity 306
Devices By Manufacturer 306
Devices By Memory 306
Devices By Model 306
Devices By Processor 306
Devices By Subtype 306
Inventory Counts 306
Managed Operating Systems 306
Provision Platforms 306
Provisioning 306
Shortcuts 306
VMware Device Counts 306
VMware Device Reports 306
VMware ESXi Device By Status 306
VMware ESXi Version Counts 306
License Compliance 203
Security Dashboard widgets 584
Critical Patch Compliance 584
Service Desk Dashboard widgets 787
Active Tickets 787
Active Tickets By Category 787
Active Tickets By Owner 787
Active Tickets By Priority 787
Average Ticket Resolution Time 787
Closed Tickets 787
Overdue Tickets By Owner 787
Overdue Tickets Count 787
Overdue Tickets Today 787
Reopened Tickets 787
Reports 787
Shortcuts 787
Tickets Due Today 787, 787
Tickets Opened Today 787
Tickets Overdue 787
Views 787
Software Installed But Not Used in 60 Days 203
Software License Configuration 203
Software Publishers 203
Software Titles 203
Windows
manage KACE Agent 422
manual deployment of KACE Agent 419, 420
Windows Feature Updates
about 632
configuring schedules 633, 637
download settings for 599
subscribing to updates 632
viewing available updates 640
viewing schedules 637
viewing update details 641
Windows Feature Updates, viewing 640
Windows Group Policy
using to deploy Agent with provisioning tool 401, 402
wizards
for Agent provisioning 404
for generating SSL certificates 113
for reporting 661
for Smart Labels 141
work information for Service Desk tickets 809
workflow
for Asset Subtypes and SNMP 219
for patch subscription 596
for patching 589
for using ticket approvers 873
Workspace ONE
Discovery Schedule for device 330
workstations, patching workflow for 605

X

XML editor, for scripts 574

XML schema
Linux and Mac 451
Windows 447