



KACE® Systems Management Appliance (K1000) 7.1

Administrator Guide



Table of Contents

About the KACE Systems Management Appliance (K1000).....	26
About K1000 components.....	26
About the Administrator Console.....	28
Components available in Admin mode without the Organization component.....	31
Components available in Admin mode with the Organization component enabled.....	33
Components available in System mode with the Organization component enabled.....	35
Using the Home component.....	36
About Dashboards.....	36
View the Dashboard in Admin mode.....	37
View the Dashboard in System mode.....	37
Customize Dashboard pages.....	38
About Dashboard widgets.....	38
View Dashboard details.....	43
View the K1000 version, model, and license information.....	45
View K1000 license information.....	46
About appliance software updates.....	47
About labels.....	47
Searching for information and filtering lists.....	48
Search at the Admin level.....	48
Search at the page level.....	48
Searching at the page level with advanced options.....	49
Create Custom Views using Advanced Search criteria.....	51
Access product documentation.....	52
Log in to the Administrator Console: First login following initial network configuration.....	54
Getting started.....	57
Configuring the appliance.....	57
Requirements and specifications.....	57
Power-on the appliance and log in to the Administrator Console.....	57
Access the Command Line Console.....	59
Tracking configuration changes.....	60
Configuring System-level and Admin-level General Settings.....	60
Configure appliance General Settings with the Organization component enabled.....	60
Configure Admin-level or organization-specific General Settings.....	66
Configure appliance General Settings without the Organization component.....	70
Configure appliance date and time settings.....	77
Verifying port settings, NTP service, and website access.....	77

Verify port settings.....	78
Verifying the status of the NTP service.....	79
Make necessary websites accessible to the K1000 appliance.....	79
Configuring network and security settings.....	80
Changing appliance network settings.....	80
Configure local routing tables.....	83
Configure local web server settings and whitelist hosts.....	83
Configure security settings for the appliance.....	85
Configure Active Directory as the single sign on method.....	91
Configure Quest Identity Broker as the single sign on method.....	93
Generate an SSL certificate.....	94
Configuring Agent settings.....	95
About Konea.....	95
Configure Agent settings.....	96
Configuring session timeout and auto-refresh settings.....	98
Set session timeout.....	98
Set auto-refresh properties.....	98
Configuring locale settings.....	99
How locale settings are applied.....	99
Configure locale settings for the Administrator Console and the Command Line	
Console.....	99
Configure locale settings for the User Console.....	100
Configure locale settings for organizations.....	101
Configure locale settings for users.....	102
Configure data sharing preferences.....	102
About DIACAP compliance requirements.....	103
Enable or disable the Acceptable Use Policy.....	103
Configuring Mobile Device Access.....	104
Enable Mobile Device Access for the appliance.....	105
Enable Mobile Device Access for users.....	105
Download and use KACE GO.....	106
Disable Mobile Device Access on the appliance.....	107
Disable Mobile Device Access for users.....	107
Enable fast switching for organizations and linked appliances.....	107
Linking Quest KACE appliances.....	108
Enable appliance linking.....	109
Add Names and Keys to appliances.....	109
Enable access to Federation API settings.....	110
Disable appliance linking.....	111

Configuring history settings.....	111
About history settings.....	111
Managing settings history.....	112
Managing asset history.....	113
Managing object history.....	114
Using change history information.....	115
Setting up and using labels to manage groups of items.....	116
About labels.....	116
About Smart Labels.....	116
About LDAP Labels.....	117
About label groups.....	117
About organization filters.....	117
Tracking changes to label settings.....	118
Managing manual labels.....	118
Add or edit manual labels.....	118
View manual label details.....	119
Delete manual labels.....	120
Managing Smart Labels.....	120
Add Smart Labels.....	120
Example: Combine Smart Labels to identify devices.....	121
Edit Smart Labels.....	123
Setting up labels for user accounts.....	123
Using Smart Labels for patching.....	124
Using Smart Labels with Discovery Results.....	126
Adding Smart Labels for devices.....	127
Assign the Smart Label run order.....	131
Delete Smart Labels.....	131
Managing label groups.....	132
Add, view, or edit label groups.....	132
Assign labels to or remove labels from label groups.....	133
Delete label groups.....	133
Managing LDAP Labels.....	134
Add or edit LDAP Labels.....	134
Enable LDAP Labels.....	136
Delete LDAP Labels.....	137
Use the LDAP Browser.....	137
Configuring user accounts, LDAP authentication, and SSO.....	139
About user accounts and user authentication.....	139

About locale settings.....	139
Managing System-level user accounts.....	140
Add or edit System-level user accounts.....	140
Manage appliance administrator email notifications.....	142
Delete System-level user accounts.....	143
Managing organization user accounts.....	143
Add or edit User Roles.....	143
Delete User Roles.....	144
Add or edit organization user accounts.....	144
Customize user details.....	147
View or edit user profiles.....	147
Using an LDAP server for user authentication.....	149
About the login account on your LDAP server.....	149
Configure and test LDAP user authentication.....	150
Importing users from an LDAP server.....	152
Import user information manually.....	152
Import user information according to a schedule.....	156
About single sign on (SSO).....	159
Using external LDAP or Active Directory servers for single sign on.....	160
About Quest Identity Broker.....	160
Enabling and disabling single sign on.....	160
Enable single sign on.....	161
Disable single sign on.....	161
Using Active Directory for single sign on.....	161
Configure Active Directory as the single sign on method.....	162
Configuring browser settings for single sign on.....	163
Unjoin the domain and disable Active Directory single sign on.....	164
Using Quest Identity Broker for single sign on.....	165
Configure Quest Identity Broker as the single sign on method.....	165
Manage Quest Identity Broker user approval requests.....	166
Use single sign on through Quest Identity Broker.....	168
Using Replication Shares.....	168
Create Replication Shares.....	169
View Replication Share details.....	172
Managing credentials.....	172
Tracking changes to Credentials Management settings.....	173
Add and edit User/Password credentials.....	173
Add and edit Google OAuth credentials.....	174

Add and edit SNMP credentials.....	176
View credential usage.....	178
Create reports from the Credentials Management list.....	178
Export credentials information.....	179
Delete credentials.....	179
Configuring assets.....	179
About the Asset Management component.....	179
About managing assets.....	180
How asset information differs from inventory information.....	180
Identifying the assets to track.....	181
View assets and search for asset information.....	181
Add barcodes to assets.....	182
Change device owners.....	183
Adding and customizing Asset Types and maintaining asset information.....	183
About Asset Types.....	184
Customizing Asset Types.....	184
About Asset Subtypes, custom fields, and device detail preferences.....	190
Managing Software assets.....	197
Customize the Software Asset Type.....	197
Adding Software assets.....	197
Managing physical and logical assets.....	199
Add physical Asset Types.....	199
Archive device Assets.....	200
Maintaining and using manual asset information.....	201
Managing locations.....	202
Manage locations.....	202
Add or edit locations.....	203
Customize location fields.....	203
Setting up License Compliance.....	206
About License Compliance for Software Catalog applications.....	206
About license upgrades.....	206
About license downgrades.....	207
Customize the License Asset Type.....	207
Add License assets for Software Catalog inventory.....	208
Add License assets for Software page inventory.....	212
Importing license data in CSV files.....	215
How asset information is handled during import.....	216
Importing asset data using CSV files.....	216

Managing License Compliance.....	218
View License Compliance information for Software Catalog applications.....	218
Update software License Compliance information manually.....	221
Customize license usage warning thresholds.....	221
View License Compliance and Configuration information.....	222
Setting up Service Desk.....	223
Setting up roles for user accounts.....	223
About default roles.....	223
Create a Service Desk staff role.....	224
Assign user roles.....	226
Apply labels and roles to Service Desk staff.....	227
Create the DefaultTicketOwners account.....	227
Configuring email settings.....	228
About email notifications.....	229
About Ticket Rules.....	229
About POP3 email accounts.....	229
Create and configure POP3 email accounts.....	230
Configuring email triggers and email templates.....	232
Configure CC lists for ticket categories.....	240
Automatically add email addresses to ticket CC List fields.....	241
Exclude addresses from ticket CC List fields.....	241
Prevent email loops.....	242
Creating and managing organizations.....	243
About organizations.....	243
About the Default organization.....	243
Tracking changes to organization settings.....	244
Managing Organization Roles and User Roles.....	244
Available default roles.....	244
Add or edit Organization Roles.....	245
Duplicate Organization Roles.....	246
Delete roles.....	247
Adding, editing, and deleting organizations.....	247
Add or edit organizations.....	247
Delete organizations.....	253
Customizing the logos used for the User Console and organization reports.....	253
Managing user accounts for organizations.....	253
Managing organization filters.....	253
How organization filters work.....	254

Add or edit organization Data Filters.....	254
Add or edit organization LDAP Filters.....	255
Test organization filters.....	257
Delete organization filters.....	257
Managing devices within organizations.....	258
Using Advanced Search.....	258
Filter devices.....	258
Redirect devices.....	258
Understanding device details.....	259
Running single organization and consolidated reports.....	259
Importing and exporting appliance resources.....	259
About importing and exporting resources.....	259
Transferring resources among appliances using Samba share directories.....	260
Export resources from an appliance.....	260
Import resources to an appliance.....	260
Transferring resources among organizations.....	261
Export resources from organizations.....	261
Import resources to organizations.....	262
Managing exported resources at the System level.....	262
View or delete shared resources.....	262
Move shared resources from the local K1000 to network locations.....	262
View or delete the status of resource exports.....	263
Managing inventory.....	264
Using Device Discovery.....	264
About Device Discovery and device management.....	264
Tracking changes to Discovery settings.....	264
Discovering devices on your network.....	264
Add a Discovery Schedule to perform a quick "what and where" scan of your network.....	265
Add a Discovery Schedule for a thorough scan of managed Windows, Mac, Linux, and UNIX computers.....	274
Obtain a Client ID and Client Secret for use in discovering Chrome devices.....	277
Add a Discovery Schedule for a G Suite device.....	278
Add a Discovery Schedule for a Dell Mobility Management (DMM) device.....	280
Add a Discovery Schedule for SNMP-enabled non-computer devices.....	281
Add a Discovery Schedule for an AirWatch device.....	283
About Discovery Results.....	285
View and search Discovery Results.....	285
Provision the Agent using the discovered IP address or hostname.....	286

Stop a running discovery scan.....	286
Delete Discovery Schedules.....	287
Managing device inventory.....	287
About managing devices.....	287
Features available for each device management method.....	288
About inventory information.....	300
Tracking changes to inventory settings.....	301
Managing inventory information.....	301
Add custom data fields.....	301
Schedule inventory data collection for managed devices.....	302
View device inventory and details.....	304
Groups and sections of items in device details.....	305
About Dell Data Protection Encryption (DDP E) and encryption information in device details.....	324
Add a Dump Inventory registry key to permit inventory collection on Windows DDP E client devices.....	330
About Intel AMT information in device details.....	334
Finding and managing devices.....	335
Finding devices in inventory.....	335
Labeling devices to group them.....	336
Run actions on devices.....	337
View devices that have been added manually.....	337
Delete devices from inventory.....	338
Provisioning the K1000 Agent.....	338
Enabling file sharing.....	339
Provisioning the K1000 Agent using the GPO Provisioning Tool for Windows devices.....	341
Provisioning the K1000 Agent using onboard provisioning.....	343
Managing provisioning schedules.....	346
Managing Agent communications.....	349
Updating the K1000 Agent on managed devices.....	354
Manually deploying the K1000 Agent.....	357
Obtaining Agent installation files.....	357
Manually deploying the K1000 Agent on Windows devices.....	357
Manually deploying and upgrading the K1000 Agent on Linux devices.....	359
Performing Agent operations on Linux devices.....	360
Manually deploying and upgrading the K1000 Agent on Mac devices.....	361
Performing other Agent operations on Mac devices.....	363
Viewing information collected by the Agent.....	364

Using Agentless management.....	364
About Agentless device management.....	364
Managing Agentless devices.....	365
Using SNMP Inventory Configurations to identify specific SNMP objects and non-computer devices to add to inventory.....	372
Adding devices manually in the Administrator Console or by using the API.....	375
About managing devices.....	375
Tracking changes to inventory settings.....	375
Add devices manually with the Administrator Console.....	376
Adding devices manually using the API.....	380
Forcing inventory updates.....	388
Force inventory updates from the appliance.....	389
Force inventory updates from Windows devices.....	389
Force inventory updates from Mac OS X devices.....	389
Force inventory updates from Linux devices.....	389
Managing MIA devices.....	390
Configure MIA settings.....	390
Apply labels to MIA devices.....	391
Delete MIA devices manually.....	391
Troubleshoot devices that fail to appear in inventory.....	391
Obtaining Dell warranty information.....	393
Obtain Dell warranty information on a single Dell device instantly.....	393
Renew a Dell warranty.....	394
Run Dell warranty reports.....	394
Managing applications on the Software page.....	394
About the Software page.....	394
View items in Software page inventory.....	395
Tracking changes to inventory settings.....	395
Adding and deleting applications in Software page inventory.....	395
Add applications to Software page inventory manually.....	395
Delete applications.....	397
Creating Software assets.....	397
Add Software assets in the Inventory section.....	397
Add Software assets in the Assets section.....	397
Attach digital assets to applications and select supported operating systems.....	398
Copy files to the K1000 Client Drop location.....	399
Using software threat levels and categories.....	400
Assign threat levels to applications.....	400
Assign categories to applications.....	400

Finding and labeling applications.....	400
About finding applications using Advanced Search.....	400
Add manual software labels.....	401
Apply manual labels to or remove labels from software.....	401
Add software Smart Labels.....	401
Managing the ITNinja feed.....	402
Enable the ITNinja feed.....	403
Viewing ITNinja information.....	403
Disable the ITNinja feed.....	404
Managing Software Catalog inventory.....	404
About the Software Catalog.....	404
Application classifications.....	405
About cataloged applications.....	405
About Locally Cataloged applications.....	405
About Not Allowed applications.....	406
Application categories.....	406
How Software Catalog information is collected.....	406
How the Software Catalog is used with the Organization component.....	406
How Software Catalog information is localized.....	406
How you can help improve the Software Catalog.....	406
Differences between the Software page and the Software Catalog page.....	407
Viewing Software Catalog information.....	408
View lists of Discovered and Not Discovered applications.....	409
View the list of Uncataloged applications.....	410
View the list of Locally Cataloged applications.....	411
View details of Software Catalog applications.....	412
Adding applications to the Software Catalog.....	415
Submitting cataloging requests automatically adds applications to the local Software Catalog.....	416
How Locally Cataloged applications change to Cataloged applications.....	416
How custom names are resolved when Locally Cataloged applications are added to the Software Catalog.....	416
Submit cataloging requests.....	417
Cancel cataloging requests and remove local cataloging.....	418
Managing License assets for Software Catalog applications.....	418
Add License assets for Software Catalog inventory.....	419
Migrate License assets to applications in the Software Catalog.....	423
Using software metering.....	423
About software metering.....	423

About metering information.....	423
Enabling and configuring metering for devices and applications.....	424
Viewing Software Catalog metering information.....	430
Disabling metering for Software Catalog applications and managed devices.....	432
Managing metering and scheduling inventory collection.....	433
Using Application Control.....	434
Requirements for blacklisting applications.....	434
How applications are blacklisted.....	435
About blacklisting application editions that share executable files.....	435
Applications that cannot be blacklisted.....	435
Apply the Application Control label to devices.....	435
Mark applications and suites as Not Allowed.....	436
View applications and suites that are marked as Not Allowed.....	436
Create reports showing applications marked as Not Allowed.....	437
Remove the Not Allowed designation from applications.....	438
Update or reinstall the Software Catalog.....	438
Managing process, startup program, and service inventory.....	439
Managing process inventory.....	439
View and edit process details.....	440
Add labels for processes.....	440
Apply labels to or remove labels from processes.....	440
Categorize processes.....	441
Assign threat levels to processes.....	441
Delete processes.....	441
Managing startup program inventory.....	442
View and edit startup program details.....	442
Add labels for startup programs.....	443
Apply labels to or remove labels from startup programs.....	443
Categorize startup programs.....	443
Assign threat levels to startup programs.....	443
Delete startup programs.....	444
Managing service inventory.....	444
View and edit service details.....	444
Add labels for services.....	445
Apply labels to and remove labels from services.....	445
Categorize services.....	445
Assign threat levels to services.....	446
Delete services.....	446

Writing custom inventory rules.....	446
About Custom Inventory rules.....	447
Types of Custom Inventory rules.....	447
Create Custom Inventory rules.....	447
How Custom Inventory rules are implemented.....	448
Syntax for Custom Inventory rules.....	449
Checking for conditions (conditional rules).....	450
Getting values from a device (Custom Inventory Field).....	458
Matching filenames to regular expressions.....	461
Understanding regular expressions.....	461
Regular Expression Rule Reference.....	463
Defining rule arguments.....	464
Test Custom Inventory rules.....	468
Deploying packages to managed devices.....	469
Distributing software and using Wake-on-LAN.....	469
About software distribution.....	469
About testing software distribution.....	470
Tracking changes to distribution settings.....	470
Types of distribution packages.....	471
Attaching digital assets to applications and selecting supported operating systems...	471
Distributing packages from the appliance.....	471
Distributing packages from alternate download locations and Replication Shares.....	472
About alternate download locations.....	472
About Replication Shares.....	472
Distributing applications to Mac OS X devices.....	472
Using Managed Installations.....	473
Adding applications to inventory.....	473
About creating Managed Installations.....	473
About installation parameters.....	474
Identify parameters that are supported by installer files.....	474
Create Managed Installations for Windows devices.....	474
Examples of common deployments on Windows.....	479
Create Managed Installations for ZIP files.....	479
Create Managed Installations for RPM files.....	480
Create Managed Installations for TAR.GZ files.....	486
Create Managed Installations for Mac OS X devices.....	486
Create and use File Synchronizations.....	491
Using Wake-on-LAN.....	494

Issue Wake-on-LAN requests.....	494
Schedule Wake-on-LAN requests.....	494
Troubleshooting Wake-on-LAN.....	495
Exporting Managed Installations.....	495
Broadcasting alerts to managed devices.....	495
Create alerts to be broadcast.....	496
Running scripts on managed devices.....	497
About scripts.....	498
Obtaining script dependencies.....	499
Tracking changes to scripting settings.....	499
About default scripts.....	499
Adding and editing scripts.....	501
Token replacement variables.....	502
Add offline KScripts or online KScripts.....	504
Edit scripts.....	510
Delete scripts from the Scripts page.....	510
Delete scripts from the Script Detail page.....	511
Structure of importable scripts.....	511
Import scripts.....	512
Duplicate scripts.....	512
Using the Run and Run Now commands.....	512
Run scripts from the Run Now page.....	513
Run scripts from the Script Detail page.....	514
Run scripts from the Scripts page.....	514
Monitor Run Now status and view script details.....	514
About configuration policy templates.....	515
Using Windows configuration policies.....	515
About starting Windows Automatic Updates on Windows devices.....	516
Add Automatic Update scripts.....	516
About Dell Command Monitor.....	517
Add Dell Command Monitor scripts.....	521
Add Desktop Wallpaper scripts.....	522
Add Desktop Shortcuts scripts.....	522
Add Event Log Reporter scripts.....	523
Add MSI Installer scripts.....	524
About power management and power consumption.....	525
Add power management scripts for Windows devices.....	526
Add Registry scripts.....	527

Add Remote Desktop Control Troubleshooter scripts.....	527
Add UltraVNC scripts.....	528
Add Uninstaller scripts.....	529
Using Mac OS X configuration policies.....	530
Add Active Directory scripts.....	530
Add Power Management scripts.....	531
Add VNC scripts.....	532
Edit policies and scripts.....	533
Search the scripting logs.....	533
Exporting scripts.....	534
Managing Mac profiles.....	535
Tracking changes to Mac profile settings.....	535
Adding, editing, and uploading Mac profiles.....	535
Add or edit Mac user profiles.....	535
Add or edit Mac system profiles.....	542
Add Mac profiles using existing profiles as templates.....	546
Upload Mac profiles to the K1000 appliance.....	547
Installing and managing Mac profiles.....	547
Distribute Mac profiles on a schedule.....	547
Install Mac profiles on devices using the Run option.....	549
Identify devices that have Mac profiles installed.....	549
View Mac profiles.....	550
Export the Mac profiles list.....	551
Removing and deleting Mac profiles.....	551
Remove Mac profiles from managed devices.....	551
Example: Remove a profile that has been deployed to specified devices.....	554
Delete Mac profiles from the K1000 appliance.....	555
Patching devices and maintaining security.....	556
About patch management.....	556
Patching workflow.....	556
About patch signature files.....	558
About patch packages.....	558
About patch testing and security.....	558
About the patch testing environment.....	558
About the patch quality assurance process.....	559
Best practices for patching.....	560
Subscribing to and downloading patches.....	562
About patch subscription and downloads.....	562

Websites that must be accessible to the K1000 appliance.....	563
Overview of first-time patch-subscription workflow.....	564
View details about operating systems and applications.....	565
Subscribing to patches and configuring download settings.....	565
Subscribe to patches.....	565
Select patch download settings.....	568
Viewing available patches and download status.....	571
View available patches.....	571
View patch download status.....	571
Creating and managing patch schedules.....	572
About scheduling critical OS patches for desktops and servers.....	572
Workflow for critical OS patches for desktops and servers.....	572
About scheduling critical patches for laptops.....	572
Workflow for critical patches for laptops.....	573
About scheduling non-critical patches.....	573
Configuring patch schedules.....	573
Fields on the Patch Schedule Details page.....	574
Configure Detect-only patch schedules.....	581
Configure Detect and Deploy patch schedules.....	582
Configure Deploy-only patch schedules.....	583
Configure Detect and Rollback patch schedules.....	583
Configure Rollback-only patch schedules.....	584
Viewing patch schedules, status, and reports.....	585
View patch schedules.....	585
View patch status.....	587
View patch status by device.....	587
View files within patches.....	588
View patch reports.....	588
Managing patch rollbacks.....	588
Determine whether a patch can be rolled back.....	588
Undo the last patching job.....	589
Managing patch inventory.....	589
Prerequisites for managing patch inventory.....	589
Viewing patch information.....	589
View downloaded patches.....	590
View patch details.....	592
Resetting the number of patch deploy attempts.....	593
View patch information for devices in inventory.....	594

View devices missing patches.....	594
Viewing patch statistics and logs.....	594
View patch statistics.....	594
View the patch log.....	595
Mark patches as inactive.....	595
Patch Mac OS X devices.....	595
Managing Dell devices and updates.....	596
Managing Dell devices with Dell Updates.....	596
Differences between patching and Dell Updates.....	596
Configuring Dell Updates.....	597
Configure Dell Update catalog updates.....	597
Create Dell Update schedules.....	598
Maintaining device and appliance security.....	599
Testing device security.....	599
About OVAL security checks.....	599
Understanding OVAL tests and definitions.....	599
About SCAP.....	605
About benchmarks.....	607
How a SCAP scan works.....	608
Editing SCAP scan schedules.....	610
About security policy templates.....	613
Using Windows security policy templates.....	614
Using Mac security policy templates.....	620
Resolve Windows security issues that prevent Agent provisioning.....	623
Maintaining appliance security.....	623
Security run output.....	623
Using reports and scheduling notifications.....	625
About reports and notifications.....	625
About reports.....	625
About notifications.....	625
Tracking changes to report settings.....	625
Creating and modifying reports.....	626
Creating reports.....	626
Create reports using the report wizard.....	626
Create reports using SQL queries.....	628
Create reports from list pages.....	630
Duplicate reports.....	631
Edit SQL statements on reports created with the report wizard.....	631

Create reports from history lists.....	632
Modifying reports.....	632
Edit reports.....	632
Delete reports.....	633
Customizing logos used for reports.....	633
Create or modify linked reports.....	633
Scheduling reports and notifications.....	635
Running single-organization and consolidated reports.....	635
Run single-organization reports.....	635
Run consolidated organization reports.....	636
Scheduling reports.....	636
Add report schedules.....	636
Delete report schedules.....	638
Scheduling notifications.....	638
Add notification schedules from the Reporting section.....	638
Add notification schedules from list pages.....	639
Edit notification schedules.....	640
Delete notification schedules.....	641
Monitoring servers.....	642
Getting started with server monitoring.....	644
Enable monitoring for a device.....	644
Enable monitoring for one or more servers from the Devices inventory list.....	644
Enable monitoring for a server from its Device Detail page.....	645
Obtain a new license key to increase server monitoring capacity.....	646
Apply a new license key to increase server monitoring capacity.....	646
Working with monitoring profiles.....	646
Edit a profile.....	648
Configure SNMP trap messages and alerting criteria.....	649
Create a new profile using a default profile as a template.....	651
Profile log paths for MySQL and Apache.....	653
Upload a profile that was created by another user.....	653
Download a profile so that it can be used by others.....	654
Bind an additional profile to a device.....	654
Define nonstandard log date format.....	654
Configuring application and threshold monitoring with Log Enablement Packages.....	655
Install one or more LEPs on monitored devices.....	656
Set up a Windows Server 2003 device with an ITNinja monitoring Log Enablement Package (LEP).....	656

Edit the monitoring Log Enablement Package (LEP) for a Windows Server 2008 or higher device.....	658
Edit the monitoring Log Enablement Package (LEP) for a Windows Server 2003 device.....	659
Managing monitoring for devices.....	660
Pause monitoring for a device.....	660
Pause or resume monitoring for multiple devices.....	661
Set the polling interval and any automatic dismissal or deletion of alerts.....	661
Disable ping probe.....	662
Receive alerts when device configurations change.....	662
Schedule a Maintenance Window during which time alerts are not collected from a device.....	662
Create and assign monitoring-specific roles.....	663
Disable monitoring for one or more devices.....	666
Enable monitoring for one or more devices.....	666
Working with alerts.....	667
Add notification schedules from the Monitoring Alerts list page.....	667
Create a Service Desk ticket from an alert.....	669
Search for alerts using Advanced Search criteria.....	672
Filtering alerts using the Include Text and Exclude Text capability.....	672
Filter alerts using the Include Text and Exclude Text capability from the Profile Details page.....	673
Filter alerts using the Exclude Text capability from the Monitoring Alerts list page.....	673
Examples of Include Text and Exclude Text for monitoring profiles.....	674
Dismiss an alert.....	676
Retrieve and review alerts that have been dismissed from the alerts list.....	677
Delete alerts.....	677
Using the Service Desk.....	678
Configuring Service Desk.....	678
System requirements.....	678
About Service Desk.....	678
Overview of setup tasks.....	679
Configuring Service Desk business hours and holidays.....	680
Configure Service Desk business hours.....	680
Configure Service Desk holidays.....	680
Configuring Service Level Agreements.....	681
Enable Service Level Agreements.....	681
Configuring Service Desk ticket queues.....	682
Configure ticket queues.....	682
Rename Service Desk titles and labels.....	686

Enable or disable the conflict warning.....	687
Configuring ticket settings.....	688
Customize the Ticket Detail page.....	688
Customizing the User Console home page.....	691
Change the User Console logo and text at the System level.....	691
Change the User Console logo and login text at the Admin-level.....	693
Show or hide action buttons and widgets on the User Console home page.....	694
Show or hide links to Knowledge Base articles on the User Console home page.....	696
Add, edit, hide, or delete User Console announcements.....	696
Prioritize User Console announcements or mark an announcement as urgent.....	698
Add, edit, or delete custom links on the User Console home page.....	699
Add ticket links to the User Console home page.....	700
Add a quick-action link for reporting problems on the User Console home page.....	700
About the session timeout period.....	701
Using the Satisfaction Survey.....	701
Changing the Satisfaction Survey default behavior.....	701
Enable or disable security for Service Desk attachments.....	702
Managing Service Desk tickets, processes, and reports.....	703
Overview of Service Desk ticket lifecycle.....	703
Creating tickets from the Administrator Console and User Console.....	704
Create tickets from the User Console.....	704
Create tickets from the Administrator Console Ticket page.....	705
Create tickets from the Device Detail page.....	710
Create tickets from the Asset Detail page.....	711
Create a Service Desk ticket from an alert.....	712
Creating and managing tickets by email.....	715
About attachments to tickets created through email.....	715
Enable email ticket creation.....	715
Modifying ticket attributes using email.....	716
Clearing a ticket field using email.....	716
Changing ticket fields using email.....	716
Changing ticket approval fields using email.....	717
Viewing tickets and managing comments, work, and attachments.....	718
Navigate among tickets, related devices, and assets.....	718
Add work information for tickets.....	718
Use default views for tickets.....	719
Create custom views for tickets.....	721
Set a view as the default view for tickets.....	721

Add comments to tickets.....	721
Add owner-only comments to tickets.....	722
View ticket comments.....	722
Add or delete screenshots and attachments to Service Desk tickets.....	723
View ticket activity history.....	724
Send ticket information through email.....	724
Run Device Actions from tickets.....	725
Using the ticket escalation process.....	725
Understanding ticket states.....	725
Understanding the escalation time limit.....	726
Understanding escalation.....	726
Changing ticket escalation settings.....	726
Change the list of escalation email recipients.....	726
Change the escalation time limits.....	727
Change the default escalation email message.....	727
Using Service Desk processes.....	727
Add, edit, and enable process templates.....	728
Define process types.....	732
Create process tickets to manage related tasks.....	733
View process information.....	733
Cancel or complete process tickets.....	734
Delete process templates.....	735
Convert process tickets to regular tickets.....	735
Convert regular tickets to process tickets.....	735
Using Ticket Rules.....	736
Using and configuring system Ticket Rules.....	736
Understanding and customizing system Ticket Rules.....	736
Create custom Ticket Rules.....	737
Duplicate a custom Ticket Rule.....	740
Delete a custom Ticket Rule.....	740
Move a Ticket Rule from one queue to another.....	741
Run Service Desk reports.....	741
Archiving, restoring, and deleting tickets.....	741
Enable ticket archival.....	742
Configure queue archive settings.....	743
Archive selected tickets.....	744
Restore archived tickets.....	744
Delete archived tickets.....	744

Managing ticket deletion.....	745
Configure ticket deletion settings.....	745
Delete tickets.....	745
Managing Service Desk ticket queues.....	745
About Service Desk ticket queues.....	746
Adding and deleting queues.....	746
Add a queue.....	746
Add a queue by duplicating an existing queue.....	747
Delete a queue or queues.....	747
Viewing tickets in queues.....	747
View tickets across all queues.....	748
Setting the default queue.....	748
Set the default queue at the system level.....	748
Set the default queue at the user level.....	749
Set the default fields for the All Queues ticket list.....	749
Move tickets between queues.....	750
About User Downloads and Knowledge Base articles.....	751
Managing User Downloads.....	751
Add User Downloads.....	751
Apply labels to User Downloads.....	753
Remove labels from User Downloads.....	754
Delete User Downloads.....	754
Managing Knowledge Base articles.....	754
Add, edit, or duplicate Knowledge Base articles.....	754
Delete Knowledge Base articles.....	756
View user ratings and the number of views for Knowledge Base articles.....	756
Customizing Service Desk ticket settings.....	757
About customizing Service Desk ticket settings.....	757
Create ticket categories and subcategories.....	757
Customizing ticket values.....	759
Customize ticket status values.....	760
Customize ticket priority values.....	761
Customize ticket impact values.....	762
Customizing ticket layout.....	762
Customize Layout and Related Ticket Fields.....	763
Configure Comment Field Options.....	765
Define custom ticket fields.....	765
Preview ticket layout.....	767

Customize the ticket list layout.....	768
Using parent-child ticket relationships.....	769
Enable parent-child ticket relationships for a queue.....	769
Enable parent tickets to close child tickets.....	770
Create child tickets for any ticket.....	770
Designate tickets as parents and add existing tickets as their children.....	771
Use a parent ticket as a to-do list.....	772
Use parent tickets to organize duplicate tickets.....	772
Using ticket approvers.....	773
Configure ticket approvers.....	773
Approving tickets by email.....	774
Configuring SMTP email servers.....	774
Connect your email server to the K1000 appliance.....	774
Using internal and external SMTP servers.....	775
Use the internal SMTP server.....	775
Use an external SMTP server or Secure SMTP server.....	775
Maintenance and troubleshooting.....	778
Maintaining the appliance.....	778
Tracking changes to settings.....	778
About appliance backups.....	778
Set the daily backup schedule and the number of backups to retain.....	779
Back up the appliance manually.....	780
Download backup files from the Administrator Console.....	780
Access backup files through FTP.....	780
About deleting appliance backup data.....	781
Restoring the appliance.....	782
Restore the appliance using the most recent backup.....	782
Upload backup files to the appliance.....	783
Restore the appliance from backups.....	784
Restore the appliance to factory settings.....	785
Updating appliance software.....	785
Check for and apply advertised appliance updates.....	785
Upload an update file to the appliance manually.....	786
Verify updates.....	786
Update the appliance license key.....	787
Reboot or shut down the appliance.....	787
Update OVAL definitions from KACE.....	787
Understanding the daily run output.....	788

Disk status.....	788
Appliance network interface status.....	789
Appliance up-time and load averages.....	789
Email system health.....	789
Appliance backup status.....	790
Status of RAID drives.....	790
Troubleshooting the K1000.....	790
Using Troubleshooting Tools.....	790
Verify the status of devices on the network.....	791
Enable a tether to Quest Support.....	791
Troubleshooting appliance issues.....	792
View appliance logs.....	792
Download appliance activity logs.....	795
Viewing the daily run output.....	796
Troubleshooting and debugging the K1000 Agent.....	796
Resolve Windows security issues that prevent Agent provisioning.....	796
Enabling debugging on Windows devices.....	796
Enable debugging on Linux devices.....	797
Enable debugging on Mac OS X devices.....	797
Testing and troubleshooting email communication.....	798
Test outgoing email.....	798
Test incoming email.....	798
Use Telnet to test incoming email.....	799
Access appliance logs to view Microsoft Exchange Server errors.....	799
Troubleshooting email errors.....	800
About Two-Factor Authentication.....	800
Appendixes.....	801
Database table names.....	801
Adding steps to task sections of scripts.....	821
LDAP variables.....	836
Glossary.....	839
A.....	839
B.....	841
C.....	842
D.....	843
E.....	845
F.....	846
I.....	847

K.....	848
L.....	849
M.....	850
N.....	852
O.....	853
P.....	855
Q.....	856
R.....	857
S.....	858
T.....	860
U.....	861
V.....	862
W.....	863
About us.....	864
We are more than just a name.....	864
Our brand, our vision. Together.....	864
Contacting Quest.....	864
Technical support resources.....	864
Legal notices.....	865
Index.....	866

About the KACE Systems Management Appliance (K1000)

Quest® KACE® Systems Management Appliance (K1000) is a physical or virtual appliance designed to automate device management, application deployment, patching, asset management, reporting, and Service Desk ticket management.

For more information about K1000 series appliances, go to the Quest website, <https://www.quest.com/products/kace-k1000-systems-management-appliance/>.

About K1000 components

K1000 components include software, hardware, web-based interfaces, and a mobile app interface.

The K1000 has the following components:

Table 1. K1000 components

Component	Description
Physical appliance or virtual appliance	The K1000 is available as a physical or hardware-based appliance, and as a virtual appliance. The virtual appliance (VK1000) uses a VMware® infrastructure. The same system management features are available on both the physical and virtual appliances. For the latest information about K1000 hardware, requirements for managed devices, and browser requirements for accessing the Administrator Console, see the technical specifications: • For physical appliances: Go to https://documents.quest.com/KACE-Systems-Management-Appliance/Technical-Specifications-for-Physical-Appliances. • For virtual appliances: Go to https://documents.quest.com/KACE-Systems-Management-Appliance/Technical-Specifications-for-Virtual-Appliances. • For K1000 as a Service: Go to http://documents.quest.com/KACE-Systems-Management-Appliance/technical-specifications-for-kace-as-a-service/.
Command Line Console	The Command Line Console is a terminal window interface to the K1000 appliance. The interface is designed primarily to configure the appliance and

Component	Description
Administrator Console	enforce policies. See Power-on the appliance and log in to the Administrator Console. The Administrator Console is the web-based interface used to control the K1000 appliance. To access the Administrator Console, go to <code>http://K1000_hostname/admin</code> where <code>K1000_hostname</code> is the hostname of your appliance. If the Organization component is enabled, you can access the System-level settings of the Administrator Console at <code>http://K1000_hostname/system</code>. To view the full path of URLs in the Administrator Console, which can be useful when searching the database or sharing links, add <code>ui</code> to the URL you use to log in. For example: <code>http://K1000_hostname/admin</code>.
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 <code>http://K1000_hostname/user</code> where <code>K1000_hostname</code> is the hostname of your appliance. 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.
K1000 Agent	The K1000 Agent is an application that can be installed on devices to enable device management through the K1000 appliance. Agents that are installed on managed devices communicate with the K1000 appliance through AMP (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 K1000 Agent.

Component	Description
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 StoreSM 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 K1000 license 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://K1000_hostname/admin`, where K1000_hostname is the hostname 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://K1000_hostname/admin` to log in to the Default organization. K1000_hostname is the hostname 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.

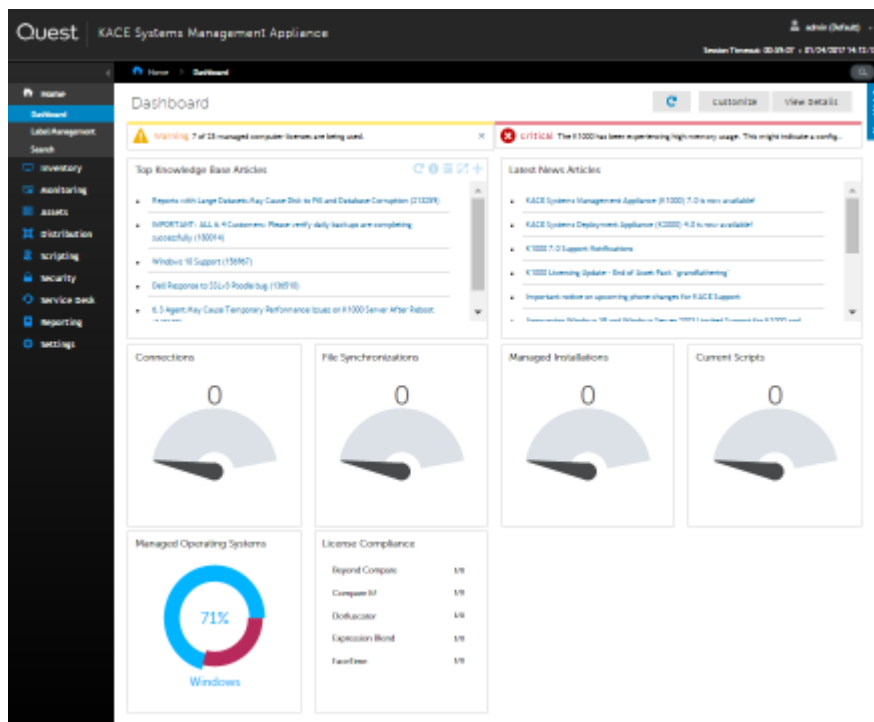
If you have multiple organizations and the *fast switching* option is enabled, you can switch between organizations and the System level using the drop-down list in the top-right corner of the page next to the login information. See [Enable fast switching for organizations and linked appliances](#).

- **System mode with the Organization component enabled:** If the Organization component is enabled on your appliance, go to `http://K1000_hostname/system`, to log in to System mode. K1000_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](#).

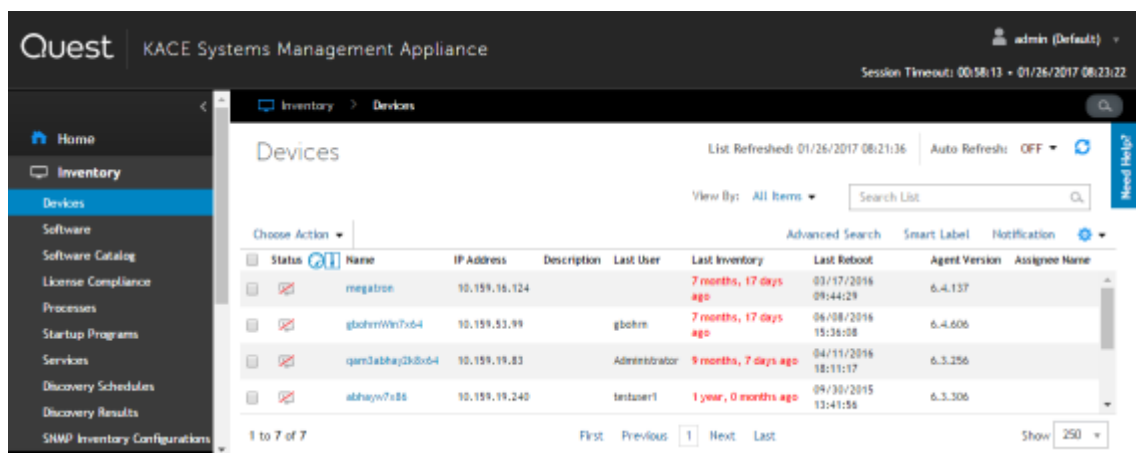
In addition, if the *fast switching* option is enabled, and the passwords for the default admin accounts of the organizations are the same, you can switch between organizations using the drop-down list in the top-right corner of the page. See [Enable fast switching for organizations and linked appliances](#).

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.



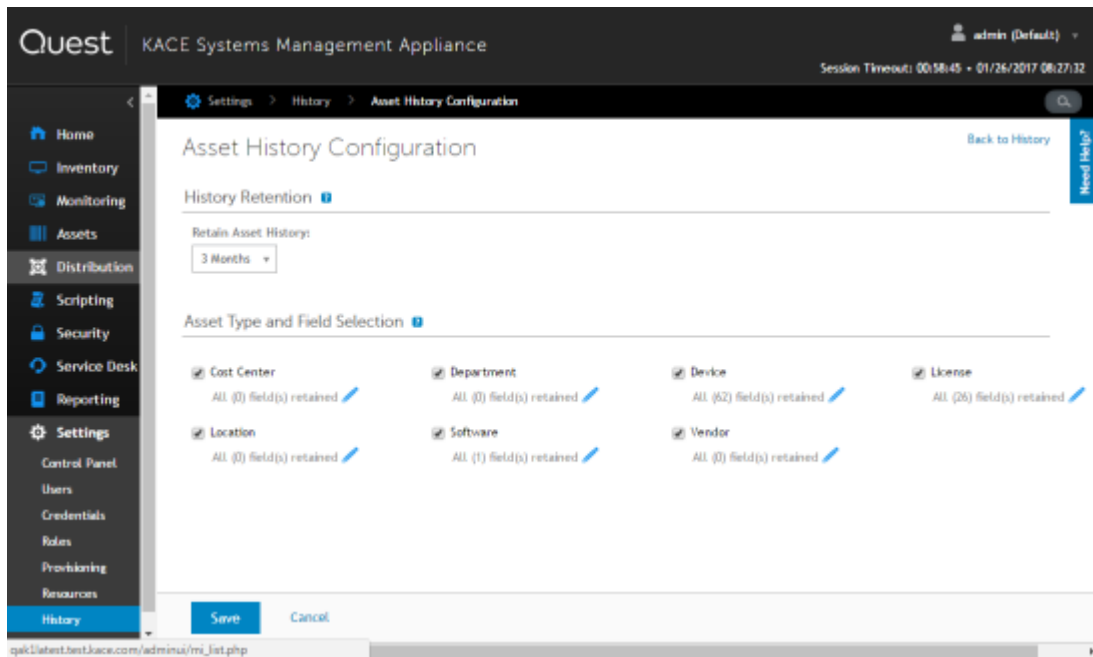
- **List pages.** These pages enable you to view items available on the appliance or, if the Organization component is enabled, in the selected organization.



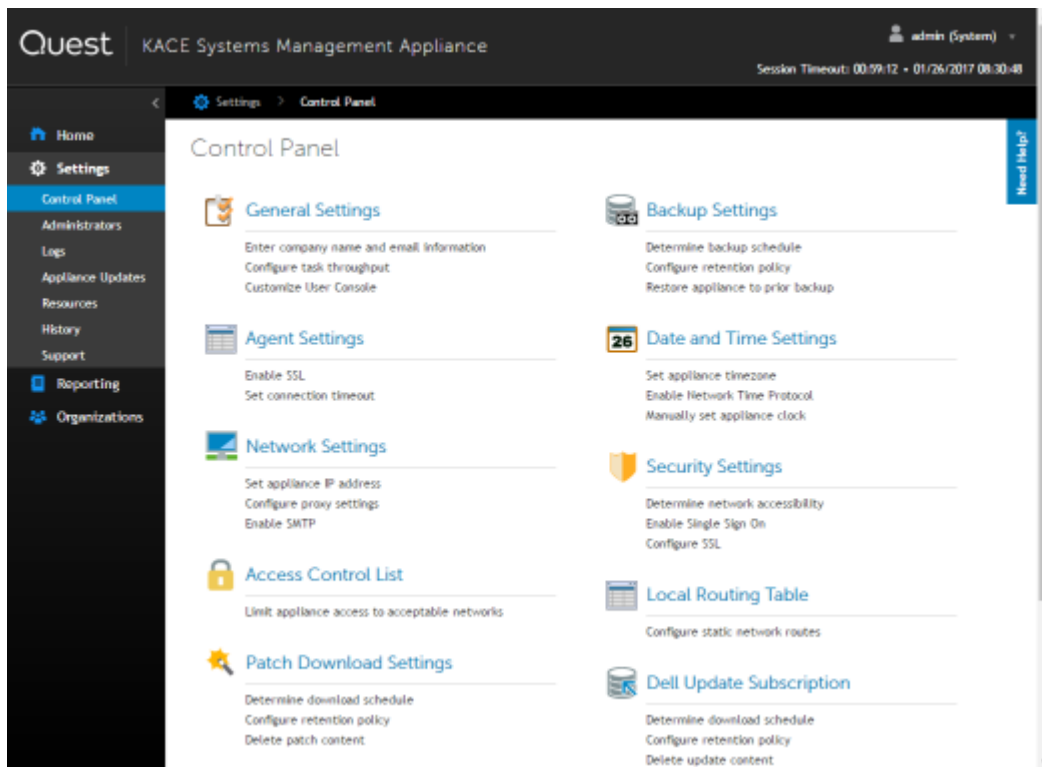
- **Detail pages.** These pages enable you to view and edit details of the selected item.



- **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.

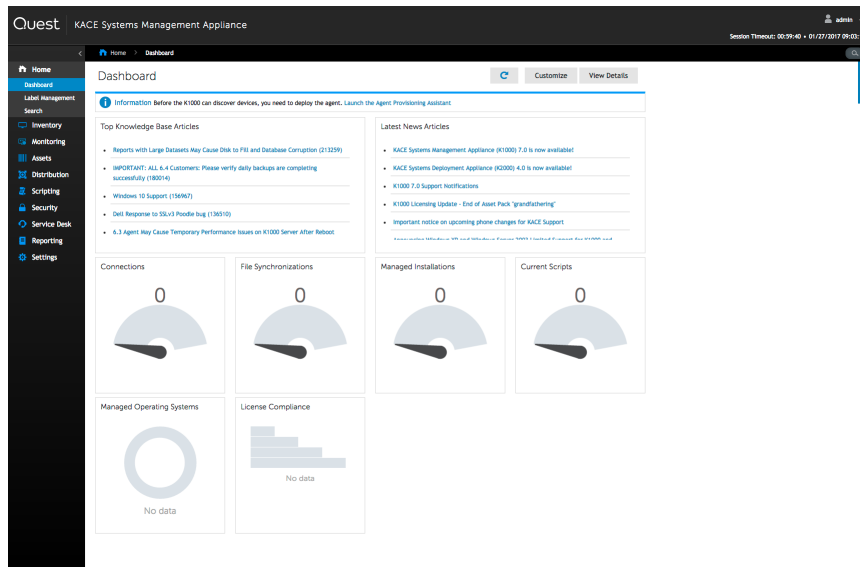


Table 2. Components available in Admin mode without the Organization component

Component	UI page	Used to...
Home	- Dashboard - Label Management - Search	Review appliance statistics, manage labels, view historical information, and search for data. See Using the Home component .
Inventory	- Devices - Software - Software Catalog - License Compliance - 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 License Compliance Managing process, startup program, and service inventory Using Device Discovery Using SNMP Inventory Configurations to identify

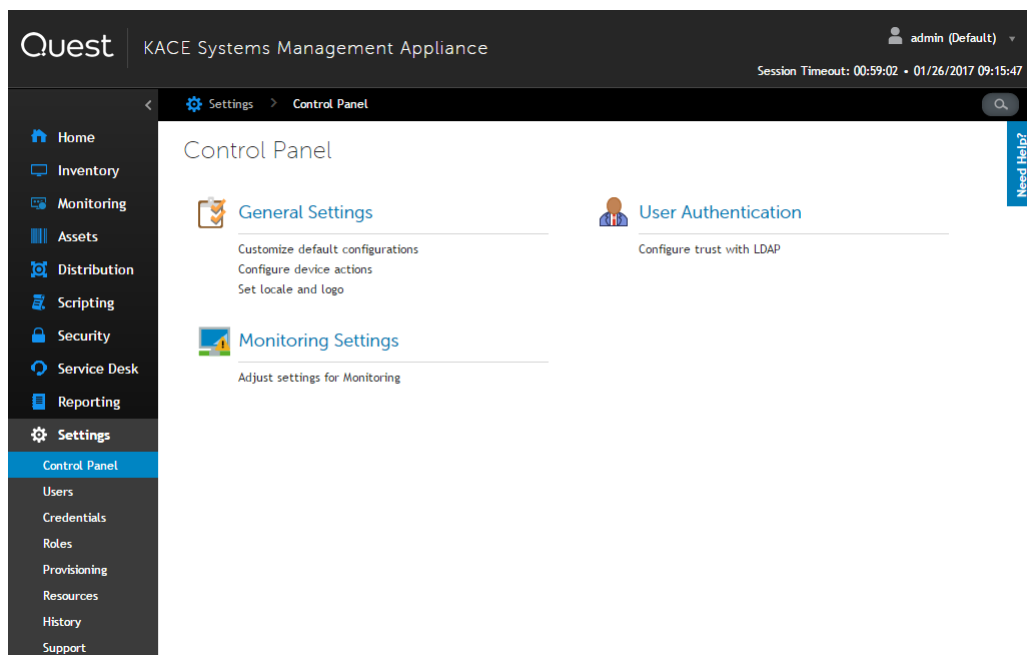
Component	UI page	Used to...
		specific SNMP objects and non-computer devices to add to inventory
Monitoring	• Devices • Alerts • Profiles • Maintenance Windows • Log Enablement Packages	Manage basic event monitoring for 5 servers with your standard license, gathering event data from core Windows® event logs, syslogs, and application logs. With the Monitoring Module license, manage event monitoring for up to 200 servers. See Monitoring servers
Assets	• Assets • Asset Types • 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.
Distribution	• Managed Installations • File Synchronizations • Wake-on-LAN • Replication • Alerts	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 • Configuration Policies • Security Policies • Mac Profiles	Automate tasks performed on managed devices. See Running scripts on managed devices.
Security	• Patch Management • OVAL Scan • SCAP Scan • Dell Updates	Reduce the risks from malware, spyware, and viruses. OVAL (Open Vulnerability Assessment Language) is a battery of tests that can be run to identify security vulnerabilities on managed devices.

Component	UI page	Used to...
		See Patching devices and maintaining security .
Service Desk (also known as <i>Help Desk</i> on appliances that have been upgraded from early versions)	• 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. See Using reports and scheduling notifications.
Settings	• Control Panel • Users • Credentials • Quest Identity Broker • Roles • Logs • Appliance Updates • Provisioning • Resources • History • Support	Administer your appliance and Agent provisioning. See: • Configuring the appliance • Configuring user accounts, LDAP authentication, and SSO • Managing credentials • About Quest Identity Broker • Maintaining the appliance • Provisioning the K1000 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://K1000_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 [Table 3](#) for components, and see the following illustration.

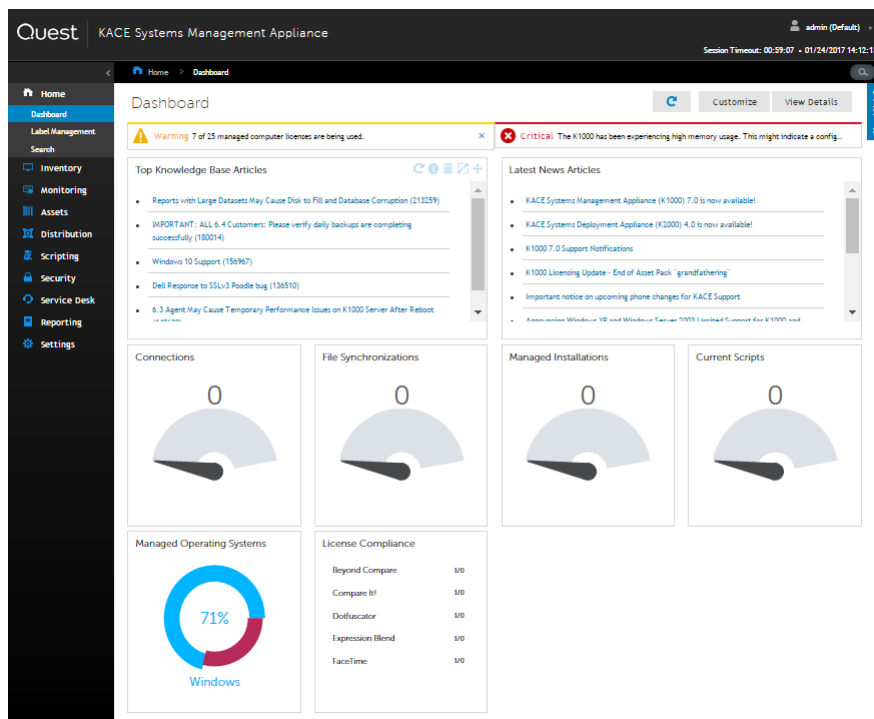


Table 3. Components available in Admin mode with the Organization component enabled

Component	UI page	Used to...
Settings	- Control Panel - Users - Credentials - Quest Identity Broker - 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 About Quest Identity Broker Provisioning the K1000 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 K1000 System Administration Console, http://K1000_hostname/system, or select **System** in the drop-down list in the top-right corner of the Administrator Console, the following components are available.

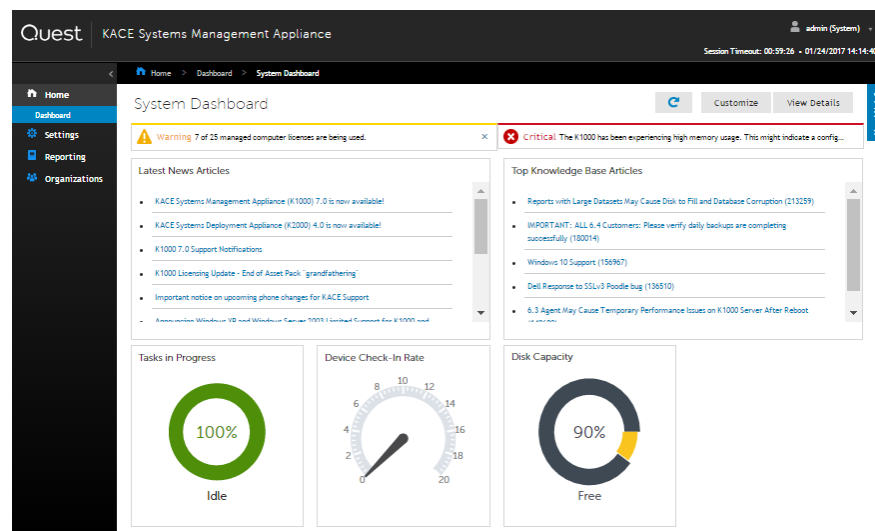


Table 4. Components available in System mode with the Organization component enabled

Component	Sub-tabs	Used to...
Home	Dashboard	Review summary statistics for the appliance. See Using the Home component .
Settings	- Control Panel - Administrators - Logs - Appliance Updates - Resources - History - Support	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. See Using reports and scheduling notifications .
Organizations	- Organizations - Roles - Filters - Devices	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://K1000_hostname/admin), the Dashboard shows information for the selected organization. When you are logged in to the System Administration Console (http://K1000_hostname/system), the Dashboard shows information for the appliance, including all organizations.



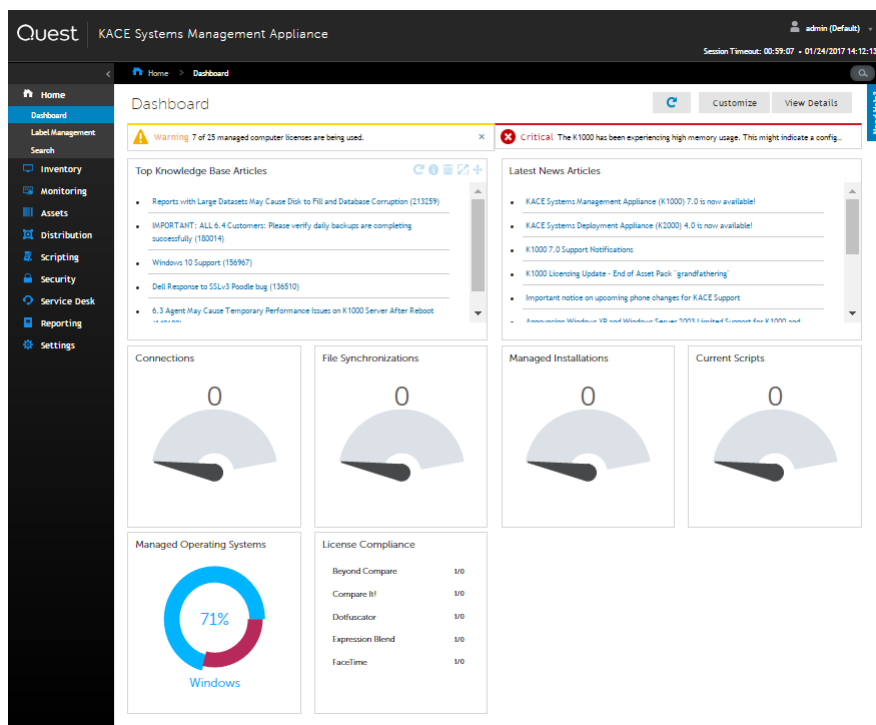
TIP: The appliance updates the summary widgets periodically. To update all of the widgets any time, click the **Refresh** button in the upper right of the page: . To update individual widgets, hover over the widget, then click the **Refresh** button above the widget.

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 K1000 Administrator Console, http://K1000_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.

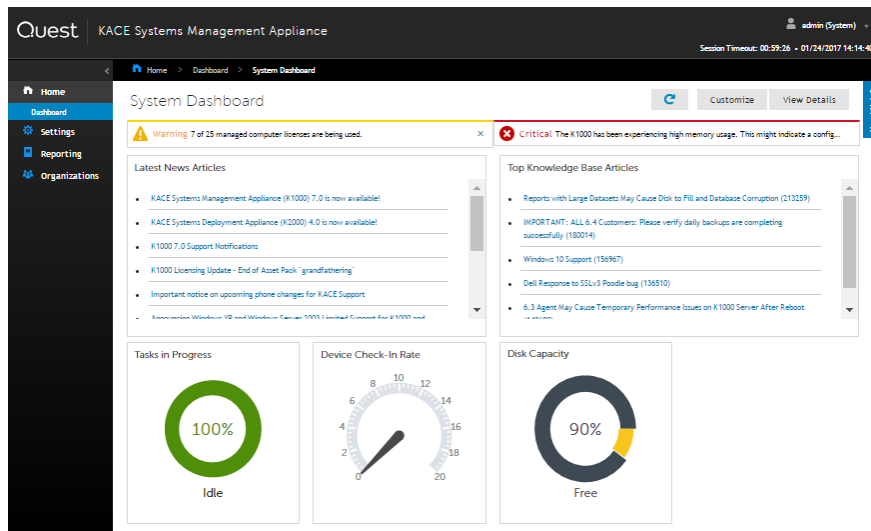


View the Dashboard in System mode

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

- Log in to the K1000 System Administration Console, http://K1000_hostname/system, or select **System** from the drop-down list in the top-right corner of the page.

The *System Dashboard* page appears.



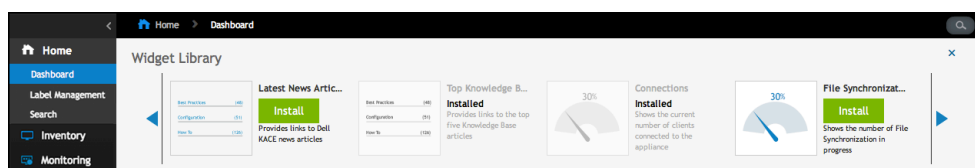
Customize Dashboard pages

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

- Do one of the following:
 - Log in to the K1000 Administrator Console, http://K1000_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 K1000 System Administration Console, http://K1000_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.

- Mouse over the widget, then use any of the following buttons:
 - : Refresh the information in the widget.
 - : Display information about the widget.
 - : Hide the widget.
 - : Resize the widget.
 - : Drag the widget to a different position on the page.
- Click the **Customize** button in the top-right corner of the page to view available widgets.



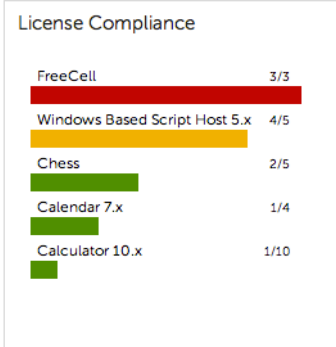
- To show a widget that is currently hidden, click **Install**.

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
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 K1000 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.
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.
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.
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.
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.
Critical Patch Compliance	This widget shows the deployment progress of patches that are marked as critical. If the

Widget	Description
	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 <i>Software</i> page and the <i>Software Catalog</i> page, and the license mode for applications must be <i>Unit License</i> or <i>Enterprise</i> for license information to appear on this widget. Applications with other license modes, such as <i>Shareware</i>, <i>Freeware</i>, or <i>Not Specified</i>, are not displayed on this widget. This widget is for information only, and the K1000 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 K1000 Agent provisioning or installation tasks. If the Organization

Widget	Description
	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 K1000 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 K1000 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 <i>System Dashboard</i> page.
SCAP Summary	This widget provides information about SCAP scans that have been performed on devices. 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 K1000 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.
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.
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 K1000 device inventory. If the Organization component is enabled on your appliance, this widget shows the percentage of devices in the selected organization.

Widget	Description
Software Publishers	This widget displays the publishers 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 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 <i>Reports</i> list page for Dell Warranty reports. 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 urgent, recommended, or optional depending on the urgency of the update. After a Dell Update schedule is created, data appears in the widget. See Create Dell Update schedules. 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

Widget	Description
	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 <i>Low Resource Alerts</i> options on the <i>Settings History Configuration</i> page. For more information, see Configure System-level settings history subscriptions with the Organization component enabled.
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.

View Dashboard details

Dashboard details show statistics for the appliance or the selected organization.

If the Organization component is enabled on your appliance, and you are logged in to the Administrator Console (http://K1000_hostname/admin), the statistics are shown for the selected organization. When you are logged in to the System Administration Console (http://K1000_hostname/system), the statistics are shown for the appliance, including all organizations.

On new appliances that have no managed devices, the *Dashboard Detail* page shows zero or no records.

- Do one of the following:
 - Log in to the K1000 Administrator Console, http://K1000_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 K1000 System Administration Console, http://K1000_hostname/system, or select **System** from the drop-down list in the top-right corner of the page.

- Click **Home**.

The *Dashboard* or *System Dashboard* page appears.

- In the top-right corner of the page, click **View Details**.

The *Dashboard Detail* page appears. It shows the following information:

Summary Section	Description
Alerts	Information about license capacity and usage for managed devices in inventory.
Devices	Information about managed devices, including a breakdown of the operating systems in use. In addition, if the number of managed devices exceeds the number allowed by your license key, you are notified of it here.

Summary Section	Description
Software	A summary of the applications that are available in inventory on the appliance. This includes applications listed on the <i>Software</i> page and the <i>Software Catalog</i> page.
Distributions	The applications that have been distributed to managed devices, separated by distribution method. This section also indicates the number of packages that are enabled and disabled.
Monitoring Alerts Summary	The number of unacknowledged alerts for monitored devices, grouped by alert level. The following icons indicate alert level: •  Critical •  Error •  Warning •  Information •  Recovered
Alert Summary	The alerts that have been distributed to managed devices, separated by the alert type. This summary also indicates the number of alerts that are active and expired. The <i>IT Advisory</i> refers to the number of Knowledge Base articles in User Console.
Patches	The patches received from software vendors such as Microsoft® and Apple. The summary includes the date and time of the last patch (successful and attempted), total patches, and total packages downloaded.
OVAL	Information about the Open Vulnerability Assessment Language (OVAL), a battery of tests that can be run to identify security vulnerabilities on managed devices. OVAL information includes: • The definitions received • The date and time of the last OVAL download (attempted and successful) • The number of OVAL tests in the appliance • The number of devices scanned • The number of vulnerabilities detected on managed devices
Discovery (Network Scan)	The results of Discovery scans that have run on the network, including the number of IP addresses

scanned, the number of services discovered, and the number of scans that have been performed.



NOTE: When this page is refreshed, the record count is updated. New K1000 installations contain zero records.

For more information about OVAL, see [Maintaining device and appliance security](#).

View the K1000 version, model, and license information

The **About K1000** link in the *Help* panel displays the K1000 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 **Need 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 (K1000) 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.

- **Live Chat** (💬): Starts a chat with a KACE System Management Appliance (K1000) 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.

- **KACE GO 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 K1000** (📄): Displays information about your KACE System Management Appliance (K1000) installation.



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

- Click the **About K1000** link located at the bottom-right corner of the panel.

The K1000 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 Servers, and Assets that your license entitles you to manage.

Managed Computers are devices in K1000 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 Servers are servers that 1) meet the requirements for Managed Computers and 2) have Monitoring enabled.

Assets that count toward your license limit include devices that 1) have been added to the K1000 inventory but do not meet the definition of Managed Computers or Monitored Servers 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 assets you create and manage using the Asset Management component do not count toward the license limit.



NOTE: Your K1000 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 https://quest.com/docs/Product_Guide.pdf.

NOTE: To increase your license capacity, go to the Quest website: <https://quest.com/buy>.

- License terms and conditions.
- Third-party code attributions.

Optional: View K1000 license information with enabled components. See [View K1000 license information](#).

View K1000 license information

K1000 license information appears in the *Appliance Updates* section of the Administrator Console.

- Go to the appliance *Control Panel*:
 - If the Organization component is not enabled on the appliance, log in to the K1000 Administrator Console, `http://K1000_hostname/admin`, then click **Settings**.
 - If the Organization component is enabled on the appliance, log in to the K1000 System Administration Console, `http://K1000_hostname/system`, or select **System** in the drop-down list in the top-right corner of the page, then click **Settings**.
- Click **Appliance Updates**.
- 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 K1000 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 Servers:** The number of Monitored Servers your license entitles you to manage. Monitored Servers are servers that 1) meet the requirements for Managed Computers and 2) have Monitoring enabled.
- Assets:** Assets that count toward your license limit include devices that 1) have been added to the K1000 inventory but do not meet the definition of Managed Computers or Monitored Servers 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 assets you create and manage using the Asset Management component do not count toward the license limit.



NOTE: Your K1000 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.

NOTE: To increase your license capacity, go to the Quest website: <https://quest.com/buy>.

- **Expires:** The license expiration date, in month/day/year format.
- **Components:** The components enabled under your license.

Optional: View the K1000 serial number, model number, license terms and conditions, and third-party code attributions. See [View the K1000 version, model, and license information](#).

About appliance software updates

The K1000 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](#)

[Managing LDAP Labels](#)

Searching for information and filtering lists

You can search the K1000 databases, and filter list pages, to find information on the appliance.

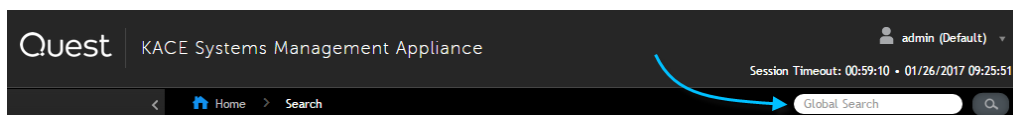
If the Organization component is enabled on your appliance, you can search the database of each organization separately. You cannot search the databases of all organizations at once, and you cannot search at the System level.

Search at the Admin level

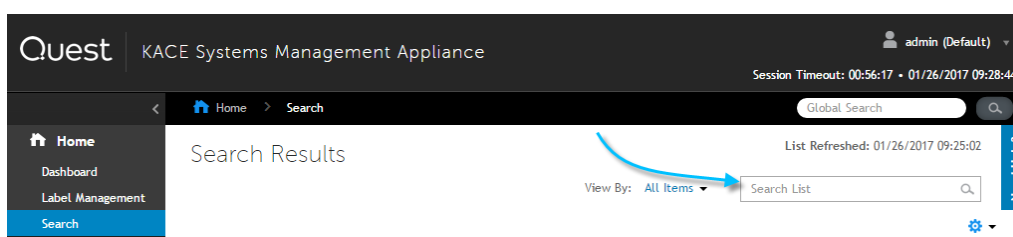
You can search the Admin-level databases to find information on the appliance.

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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the 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 **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:



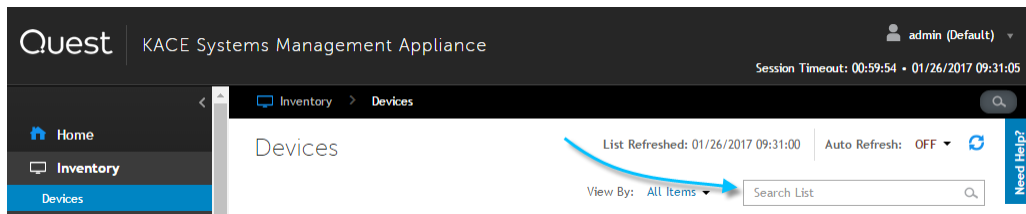
TIP: Use the percent sign (%) as a wildcard. For example, you can use the percent sign in a search string to find all items that match the criteria before and after the percent sign.

Search at the page level

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

1. Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the 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 Advanced Search criteria

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

1. Go to the *Devices* list:
 - a. Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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**.
2. Click the **Advanced Search** tab above the *Devices* list on the right.

The *Advanced Search* 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the 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 *Advanced Search* tab above the list on the right and enter the search criteria.

See [Example: Search for managed devices using Advanced Search 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.

The screenshot shows the 'Smart Label' configuration interface. At the top, there are tabs for 'Advanced Search', 'Smart Label', and 'Notification'. The 'Smart Label' tab is active. Below the tabs, there are two search criteria: 'Name contains Windows' and 'Disk % Capacity > 95'. Each criterion has an 'Add Line' and 'Add Group' button. At the bottom, there is a 'Choose label:' dropdown, a 'Test' button, a 'Save' button, and a 'Metering Enabled' checkbox.

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.
 - 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.

The screenshot shows the 'Notification' configuration interface. At the top, there are tabs for 'Advanced Search', 'Smart Label', and 'Notification'. The 'Notification' tab is active. Below the tabs, there are two search criteria: 'Name contains Windows' and 'Disk % Capacity > 95'. Each criterion has an 'Add Line' and 'Add Group' button. Below the search criteria, there are fields for 'Frequency' (set to '15 Minutes'), 'Title', and 'Recipient'. At the bottom, there are 'Test' and 'Save' buttons.

8. Provide the following information:

Field	Description
Title	The information that you want to appear in the <i>Subject</i> 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 Advanced Search criteria](#)

Load Smart Labels from the Advanced Search tab

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

1. Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the 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 **Advanced Search** tab above the list on the right to display the *Advanced Search* panel.
4. At the top of the *Advanced Search* 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 *Advanced Search* panel.

Create Custom Views using Advanced Search criteria

You can create Custom Views using Advanced Search criteria. Custom Views display list items using predefined Advanced Search 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the 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 **Advanced Search** 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 Advanced Search 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 **Need 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** (

KACE Systems Management Appliance (K1000) 7.1
Access product documentation

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

- **Live Chat** (): Starts a chat with a KACE System Management Appliance (K1000) product specialist.

i **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.

i **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.

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

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

i **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 K1000** (): Displays information about your KACE System Management Appliance (K1000) installation.

i **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.

i **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.

i **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.** Chat with a product specialist.

- a. Click .

The *Live Chat* dialog box appears.



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.

- b. In the *Live Chat* dialog box, provide your full name and email address.
- c. Click **Product**, and in the list that appears, select *KACE Systems Management Appliance*.
- d. Click **Start Chat**.

7. **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.

8. **Administrator or System Console only.** Click .

The **Settings > Support** page appears. This page provides resources for troubleshooting system management issues and contacting Quest Support.

9. **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, see [Download and use KACE GO](#).

10. **Administrator or System Console only.** Review information about your KACE System Management Appliance (K1000) installation.

- a. Click .

A dialog box displaying product information appears.

- b. To close it, click **Close**.

11. 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.

i **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://K1000_hostname/admin`. For example, `http://k1000/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 .
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. i NOTE: If you have multiple K1000 or K2000 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

Option	Description
	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 KACE Systems Management Appliance (K1000), 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

K1000 technical specifications describe appliance capacity and requirements for managing devices.

For the latest information about K1000 hardware, requirements for managed devices, and browser requirements for accessing the Administrator Console, see the technical specifications:

- For physical appliances: Go to <https://documents.quest.com/KACE-Systems-Management-Appliance/Technical-Specifications-for-Physical-Appliances>.
- For virtual appliances: Go to <https://documents.quest.com/KACE-Systems-Management-Appliance/Technical-Specifications-for-Virtual-Appliances>.
- For K1000 as a Service: Go to <https://documents.quest.com/KACE-as-a-Service/Technical-Specifications-for-K1000-as-a-Service>.



NOTE: To run Device Actions, you must have the Administrator Console open in Internet Explorer®, because ActiveX® is required to launch these programs on the local device. Other browsers do not support ActiveX.

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 K1000 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 appliance (VK1000), 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 hostname 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 DMZ (demilitarized zone) 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 K1000 as a Service, see the K1000 as a Service Setup Guide. Go to <https://support.quest.com/kace-systems-management-appliance/release-notes-guides>.

1. If you are configuring the physical version of the appliance:
 - a. Install the appliance in its rack and connect a monitor directly to the appliance.
 - b. Connect a network cable to the port indicated:



- c. Power on the appliance.

The Command Line Console login screen appears on the monitor connected to the appliance. The login screen shows the appliance's DHCP network settings.

2. 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.

3. 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://k1000.local/admin`.

The *Software Transaction Agreement* page appears.

4. Accept the agreement.

The *Initial Setup* wizard appears.

5. Verify that you have the information required to configure the appliance, then click **Next**.
6. Review the information on the *System Support Two-Factor Authentication* page that appears, and record the secret key and offline tokens in a secure place, as instructed.
7. 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.

Option	Description
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. i NOTE: If you have multiple K1000 or K2000 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.
8.	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. i NOTE: If you changed the appliance IP address, go to the new address to display the login page.
9.	Log in to the Administrator Console using the login ID admin and the password you chose during initial setup. 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 K1000 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 physical version of the appliance:
 - a. Connect a monitor and keyboard directly to the appliance.
 - b. Connect a network cable to the port indicated:



- c. Power on the appliance.

The Command Line Console login screen appears on the monitor connected to the appliance.

2. 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.
3. At the prompts, enter:

Login: konfig

Password: konfig

4. Choose the language to use for the Command Line Console. Use the up- and down-arrow keys to move between fields.
 5. Configure network settings. See [Changing appliance network settings](#).
- i** **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.
6. 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 K1000 System Administration Console, http://K1000_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**.
 - c. On the *Control Panel*, click **General Settings**.
2. In the top section, provide the following information:

Option	Description
Company Name	Enter the name of your company.
Default Locale	Select the language to use in the Command Line Console, which uses the <code>konfig</code> user account.
Company Email Suffix	Enter the domain from which your users send email. For example: quest.com.
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.
Enable mobile device access	Enable or disable Mobile Device Access to the appliance. Mobile device access enables you to interact with the K1000 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 .
Require organization selection at login	Display the <i>Organization</i> drop-down list on the Administrator Console login page, <code>http://K1000_hostname/admin</code> , where <code>K1000_hostname</code> is the hostname of your appliance. This enables you to choose an organization when you log in. If this option is disabled, the <i>Organization</i> drop-down list is not displayed on the login page, and you can only log in to the Default organization from <code>http://K1000_hostname/admin</code> . 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 <i>fast-switching</i> 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

Option	Description
	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.
Enable linked reporting	Select to allow the generation of reports from Federated (linked) K1000 appliances.

3. In the *Agent* section, view or configure K1000 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 Load Average	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 Load Average is not more than 10.0, and the Last Task Throughput Update time is more than 15 minutes.

4. 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.

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.
Message	Details of the policy, which are displayed below the <i>Title</i> on the login page. Users must agree to the

Option	Description
	terms of the policy before they can log in to the User Console.

6. In the *Reporting* section, specify the password for the reporting system:

Option	Description
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.
User Password	The report user password. This password is used only by the reporting system and MySQL™.

7. 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 [View appliance logs](#).
8. In the *Share with Quest* section, select data sharing options:
- To validate the K1000 product license, Quest collects minimal license-related information, such as the MAC Address of the K1000 appliance, the version of the K1000 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 and share anonymous information with ITNinja.com. 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, and ITNinja uses anonymous data to identify relevant content on http://www.itninja.com for dynamic feeds to the K1000 Administrator Console. ITNinja.com is a community website where IT professionals can share information and research on a wide variety of systems management and deployment topics. The ITNinja feed is a feature that dynamically displays software deployment tips and other contextual information on relevant pages in the K1000 Administrator Console. To enable the ITNinja feed, you need to select Share detailed Usage data.... This setting shares information anonymously with ITNinja. The ITNinja 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 the <i>Software Catalog</i> detail page. Clear this option to prevent the appliance from sharing inventory data with the ITNinja community. However, clearing this option does not remove any information that has already been shared. For more information, contact Quest Support.

9. To use a custom logo in the User Console, select images in the *Logo Overrides* section. Click **Browse** or **Choose File** to select the logo file.



NOTE: You can change the logo in the User Console only; you cannot change the logo in the Administrator Console.

Option	Description
User Console	The logo or other graphic displayed at the top of the 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 <code>http://<K1000_hostname>/user</code> where <code><K1000_hostname></code> is the hostname of your appliance. Follow these guidelines for User Console graphics: • 224 pixels wide by 50 pixels high is the default size. • 104 pixels wide by 50 pixels high stays inside the blue highlight around the Log Out link. • 300 pixels wide by 75 pixels high is the maximum size that does not impact the layout.

Report	This setting controls the logo used when generating System-level reports. Upload a logo or other graphic to be displayed at the top of reports. The graphic must be 201 pixels wide by 63 pixels high as specified in the auto-generated XML layout. To use a different size, adjust the output of the XML report. To see the default report logo and a customized version, refer to the following illustrations.

Figure 1. Default User Console logo

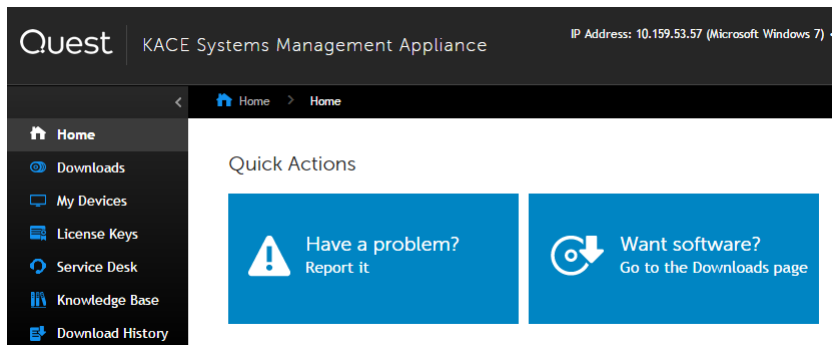


Figure 2. Custom User Console logo

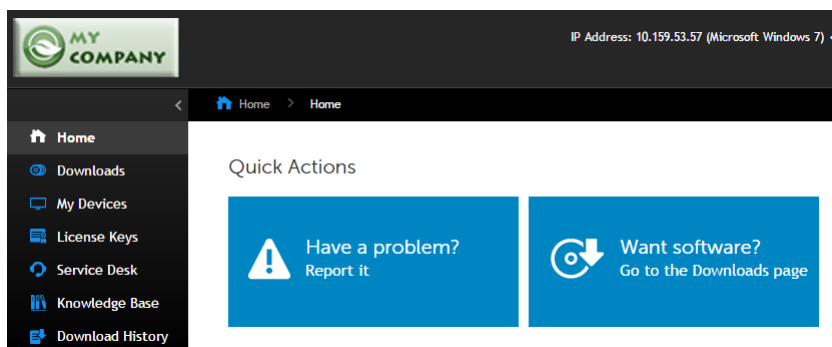


Figure 3. Default report logo

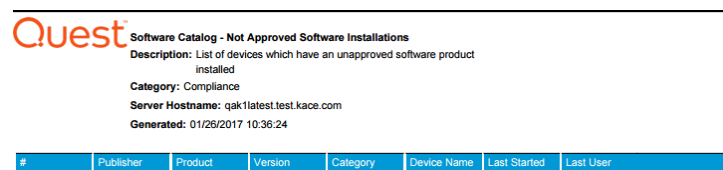


Figure 4. Custom report logo

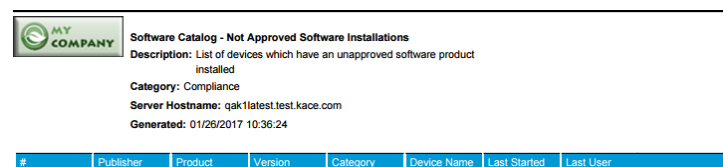


Figure 5. Default Alert logo

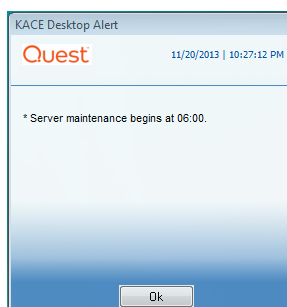
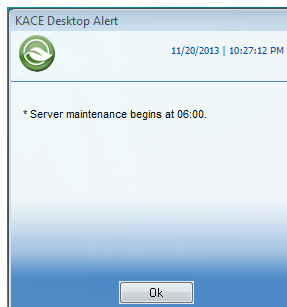


Figure 6. Custom Alert logo



10. Click **Save and Restart Services**.

Related topics

[Configuring locale settings](#)

[Configuring Mobile Device Access](#)

[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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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. 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. <i>Organization Name</i> 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

- 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.
- 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.
 - 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*
 - In the *Data Retention* section, select the options for retaining data in the K1000 appliance database.

Option	Description
Retain Device Uptime Data	The number of months that device uptime information is retained in the K1000 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).
Retain Metering Data	The number of months that metering data is retained in the K1000 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.

Option	Description
Retain Uncataloged data in the Software Catalog	Whether to retain information about Uncataloged applications in the K1000 appliance database. Uncataloged applications are executables that are in the K1000 inventory but that do not appear in the Software Catalog, and the K1000 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 K1000 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.

8. In the *Asset Archive* section, type the number of days that you want to keep the assets marked for archiving, before actually archiving them. The default value is 3 days.
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**, then 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-]."

If you are using Internet Explorer, you can define any valid statement to perform a task on a remote device, then assign a name to it to use the next time you want to perform that task. For example, you can enter the statement, `ping.exe -t KACEHOSTIP` and name it Ping. A valid statement is a maximum of 150 characters, and the name that you assign to it must be any printable character of up to 20 characters. For information about running Device Actions, see [Run actions on devices](#).

i **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.

NOTE: To run Device Actions, you must have the Administrator Console open in Internet Explorer, because ActiveX is required to launch these programs on the local device. Other browsers do not support ActiveX. See <https://support.quest.com/kb/148787>.

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

Use this setting with caution. It is usually better to test patch actions on a limited number of devices, and to limit patch actions to selected devices or device labels. This limitation ensures that patch actions are applied appropriately.

i **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. To use a custom logo in the User Console, select images in the *Logo Overrides* section.

i **NOTE:** You can change the logo in the User Console only; you cannot change the logo in the Administrator Console.

Option	Description
User Console	The logo or other graphic displayed at the top of the User Console. Follow these guidelines for graphics: 224 pixels wide by 50 pixels high is the default size. 104 pixels wide by 50 pixels high stays inside the blue highlight around the Log Out link. 300 pixels wide by 75 pixels high is the maximum size that does not impact the layout. To see the default login page and a customized version, see Configure appliance General Settings with the Organization component enabled.
Report	This setting controls the logo used when generating reports for the selected organization. Upload a logo or other graphic to be displayed at the top of reports. The graphic must be 201 pixels wide by 63 pixels high as specified in the auto-generated XML layout. To use a different size, adjust the output of the XML report. To see the default report logo and a customized version, see Configure appliance General Settings with the Organization component enabled.

Option	Description
	If the Organization component is enabled on your appliance, you can specify different logos for the reports produced for each organization and for the System. For information about using custom logos at the System level, see Configure appliance General Settings with the Organization component enabled.
Agent Alert	Upload a logo or graphic to be used in pop-up messages on Agent-managed devices. These pop-ups include snooze dialogs, installation progress messages, alert messages, and message windows created by scripts. After you upload a graphic, it becomes available to managed devices the next time they check in to the appliance. Graphics for pop-up messages must be in BMP format with a maximum color depth of 256 and a size of 100 pixels wide by 38 pixels high. To see the default alert logo and a customized version, see Configure appliance General Settings with the Organization component enabled. You can customize Alert message text and options as well. See Adding and editing scripts.

13. Click **Save and Restart Services**.

14. 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](#).

- Go to the Admin-level *General Settings* page:
 - Log in to the K1000 Administrator Console, http://K1000_hostname/admin.
 - On the left navigation bar, click **Settings**, then click **General Settings**.
- 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.

Option	Description
Company Email Suffix	Enter the domain from which your users send email. For example: example.com.
Enable mobile device access	Enable or disable Mobile Device Access to the appliance. Mobile device access enables you to interact with the K1000 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.
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.

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 K1000 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 <i>Client Drop Size</i> filter determines whether files uploaded to the organization's Client Drop location are displayed on the <i>Upload and Associate Client Drop File</i> list on the <i>Software Detail</i> page. For example, if the Client Drop Size filter is set to 1 GB, the <i>Upload and Associate Client Drop File</i> 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 <i>Software Detail</i> page and saved.

Options	Description
	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 <i>Backup Settings</i> page within five minutes. See Copy files to the K1000 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 <code>http://<K1000_hostname>/user</code> where <code><K1000_hostname></code> 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.
Message	Details of the policy, which are displayed below the <i>Title</i> 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 *Share With Quest* section, specify data sharing options.



NOTE: To validate the K1000 product license, Quest collects minimal license-related information, such as the MAC Address of the K1000 appliance, the version of the K1000 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

Option	Description
	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 and share anonymous information with ITNinja.com. 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, and ITNinja uses anonymous data to identify relevant content on http://www.itninja.com for dynamic feeds to the K1000 Administrator Console. ITNinja.com is a community website where IT professionals can share information and research on a wide variety of systems management and deployment topics. The ITNinja feed is a feature that dynamically displays software deployment tips and other contextual information on relevant pages in the K1000 Administrator Console. To enable the ITNinja feed, you need to select Share detailed Usage data.... This setting shares information anonymously with ITNinja. The ITNinja feed is available only if Share Summary Usage Data... is selected, 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 <i>Software Catalog</i> detail page. Clear this option to prevent the appliance from sharing inventory data with the ITNinja community. However, clearing this option does not remove any information that has already been shared. For more information, contact Quest Support.

8. 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 <code>konfig</code> user account.
9.	In the <i>Ignore Client IP Address Settings</i> 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.
10.	In the <i>License Usage Warning Configurations</i> 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 <i>Dashboard</i> .
11.	In the <i>Update Reporting User Password</i> section, provide the password of the account required to run reports on the organization. You cannot change the <i>Database Name</i> or the <i>Report Username</i> .
12.	In the <i>Data Retention</i> section, 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
Retain 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).
Retain Metering Data	The number of months that metering data is retained in the K1000 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 K1000 appliance database. Uncataloged applications are executables that are in the K1000 inventory but that do not appear in the Software Catalog, and the K1000 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 K1000 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

Option	Description
	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.

13. In the *Device Actions* section, click **Add New Action**, then 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-]."

If you are using Internet Explorer, you can define any valid statement to perform a task on a remote device, then assign a name to it to use the next time you want to perform that task. For example, you can enter the statement, `ping.exe -t KACEHOSTIP` and name it Ping. A valid statement is a maximum of 150 characters, and the name that you assign to it must be any printable character of up to 20 characters. For information about running Device Actions, see [Run actions on devices](#).

i **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.

NOTE: To run Device Actions, you must have the Administrator Console open in Internet Explorer, because ActiveX is required to launch these programs on the local device. Other browsers do not support ActiveX. See <https://support.quest.com/kb/148787>.

14. To use a custom logo in the User Console, select images in the *Logo Overrides* section.

i **NOTE:** You can change the logo in the User Console only; you cannot change the logo in the Administrator Console.

Option	Description
User Console	The logo or other graphic displayed at the top of the User Console. Follow these guidelines for graphics: • 224 pixels wide by 50 pixels high is the default size. • 104 pixels wide by 50 pixels high stays inside the blue highlight around the Log Out link. • 300 pixels wide by 75 pixels high is the maximum size that does not impact the layout. To see the default login page and a customized version, see Configure appliance General Settings with the Organization component enabled.
Report	This setting controls the logo used when generating reports for the selected organization. Upload a logo or other graphic to be displayed at the top of reports. The graphic must be 201 pixels wide by 63 pixels high as specified in the auto-generated XML layout. To use a different size, adjust the output of the XML report. To see the default report logo and a customized version, see Configure appliance General Settings with the Organization component enabled. If the Organization component is enabled on your appliance, you can specify different logos for the reports produced for each organization and for the System. For information about using custom logos at the System level, see Configure appliance General Settings with the Organization component enabled.
Agent Alert	Upload a logo or graphic to be used in pop-up messages on Agent-managed devices. These pop-ups include snooze dialogs, installation progress messages, alert messages, and message windows created by scripts. After you upload a graphic, it becomes available to managed devices the next time they check in to the appliance. Graphics for pop-up messages must be in BMP format with a maximum color depth of 256 and a size of 100 pixels wide by 38 pixels high. To see the default alert logo and a customized version, see Configure appliance General Settings with the Organization component enabled. You can customize Alert message text and options as well. See Adding and editing scripts.

15. 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 K1000 Administrator Console, `http://K1000_hostname/admin`, then click **Settings**.
 - If the Organization component is enabled on the appliance, log in to the K1000 System Administration Console, `http://K1000_hostname/system`, or select **System** in the drop-down list in the top-right corner of the page, then click **Settings**.

2. Click **Date and Time Settings**.

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 <i>Server</i> field. • Manually configure date and time. Set the appliance clock manually. Specify the time and date in the drop-down lists. The <i>Hour</i> drop-down list uses a 24-hour clock format.
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: <code>time.example.com</code> .

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.

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
443	(Required) Used for SSL access. Devices use this port when they check in to the appliance using HTTPS.	Inbound to the appliance
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 K1000 database using Microsoft Access® or Excel®.	Inbound to the appliance

Port	Use	Direction
52230	(Required) Used for AMP (Agent Messaging Protocol) communications. The appliance listens on this port for communications from devices on which the K1000 Agent is installed.	Inbound to the appliance
 TIP: On a number keypad, this port number spells out KACE+0.		

- 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 K1000 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 K1000 Agent provisioning. See Provisioning the K1000 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 K1000 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 K1000 appliance

To complete patch downloads, access product information, and interact with Quest Support, firewall, DNS server, and proxy server settings must allow the K1000 appliance to access domains on both port 80 and port 443.

- Ensure that the K1000 Administrator Console has links to the following websites:

Website	Description
https://kace.influitive.com/users/sign_in	KACEKconnect
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

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.

Changing 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 and physical versions of the appliance, network settings are initially configured during the first login to the Administrator Console or the Command Line Console. See [Changing 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 K1000 as a Service Setup Guide. Go to <https://support.quest.com/k1000-as-a-service/release-notes-guides>.

Changing 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.

- Go to the appliance *Control Panel*:
 - If the Organization component is not enabled on the appliance, log in to the K1000 Administrator Console, http://K1000_hostname/admin, then click **Settings**.
 - If the Organization component is enabled on the appliance, log in to the K1000 System Administration Console, http://K1000_hostname/system, or select **System** in the drop-down list in the top-right corner of the page, then click **Settings**.
- Click **Network Settings** to display the *Network Settings* page.
- 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

Option	Description
	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.
Autogenerate Server Name	Select this check box to enable the system to generate the K1000 web server name using this format: Hostname.Domain. For example: k1000.example.com. Clear this check box to enter a custom web server name.
Configure Network Using DHCP	Use DHCP (Dynamic Host Configuration Protocol) to automatically obtain the IP address and other network configuration information for the appliance.
Configure Network Manually	Specify the IP address, domain, subnet mask, default gateway, and DNS settings for the appliance manually.
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, <code>example.com</code> .
Subnet Mask	Enter the subnet (network segment) that the appliance is on. The default is <code>255.255.255.0</code> .
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 hostnames.
Secondary DNS	(Optional) Enter the IP address of the secondary DNS server the appliance uses to resolve hostnames.
Network Speed	If you are configuring a physical K1000, select the speed of your network. This should match the setting of your LAN switch. If you select Auto-negotiate , the system determines the best value automatically, provided that the LAN switch supports auto-negotiation.

4. **Optional:** To set a proxy server, select the **Enable Proxy Server** in the *Proxy Configuration* section, 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.

5. **Optional:** To use an external SMTP server, select **Enable SMTP Server** in the *Email Configuration* section, 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 <code>[10.10.10.10]</code> .
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 <code>your_account_name@gmail.com</code> .
Password and Confirm Password	Enter the password of the specified server account.
Enable Service Desk POP3 Server	Select this check box to use POP3 for Service Desk ticket email. After POP3 is enabled, you can specify the POP3 server settings on Service Desk <i>Queue Detail</i> pages. See Configure ticket queues .

6. To test the email service, use the *email sending* test in *Diagnostic Utilities*.
See [Using Troubleshooting Tools](#).
7. Click **Save**.

The appliance reboots. Total reboot downtime is one to two minutes, provided that the changes result in a valid configuration.

8. 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 K1000 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 K1000 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 K1000 Administrator Console, `http://K1000_hostname/admin`, then click **Settings**.
 - If the Organization component is enabled on the appliance, log in to the K1000 System Administration Console, `http://K1000_hostname/system`, or select **System** in the drop-down list in the top-right corner of the page, then click **Settings**.
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 K1000 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.
Gateway	Enter the IP address of the router that routes traffic between the K1000 appliance and the destination network.

5. Click **Save** 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 whitelist hosts

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



NOTE: After an IP address or domain name is whitelisted (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 K1000 Administrator Console, `http://K1000_hostname/admin`, then click **Settings**.
 - If the Organization component is enabled on the appliance, log in to the K1000 System Administration Console, `http://K1000_hostname/system`, or select **System** in the drop-down list in the top-right corner of the page, then click **Settings**.

2. Click **Access Control List** 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 whitelist 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. A whitelist of users who can log in to <code>http://K1000_hostname/admin</code>. • userui: This is the User Console. A whitelist of users who can log in to <code>http://K1000_hostname/user</code>. • systemui: This is the System Administration Console (available only if the Organization component is enabled on the appliance). A whitelist of users who can log in to <code>http://K1000_hostname/system</code>.
IP Address/Domain Name	Provide the address to be allowed. This can be either: • A domain name (full or partial) • An IP address (full or partial)
Subnet Mask/CIDR	(Optional) 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.

- 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>.



NOTE: Saving changes to security settings reboots 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.

- Go to the appliance *Control Panel*:
 - If the Organization component is not enabled on the appliance, log in to the K1000 Administrator Console, http://K1000_hostname/admin, then click **Settings**.
 - If the Organization component is enabled on the appliance, log in to the K1000 System Administration Console, http://K1000_hostname/system, or select **System** in the drop-down list in the top-right corner of the page, then click **Settings**.
- Click **Security Settings** to display the *Security Settings* page.
- In the top section, 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 webserver compression	Enable the appliance to compress web pages. This compression reduces the time it takes to load Administrator Console and User Console pages in the browser.
Enable inventory API access	Use API (application programming interface) commands to update inventory information. If you want to upload device information using the API, you must enable this setting. See Adding devices manually using the API .
API Password	The password for API (application programming interface) access to inventory information. This password is used only for API access and it does not need to match any other passwords.
Enable SNMP READ access	Enable unidirectional (read-only) SNMP access to managed devices on the network.

Option	Description
SNMP Community String	The SNMP community string that enables read-only SNMP access. The default value is public.
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 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

Option	Description
	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.
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 <i>Security Settings</i> page, under <i>MIB Files</i>, in the <i>Upload MIB</i> 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 <i>Security Settings</i> page. If you do not want to validate the contents of the MIB file, select the Skip MIB validation check box.
Enable Secure backup files	Require username and password authentication for access to K1000 backup files, which are available by entering a URL in a browser.

Option	Description
	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 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 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 webserver diagnostic graphs	Enable the K1000 to display usage information for the appliance web server, such as Apache access and volume statistics. This information appears in graphs in the System Performance log. If this option is cleared, the graphs are not updated. See View appliance logs .
Enable database access	Enable users to run reports on the K1000 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.
Enable secure database access (SSL)	Enable SSL access to the database and access additional SSL options.
4. Optional: In the <i>Appliance Encryption Key</i> 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 Support. The time stamp shows the time the key was generated. 5. In the <i>Single Sign On</i> section, specify authentication settings:	
Option	Description
Disabled	Prevent the K1000 from using single sign on. Single sign on enables users who are logged on to the domain to access the K1000 Administrator Console

Option	Description
	and User Console without having to re-enter their credentials on the K1000 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 .
Quest Identity Broker	Use Quest Identity Broker (QIB) for authentication. QIB is a cloud-based single sign on (SSO) solution that allows users to securely authenticate using various identity providers. See Using Quest Identity Broker for single sign on .

6. In the **Samba Share Settings** section, 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.
For appliances without the Organization component: Enable File Sharing	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.
Require NTLMv2 to appliance file shares	Enable NTLMv2 authentication for the K1000 files shares. When this is enabled, managed devices connecting to the K1000 File Shares require support for NTLMv2 and they authenticate to the K1000 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 K1000 Agent. See Manually deploying the K1000 Agent .
Require NTLMv2 to off-board file shares	Force certain K1000 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 configurations are more common and this option is usually disabled. Enabling this option

Option	Description
	enables the client ntlmv2 auth option for Samba client functions.

7. **Optional:** In the *SSL* section, 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. Quest recommends that you enable port 80 access because, by default, the Agent installers contact the appliance using port 80. Agents switch to SSL over port 443 after they acquire the server configuration. If you disable port 80 access, contact Quest Support to adjust the Agent deployment scripts to handle SSL.
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 8.
Enable SSL v3	(Displayed only if Enable SSL is selected). Enable managed devices to connect to the appliance using SSLv3, which is an older version of SSL. Because of vulnerabilities associated with SSLv3, this setting should be enabled only if you have Agent-managed devices that are running version 6.3 or earlier of the K1000 Agent. SSLv3 is disabled by default on new K1000 appliances. For more information about

Option	Description
	SSLv3 vulnerabilities, see https://support.quest.com/kb/136510 .
8.	To load an SSL certificate, do one of the following: - Click SSL Certificate Form to generate certificate requests or load self-signed certificates. See Generate an SSL certificate. - If you have an SSL certificate and private key, click Browse or Choose File in the <i>SSL Private Key File</i> or <i>SSL Certificate File</i> fields to select them. These files must be in Privacy Enhance Mail (PEM) format, similar to those used by Apache-based web servers. - Select Enable Intermediate SSL Certificate to enable and upload intermediate SSL certificates, which are signed certificates provided by certificate issuers as proxies for root certificates. Intermediate SSL certificates must be in PEM format. - If your certificate is in PKCS-12 format, click Browse or Choose File in the <i>PKCS-12 File</i> field to select it, then enter the password for the file in the <i>Password for PKCS-12 file</i> field.
9.	In the <i>Secure Attachments in Service Desk</i> 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 K1000 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.
10.	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 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 K1000 Administrator Console and User Console without having to re-enter their login credentials each time.

Before you connect the K1000 to an Active Directory server, verify that:

- Network and DNS settings are configured to enable the K1000 appliance to access the Active Directory server. See [Changing appliance network settings](#).
 - The time settings on the Active Directory server match the time settings on the K1000 appliance. For information on setting the time on the K1000 appliance, see [Configure appliance date and time settings](#).
- Go to the appliance *Control Panel*:
 - If the Organization component is not enabled on the appliance, log in to the K1000 Administrator Console, `http://K1000_hostname/admin`, then click **Settings**.
 - If the Organization component is enabled on the appliance, log in to the K1000 System Administration Console, `http://K1000_hostname/system`, or select **System** in the drop-down list in the top-right corner of the page, then click **Settings**.
 - In the *Single Sign On* section of the *Security Settings* page, select **Active Directory**, then provide the following information:

Option	Description
Domain	The hostname of the domain of your Active Directory® server, such as example.com.
Username	The username 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.

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 K1000 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 K1000 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 and Restart Services**.

When users are logged in to devices that are joined to the Active Directory domain, they can access the K1000 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 K1000 user account. See [Add or edit System-level user accounts](#).



NOTE: To use single sign on with Internet Explorer and Firefox browsers, users must configure their browser settings to use the appropriate authentication. See [Configuring browser settings for single sign on](#).

Configure Quest Identity Broker as the single sign on method

You can use Quest Identity Broker (QIB) to enable users to log in to the Administrator Console and User Console using credentials from third-party identity providers, such as your organization's Identity Provider and Microsoft Azure™ Active Directory.

QIB can be enabled for a single organization only. If the Organization component is enabled on your appliance, you can enable QIB for the default organization only. To use single sign on with multiple organizations, use Active Directory authentication. 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 K1000 Administrator Console, `http://K1000_hostname/admin`, then click **Settings**.
 - If the Organization component is enabled on the appliance, log in to the K1000 System Administration Console, `http://K1000_hostname/system`, or select **System** in the drop-down list in the top-right corner of the page, then click **Settings**.
2. In the *Single Sign On* section of the *Security Settings* page, select **Quest Identity Broker**, then provide the following information:

Option	Description
Web Server Assertion Consuming Service URL	The URL associated with your K1000 appliance. This URL is created automatically during appliance configuration. To enable QIB, contact Quest Support and provide this URL to obtain the Relying Party Identifier for your appliance.  IMPORTANT: If you enable or disable SSL for the appliance, this URL changes. As a result, you need to provide this URL to Quest Support and obtain a new <i>Relying Party Identifier</i> any time SSL settings are changed.
Relying Party Identifier	A unique identifier provided by Quest Support to enable QIB. This identifier determines which identity provider, such as your organization's Identity Provider or Microsoft Azure Active Directory, is used for authentication. You must provide your <i>Web Server Assertion Consuming Service URL</i> to Quest Support to receive this identifier.
Automatically approve user requests	Users requesting single sign on access are automatically granted access to the K1000 User Console if they are authenticated by the third-party identity provider. Accounts for these users are created automatically on the K1000 appliance.
Manually approve user requests	Administrators must approve access requests before users can access the K1000 Administrator Console or User Console. When users attempt to sign on to the K1000 using third-party credentials, the K1000 creates approval requests. When administrators log in to the Administrator Console, a notification stating that approval requests are pending appears on the information bar at the top of the <i>Dashboard</i> page. When administrators approve requests, user accounts are created on the K1000 appliance and

Option	Description
	users can access the K1000 Administrator Console or User Console.

- To specify identity provider settings, click **Advanced Settings**.



NOTE: Do not change these settings unless directed to do so by Quest Support.

Option	Description
Quest Identity BrokerURL	The URL of the identity provider.
Quest Identity BrokerIdentifier	The unique identifier of the identity provider.
Quest Identity BrokerCertificate	The certificate used to verify communications with the identity provider.

- Click **Save and Restart Services**.

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.

- Go to the appliance *Control Panel*:
 - If the Organization component is not enabled on the appliance, log in to the K1000 Administrator Console, `http://K1000_hostname/admin`, then click **Settings**.
 - If the Organization component is enabled on the appliance, log in to the K1000 System Administration Console, `http://K1000_hostname/system`, or select **System** in the drop-down list in the top-right corner of the page, then click **Settings**.
- Click **Security Settings** to display the *Security Settings* page.
- In the SSL section, click **Enable SSL**.
Additional SSL options are displayed.
- 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**.
- In the *Configure* section, 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.

Option	Description
State or Province Name	The name of your state or province.
Country Name	The name of your country.

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 K1000 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 Agent settings

Agent settings determine the port and security settings used by the K1000 Agent. These settings are specific to the Agent infrastructure and do not affect other appliance configuration settings or runtime operations.



NOTE: Changing Agent settings temporarily interrupts communications between the appliance and the Agents installed on managed devices, so use caution. For more information, contact Quest Support at <https://support.quest.com/contact-support>.

About Konea

Konea is a component that enables the communication between the K1000 Agent, which is installed on Agent-managed devices, and the K1000 appliance.

Konea provides optimized real-time communications for systems-management operations.

Configure Agent settings

You can configure K1000 Agent settings on the appliance. These settings are System-level settings. If the Organization component is enabled on the appliance, Agent settings 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 K1000 Administrator Console, `http://K1000_hostname/admin`, then click **Settings**.
 - If the Organization component is enabled on the appliance, log in to the K1000 System Administration Console, `http://K1000_hostname/system`, or select **System** in the drop-down list in the top-right corner of the page, then click **Settings**.
2. Click **Agent Settings** to display the *Agent Settings* page.
3. Specify the following settings:

Option	Description
Enable Pre-7.0 Agent Support	Select this option if you want to enable the appliance to communicate with K1000 Agents version 6.4.x and earlier.
Enable SSL	(Read only) Agent SSL settings are controlled by the appliance security settings. See Configure security settings for the appliance .
Require SSL	Configure the K1000 Agent to use secure connections. SSL (Secure Sockets Layer) connections allow the Agent to establish encrypted link to ensure that all data passed from and to the Agent remains private and integral. i IMPORTANT: After changing this setting, you must restart the Agent manually using the AMPTools restart command, to ensure these changes are reflected on the Client machine.
Verify SSL Certificates	Verify SSL certificates prior to establishing a connection. An SSL certificate contains a public key used to encrypt and information about its owner identity. i IMPORTANT: After changing this setting, you must restart the Agent manually using the AMPTools restart command, to ensure these changes are reflected on the Client machine.
Enable server debug	Enable different levels of server debugging or logging to the server's log file. See Troubleshooting appliance issues .
Compress Server Uploads	Indicate if you want to compress the files uploaded by the appliance. This can help the overall Agent performance.

Option	Description
Disable Duplicate Device Detection	Disable the process that detects duplicate devices in the inventory. In some unique cases, this process is too aggressive and needs to be disabled.  CAUTION: Do not select this check box unless instructed by Quest Support.
Process Timeouts	Specify the amount of time after which the Agent suspends a running process.
File Transfer Timeout	Specify the amount of time after which the Agent suspends a file transfer process.
Read/Write Connection Timeout	The length of time that the messaging protocol processor waits before determining that K1000 Agents have disconnected.  IMPORTANT: Do not adjust this parameter unless you have discussed the ramifications with Quest Support. The messaging protocol processor monitors K1000 Agent connections, and it assumes that Agents are connected while it waits for responses. If Agents do not respond within the timeout period, the processor concludes that they have disconnected. For appliances that have fewer than 1,500 managed devices, a 40-second timeout would be appropriate. In environments with network limitations, or for appliances with more than 1,500 managed devices, a timeout of 90-120 seconds might be better. The minimum timeout is 30 seconds, and the maximum is 180 seconds.
Disable duplicate device detection	Prevent the Agent from detecting duplicate devices. In some unique cases, this duplicate detection is too aggressive and needs to be disabled.  IMPORTANT: Do not select this setting unless you have discussed the ramifications with Quest Support.
Connected Agents	The number of K1000 Agents currently connected to the appliance.

- Click **Save and Restart Services** to save the settings and restart the messaging protocol processor.
- To restart the messaging protocol processor without saving settings, click **Restart services**.



NOTE: Restarting the processor does not restart the K1000 appliance.

Related topics

[Configure security settings for the appliance](#)

[Troubleshooting appliance issues](#)

Optional: Configure Agent communication settings, which determine the frequency at which Agents communicate with the appliance. See [Managing Agent communications](#).

Configuring session timeout and auto-refresh 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 K1000 Administrator Console, `http://K1000_hostname/admin`, then click **Settings**.
 - If the Organization component is enabled on the appliance, log in to the K1000 System Administration Console, `http://K1000_hostname/system`, or select **System** in the drop-down list in the top-right corner of the page, then click **Settings**.
2. Click **General Settings** to display 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 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**.

Set auto-refresh properties

You can set auto-refresh to show the latest results on list pages, or you can turn auto-refresh off so that pages are refreshed only when they are reloaded in the browser.

Setting the refresh frequency to 30 seconds or less is useful for pages that display status, such as the *Provisioning Results* page and the *Devices* page. On other pages, such as the *Software Catalog* page, a longer refresh rate, or turning auto refresh off, might be more appropriate, because these pages can take longer to refresh.

Auto-refresh settings are page-specific and user-specific. The settings for each page and each user account are separate.

1. Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the 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 information to be refreshed, such as **Inventory > Devices**.
The *Devices* page appears.
3. In the **Auto Refresh** drop-down list, above the list to the right, select a frequency.
The list is updated according to the selected frequency.
4. Click the **Refresh** button in the top-right corner of the page to refresh the page immediately.
5. **Optional:** In the **Auto Refresh** drop-down list, above the list to the right, select OFF to turn off auto-refresh.
Auto-refresh is disabled. Information on the page is no longer updated automatically.

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.

To see the locale options available through your license agreement, click the Help button (🔗) the top-right corner of the page, then click **About K1000** at the bottom of the *Help* panel. Supported languages are listed in the *Language Support* section. See [View the K1000 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 K1000 Administrator Console, `http://K1000_hostname/admin`, then click **Settings**.
 - If the Organization component is enabled on the appliance, log in to the K1000 System Administration Console, `http://K1000_hostname/system`, or select **System** in the drop-down list in the top-right corner of the page, then click **Settings**.
2. Click **General Settings** 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.
 - b. Click **Save and Restart Services** 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 and Restart Services**.

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

Configure locale settings for the User Console

The KACE Systems Management Appliance (K1000) supports several locales. The Administrator Console, System 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 KACE Systems Management Appliance (K1000), 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 K1000 Administrator Console, `http://K1000_hostname/admin`, then click **Settings**.
 - If the Organization component is enabled on the appliance, log in to the K1000 System Administration Console, `http://K1000_hostname/system`, or select **System** in the drop-down list in the top-right corner of the page, then click **Settings**.
2. Click **Localization** 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*, click **Export Locale**, and select the locale from which you want to translate. 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 https://www.gnu.org/software/gettext/manual/html_node/PO-Files.html
 - **PO File Format:** https://www.gnu.org/software/trans-coord/manual/web-trans/html_node/PO-Editors.html
 - **Additional information about editing PO (portable object) files with editor suggestions:** https://www.gnu.org/software/trans-coord/manual/web-trans/html_node/PO-Editors.html
 - a. Under *Import Gettext PO (portable object) File*, 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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* section, select a locale in the *Organization Locale* drop-down list.
 - b. Click **Save and Restart Services** 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 and Restart Services**.

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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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.

Configure data sharing preferences

Configure data sharing preferences at the System level. Data sharing preferences determine how much of your K1000 information is shared with Quest. In addition, data sharing preferences determine whether information from ITNinja is displayed in the Administrator Console.

To validate the K1000 product license, Quest collects minimal license-related information, such as the MAC Address of the K1000 appliance, the version of the K1000 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 K1000 Administrator Console, http://K1000_hostname/admin, then click **Settings**.
 - If the Organization component is enabled on the appliance, log in to the K1000 System Administration Console, http://K1000_hostname/system, or select **System** in the drop-down list in the top-right corner of the page, then click **Settings**.
2. Click **General Settings** to display the *General Settings* page.
3. In the *Share With Quest* section, 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.

Option	Description
Share detailed usage data...	(Recommended) Share detailed information with Quest and share anonymous information with ITNinja.com. 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, and ITNinja uses anonymous data to identify relevant content on http://www.itninja.com for dynamic feeds to the K1000 Administrator Console. ITNinja.com is a community website where IT professionals can share information and research on a wide variety of systems management and deployment topics. The ITNinja feed is a feature that dynamically displays software deployment tips and other contextual information on relevant pages in the K1000 Administrator Console. To enable the ITNinja feed, you need to select Share detailed Usage data.... This setting shares information anonymously with ITNinja. The ITNinja 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 <i>Software Catalog</i> detail page. Clear this option to prevent the appliance from sharing inventory data with the ITNinja community. 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 K1000 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 K1000 Administrator Console, `http://K1000_hostname/admin`, then click **Settings**.
 - If the Organization component is enabled on the appliance, log in to the K1000 System Administration Console, `http://K1000_hostname/system`, or select **System** in the drop-down list in the top-right corner of the page, then click **Settings**.
2. Click **General Settings** 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 <i>Title</i> 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 \(SSO\)](#).

Configuring Mobile Device Access

Mobile Device Access enables you to interact with the K1000 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 K1000 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 K1000 Administrator Console, http://K1000_hostname/admin, then click **Settings**.
 - If the Organization component is enabled on the appliance, log in to the K1000 System Administration Console, http://K1000_hostname/system, or select **System** in the drop-down list in the top-right corner of the page, then click **Settings**.
2. Click **General Settings** to display the *General Settings* page.
3. In the top section, select the *Enable mobile device access* check box.
4. 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](#).

5. Click **Save and Restart Services**.

Mobile Device Access is enabled on the appliance. Before users can access the K1000 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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
K1000 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 K1000 appliance. To use this setting, SSL must be enabled on the K1000 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-k1000-systems-management-appliance/>.

Related topics

[Configure email triggers](#)

[Configure security settings for the appliance](#)

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 K1000 Administrator Console, `http://K1000_hostname/admin`, then click **Settings**.
 - If the Organization component is enabled on the appliance, log in to the K1000 System Administration Console, `http://K1000_hostname/system`, or select **System** in the drop-down list in the top-right corner of the page, then click **Settings**.
2. Click **General Settings** to display the *General Settings* page.
3. In the top section, 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 K1000 Administrator Console, `http://K1000_hostname/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 and Restart Services**.

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 K1000 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 multiple Quest KACE K1000 or K2000 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 K2000 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 K1000 Administrator Console, `http://K1000_hostname/admin`, then click **Settings**.
 - If the Organization component is enabled on the appliance, log in to the K1000 System Administration Console, `http://K1000_hostname/system`, or select **System** in the drop-down list in the top-right corner of the page, then click **Settings**.
2. Click **Link Settings** 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 K1000 appliances. For K2000 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 K1000 Administrator Console, `http://K1000_hostname/admin`, then click **Settings**.
 - If the Organization component is enabled on the appliance, log in to the K1000 System Administration Console, `http://K1000_hostname/system`, or select **System** in the drop-down list in the top-right corner of the page, then click **Settings**.
2. Click **Linked Appliances** to display the *Linked Appliances* page.

 **NOTE:** If appliance linking is not enabled, you are redirected to the *Linked Appliance Enablement* page.
3. Select **Choose Action > New** 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 K1000 appliances, 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 K1000 Administrator Console, `http://K1000_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.
 - a. 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**.

- b. Click **Save**.



IMPORTANT: To enable linked reporting, you must assign the Administrator role to each linked appliance.

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 K1000. For K2000 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 K1000 Administrator Console, `http://K1000_hostname/admin`, then click **Settings**.
 - If the Organization component is enabled on the appliance, log in to the K1000 System Administration Console, `http://K1000_hostname/system`, or select **System** in the drop-down list in the top-right corner of the page, then click **Settings**.
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 K1000 appliance.

About history settings

The K1000 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 System-level settings history subscriptions with the Organization component enabled](#).

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 K1000 System Administration Console, http://K1000_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 System-level settings history subscriptions with the Organization component enabled](#)

Configure System-level settings history subscriptions with the Organization component enabled

If the Organization component is enabled on your appliance, you can configure settings history subscriptions at the System level.

For information about organization-level history settings, see [Managing settings history](#).

1. Go to the *Settings History Configuration* page:
 - a. Log in to the K1000 System Administration Console, http://K1000_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. On the *History Panel* in the *Subscriptions* section, click **Settings**.
2. 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.
3. 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**.
4. Click **Save**.

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 K1000 Administrator Console, `http://K1000_hostname/admin`, then click **Settings**.
 - If the Organization component is enabled on the appliance, log in to the K1000 System Administration Console, `http://K1000_hostname/system`, or select **System** in the drop-down list in the top-right corner of the page, then click **Settings**.
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 K1000 Administrator Console, `http://K1000_hostname/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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.

i **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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the 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 **Advanced Search** tab above the list on the right to display the *Advanced Search* 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.

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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization 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**.
 - 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	(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.

Option	Description
	 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	(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.
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 <i>Label Group</i> 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 <i>Licenses</i> . 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](#)

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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization 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. 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the 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.

In version 6.4 of the K1000, however, 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization 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. 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.
 - 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 XP or Windows 7 that do not have the McAfee® VirusScan® application installed.

The following are the three Smart Labels created in this example:

- The first Smart Label, *WinXP7*, is applied to devices that have Windows XP or Windows 7 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, *WinXP7MissingVirusScan*, is applied to devices that have both the *WinXP7* 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the 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**.
- 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 XP operating system:
Operating System: Name | contains | Windows XP
- d. With **AND** selected in the operator drop-down list, click **Add Line**, then specify the criteria required for the Windows 7 operating system:
Operating System: Name | contains | Windows 7
- e. In the *Choose label* drop-down list, type a name for the label, such as WinXP7, 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 *WinXP7* Smart Label applied:
Device Identity Information: Label Names | = | WinXP7
 - 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 WinXP7MissingVirusScan, 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 **Smart Labels**.
 - 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 *WinXP7* 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 row:
- g. In the *Order* column, type 1, then click **Save**.
- h. Click the **Edit** button at the far right in the *WinXP7MissingVirusScan* label row:
- i. In the *Order* column, type 2, then click **Save**.
- j. Click **Save** at the bottom of the list.

The *WinXP7* label and the *MissingVirusScan* label are set to run before the *WinXP7MissingVirusScan* label. This ensures that Windows XP and 7 devices that are missing the VirusScan application are labeled before the *WinXP7MissingVirusScan* 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization 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, 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.
 - 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization 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**.
 - 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 <i>Labels</i> list. Type a name such as All Ticket Owners.
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 XP server 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 XP servers 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.

- Go to the *Patch Catalog* list:
 - Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
 - On the left navigation bar, click **Security**.
 - On the *Patch Management* panel, click **Catalog**.
- Click the **Smart Label** tab above the list on the right.

The *Smart Label* panel appears.

The screenshot shows the 'Smart Label' configuration panel. At the top, there are tabs for 'Choose Action', 'Advanced Search', 'Smart Label' (selected), 'Notification', and a settings icon. The 'Smart Label' section contains two criteria rows. The first row has a dropdown for 'Name', a 'contains' operator, a text field with 'Windows', an 'AND' dropdown, and 'Add Line' and 'Add Group' buttons. The second row has a dropdown for 'Disk % Capacity', a '>' operator, a text field with '95', an 'AND' dropdown, and 'Add Line' and 'Add Group' buttons. Below these rows is a 'Choose label:' dropdown, 'Test' and 'Save' buttons, and a 'Metering Enabled' checkbox.

- Specify Smart Label criteria:
 - Specify criteria that identify active patches:
`Patch Listing Information: Status | is | Active`
 - Click **Add Line**, then specify criteria that identify critical patches:
`AND | Patch Listing Information: Impact | is | Critical`
 - Click **Add Line**, then specify criteria that identify Windows patches:
`AND | Patch Listing Information: Operating System | is | Windows`
 - Click **Add Line**, then specify criteria that identify operating system patches:
`AND | Patch Listing Information: Category | is | OS`
- Click **Test** to display items that match the search criteria.
- Adjust the criteria as needed until the results are what you expect.
- 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.
 - 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.

- 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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**.
 - c. On the *Patch Management* panel, click **Catalog**.
2. Click the **Smart Label** tab above the list on the right.

The *Smart Label* panel appears.

Choose Action ▾ Advanced Search Smart Label Notification ⚙ ▾

Smart Label

Name ▾ contains ▾ Windows AND ▾ Add Line Add Group

Disk % Capacity ▾ > ▾ 95 AND ▾ Add Line Add Group

Choose label: ▾ Test Save ☐ Metering Enabled

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

i **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](#).

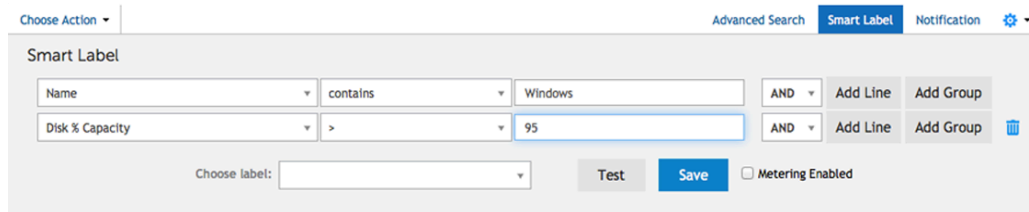
Using Smart Labels with Discovery Results

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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the 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.
 - 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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**.
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.
 - Enter a new name for the Smart Label in the *Choose label* field, then press **Enter** or **Return**.

i **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** 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 AMP 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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**.
2. Click the **Smart Label** tab above the list on the right.

The *Smart Label* panel appears.

Choose Action ▾ Advanced Search Smart Label Notification ⚙ ▾

Smart Label

Name ▾ contains ▾ Windows AND ▾ Add Line Add Group

Disk % Capacity ▾ > ▾ 95 AND ▾ Add Line Add Group

Choose label: ▾ Test Save ☐ Metering Enabled

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

i **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** 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.

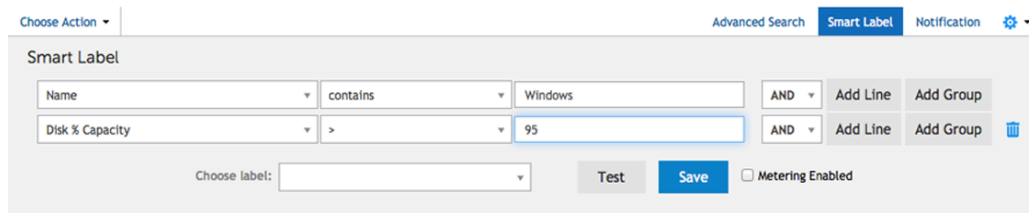
Force Inventory is available only if the AMP connection to an Agent-managed device is active, or for Agentless devices, if the device is reachable.

Add a Smart Label for laptops

You can create a Smart Label to identify devices that require laptop patches.

- Go to the *Devices* list:
 - Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
 - On the left navigation bar, click **Inventory**.
- Click the **Smart Label** tab above the list on the right.

The *Smart Label* panel appears.



- Specify search criteria:
 - Specify the criteria required to eliminate servers:
`Operating System: Name | does not contain | Server`
 - 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.
- Click **Test** to display items that match the search criteria.
 - 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.
 - Enter a new name for the Smart Label in the *Choose label* field, then press **Enter** or **Return**.

i **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.

- Click **Save** to create the Smart Label.
- 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.

- Test the Smart Label:
 - Click **Inventory** 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 AMP 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization 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. 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization 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 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization 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**.
 - 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 <i>Label Group</i> 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 <i>Licenses</i> . 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization 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 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization 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. 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization 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**.
 - 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 <i>Enabled</i> 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 <i>Associated Label Name</i> field. You must include at least one K1000 variable, such as <code>KBOX_COMPUTER_NAME</code>, 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

Option	Description
	relationships exists between the LDAP object and a K1000 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 <code>KBOX_USER_NAME</code>, 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 a K1000 object. See LDAP variables.  TIP: To test a label, replace the <code>KBOX_</code> 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 <i>Associated Label Name</i> 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: <code>ldaps://hostname</code>. If you have a non-standard SSL certificate installed on your LDAP server, such as an internally-signed certificate or a chain certificate that is not from a major certificate provider such as VeriSign®, contact Quest Support at https://support.quest.com/contact-support for assistance.
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.
Advanced Search	The search filter. For example: <pre>(&(sAMAccountName=KBOX_USERNAME) (memberOf=CN=financial,DC=example,DC=com))</pre>
Login	The credentials of the account the K1000 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.
Password	The password of the account the K1000 uses to log in to the LDAP server.
Label Attribute	For User-type labels: Enter a label attribute, such as: <code>memberOf</code>. 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	For User-type labels only: Enter the label prefix. For example: <code>ldap_</code> The label prefix is a string that is added to the beginning of all the labels.

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.

- Click the **Test** button to test the new label. Change the label parameters and test again as needed.
- If the LDAP Label is ready to use, select the *Enabled* check box. Otherwise, save the label without enabling it.
- 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization 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**.
 - 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization 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 Browser**.
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.  NOTE: To connect through SSL, use an IP address or hostname. For example: <code>ldaps://hostname</code>. If you have a non-standard SSL certificate installed on your LDAP server, such as an internally-signed

Option	Description
	certificate or a chain certificate that is not from a major certificate provider such as VeriSign, contact Quest Support at https://support.quest.com/contact-support for assistance.
Port	The LDAP port number, which is usually 389 (LDAP) or 636 (secure LDAP).
Login	The credentials of the account the K1000 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.
Password	The password of the account the K1000 uses to log in to the LDAP 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. Select a *Base DN* in the **Search Base DN** drop-down list, then click **Browse**.

The Base DN is searched and its children are displayed in a **Browse Tree**.

6. Enter a **Search Filter** to limit the children shown in the **Browse Tree**. To create a complex filter, click **Filter Builder**, then specify the following information in the *Query Builder*.

Option	Description
Attribute Name	Enter the attribute name. For example: sAMAccountName.
Relational Operator	Select the relational operator in the drop-down list. For example: = .
Attribute Value	Enter the attribute value. For example: admin.

7. To add more than one attribute, specify the following information:

Option	Description
Conjunction Operator	Select a conjunction operator in the drop-down list. For example: AND .

Option	Description
	 NOTE: This field is available for the previous attribute only when you add a new attribute.
Add	Click to add multiple attributes.
Search Scope	Click One level to search at the same level or click Sub-tree level to search at the sub tree level.

8. Click **OK**.

The query appears in the *Search Filter* text area. For example: (sAMAccountName=admin).

9. Click the **Browse Tree** to display all the immediate child nodes for the given Base DN and search filter.
10. Click **Search** to display all the direct and indirect child nodes for the given Base DN and search filter.

The search results appear in the left panel.

11. 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 change the username of the default admin account, and you cannot delete the account. However, you can change the password of the admin account. See [Add or edit System-level user accounts](#).

NOTE: In addition, 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. The admin account 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 Administrator Console. The drop-down list shows only those appliances and organizations whose admin account 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 change the username of the default admin account, and you cannot delete the account. However, you can change the password of the admin account. See [Add or edit System-level user accounts](#).

NOTE: In addition, 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. The admin account 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 Administrator Console. The drop-down list shows only those appliances and organizations whose admin account 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 K1000 System Administration Console, http://K1000_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 <i>Login ID</i> field on the login page. You cannot change the login of the default admin account.
Full Name	The user's full name.

Option	Description
Email	The user's email address.
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-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.
Enable KACE Security Notifications	Enable Quest to send security notifications to the email address of this administrator. This feature

Option	Description
	is available only to System-level administrator accounts. It is not available to Admin-level administrator accounts, or non-administrator user accounts.
Enable KACE 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.

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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 K1000 System Administration Console, http://K1000_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. At the bottom of the form, select or clear the check boxes next to the notification fields to enable or disable email notifications for the administrator.

Option	Description
Enable KACE 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

Option	Description
	administrator accounts, or non-administrator user accounts.
Enable KACE 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.

4. 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 K1000 System Administration Console, http://K1000_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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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. Click the **Expand All** link below the Administrator Console *Permissions* to display the permissions settings for all categories.
6. Set permissions for each component.
7. 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.

1. Go to the *Roles* list:
 - a. Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 <i>Login ID</i> field on the login page. You cannot change the login of the default admin account.
Name	The user's full name.
Primary 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.
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.

Option	Description
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 K1000 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.
Assigned QIB Accounts	(Read only) Attributes related to Quest Identity Broker (QIB). QIB is a cloud-based single sign on (SSO) solution that enables users to log in to the K1000 Administrator Console or User Console using credentials from third-party identity providers, such as your organization's Identity Provider and Microsoft Azure Active Directory. This section is empty if QIB is disabled, or if the user has not attempted to log in using a third-party identity provider. See About Quest Identity Broker .

3. Click **Save**.

Related topics

[Add or edit User Roles](#)

[Configuring locale settings](#)

[About labels](#)

[Configuring Mobile Device Access](#)

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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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** to display the *User Detail* 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**.

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 K1000 Administrator Console, http://K1000_hostname/admin, where K1000_hostname is the hostname 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 K1000 System Administration Console, `http://K1000_hostname/system`, where K1000_hostname is the hostname of your appliance, or select **System** from the drop-down list in the top-right corner of the page.
- Log in to the K1000 User Console, `http://K1000_hostname/user`, where K1000_hostname is the hostname of your appliance, or select **User Console** from the drop-down list in the top-right corner of the page.

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

The *User Profile* dialog box appears.

- 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 <i>Login ID</i> 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.
	Update 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.

Tab	Option	Description
	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.
	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 K1000 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 or User Console using their domain username and password.

For information about adding user accounts to the K1000 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 K1000 appliance on your LDAP server. The K1000 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 in the K1000 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 K1000 appliance to an external LDAP server.

1. Go to the Admin-level *Authentication Settings* page:
 - a. Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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**.
 - c. On the *Control Panel*, click **User Authentication**.
2. 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 .

3. 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.

4. **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.

5. 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.

Option	Description
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. If you have a non-standard SSL certificate installed on your LDAP server, such as an internally-signed certificate or a chain certificate that is not from a major certificate provider such as VeriSign, contact Quest Support at https://support.quest.com/contact-support for assistance.
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: Domain Users is a special group that is not added to the <code>memberof</code> attribute values. For Domain Users members, use this format: <code>(primaryGroupId=513)</code>.
Advanced Search	The search filter. For example: <pre>(&(sAMAccountName=KBOX_USERNAME) (memberOf=CN=financial,DC=example,DC=com))</pre>
Login	The credentials of the account the K1000 uses to log in to the LDAP server to read accounts. For example: <pre>LDAP Login:CN=service_account,CN=Users, DC=company,DC=com.</pre> If no username is provided, an anonymous bind is attempted. Each LDAP Label can connect to a different LDAP or Active Directory server.
Password	The password of the account the K1000 uses to log in to the LDAP server.

Option	Description
Role	(Required) The user's role: Administrator: The user can log in to and access all features of the Administrator Console and User Console. Read Only Administrator: The user can log in, but cannot modify any settings in the Administrator Console or User Console. User Console Only: The user can log in only to the User Console. No Access: The user cannot log in to the Administrator Console or User Console. No Access is the default role. i NOTE: These roles are predefined and you cannot edit them. However, you can create and edit custom roles as needed.

i **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.

6. Click **Save**.
7. 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 K1000 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](#)

i **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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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: <code>ldaps://hostname</code>. If you have a non-standard SSL certificate installed on your LDAP server, such as an internally-signed certificate or a chain certificate that is not from a major certificate provider such as VeriSign, contact Quest Support at https://support.quest.com/contact-support for assistance.
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: <code>OU=end_users,DC=company,DC=com.</code> 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: <code>(&(sAMAccountName=KBOX_USERNAME)(memberOf=CN=financial,DC=example,DC=com))</code>
Login	The credentials of the account the K1000 uses to log in to the LDAP server to read accounts. For example: LDAP Login: <code>CN=service_account,CN=Users,DC=company,DC=com.</code>

Option	Description
	If no username is provided, an anonymous bind is attempted. Each LDAP Label can connect to a different LDAP or Active Directory server.
Password	The password of the account the K1000 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: <pre>sAMAccountName, objectguid, mail, memberof, displayname, sn, cn, userPrincipalName, name, description, manager</pre> The LDAP attributes specified in this field can be mapped to K1000 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: <code>memberof</code>. 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: <code>ldap_</code> The label prefix is a string that is added to the beginning of all the labels.
Binary Attributes	Enter the binary attributes. For example: <code>objectsid</code>. 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 K1000 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: <code>objectguid</code> .
User Name	The name of the user. Recommended value: <code>name</code> .
Email	The email address for the user. Recommended value: <code>mail</code> .
Manager	The manager of the user. This mapping is mandatory only if you want to retrieve the manager information. Recommended value: <code>manager</code>.  IMPORTANT: To retrieve the manager object associated with the user, you must also add the manager attribute to the <i>Attributes to retrieve</i> box.

The following attribute mappings are not required, but they are recommended:

Option	Description
Api Enabled	Whether users are enabled to access the K1000 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 in the K1000 6.4 release. 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 K1000 Management 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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**.
 - c. On the *Control Panel*, click **User Authentication**.
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: <code>ldaps://hostname</code>. If you have a non-standard SSL certificate installed on your LDAP server, such as an internally-signed certificate or a chain certificate that is not from a major certificate provider such as VeriSign, contact Quest Support at https://support.quest.com/contact-support for assistance.
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: <code>OU=end_users,DC=company,DC=com.</code>  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: <pre>(&(sAMAccountName=KBOX_USERNAME) (memberOf=CN=financial,DC=example,DC=com))</pre>

Option	Description
Login	The credentials of the account the K1000 uses to log in to the LDAP server to read accounts. For example: <pre>LDAP Login:CN=service_account,CN=Users, DC=company,DC=com.</pre> If no username is provided, an anonymous bind is attempted. Each LDAP Label can connect to a different LDAP or Active Directory server.
Password	The password of the account the K1000 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: <pre>sAMAccountName, objectguid, mail, memberof, displayname, sn, cn, userPrincipalName, name, description, manager</pre> The LDAP attributes specified in this field can be mapped to K1000 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: <code>memberof</code>. 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: <code>ldap_</code> The label prefix is a string that is added to the beginning of all the labels.
Binary Attributes	Enter the binary attributes. For example: <pre>objectsid.</pre> 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.

Option	Description
Debug Output	Select the check box to view the debug output.
4. In the <i>Email Recipients</i> section, click the Edit button to enter the recipient's email address  .	
5. Select users in the <i>Recipients</i> drop-down list.	
6. In the <i>Scheduling</i> section, specify schedule options:	

Option	Description
Don't Run on a Schedule	Run in combination with an event rather than on a specific date or at a specific time.
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.

- Click **Next** to display the *User Import: Schedule - Define mapping between User attributes and LDAP Attributes* page.
- In the drop-down list next each attribute, select the value to use for K1000 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: <code>objectguid</code> .
User Name	The name of the user. Recommended value: <code>name</code> .
Email	The email address for the user. Recommended value: <code>mail</code> .
Manager	The manager of the user. This mapping is mandatory only if you want to retrieve the manager information. Recommended value: <code>manager</code>.  IMPORTANT: To retrieve the manager object associated with the user, you must also add the manager attribute to the <i>Attributes to retrieve</i> box.

The following attribute mappings are not required, but they are recommended:

Option	Description
Api Enabled	Whether users are enabled to access the K1000 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 .

Option	Description
Ams Id	Not used in the K1000 6.4 release. Recommended value: No Value .
9. Optional: In the <i>Role</i> 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 <i>Labels</i> drop-down list, select the label to apply to imported users. See About labels .	
12. In the <i>Search Results</i> 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 <i>Search Results</i> , change the <i>Maximum Number of Rows</i> on the <i>Choose attributes to import</i> page.
13. Click Next to display the <i>Import Data into the K1000 Management Appliance</i> 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, <i>Ldap Uid</i> , <i>User Name</i> , <i>Email</i> , and <i>Manager</i> , are imported. Records that do not have these values are listed in the <i>Users with invalid data</i> 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 <i>Scheduling</i> section. - Click Finish to save the schedule without importing user information. The schedule is set to run according to the options selected in the <i>Scheduling</i> 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 K1000 Administrator Console and User Console without having to re-enter their credentials on the K1000 login page.

You can use either Active Directory or Quest Identity Broker for single sign on. You cannot enable both single sign on methods simultaneously on the same appliance.

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 K1000 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.
- Quest Identity Broker:** Quest Identity Broker (QIB) is a cloud-based single sign on solution that enables users to request access to the K1000 Administrator Console or User Console using identity providers, such as your organization's Identity Provider. If the Organization component is enabled on your appliance, QIB can be enabled for the default organization only.



NOTE: Quest recommends that you access the Administrator Console using the web server name rather than the IP address. The web server name can be found on the *Network Settings* page. See [Changing appliance network settings](#).

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 K1000 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 K1000 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](#)

About Quest Identity Broker

Quest Identity Broker (QIB) is a cloud-based single sign on (SSO) solution that enables users to log in to the K1000 Administrator Console or User Console using third-party identity providers, such as your organization's Identity Provider and Microsoft Azure Active Directory.

QIB uses SAML (Security Assertion Markup Language) to authenticate users with third-party credentials. QIB can be configured to automatically create K1000 accounts that enable authenticated users to log in to the K1000 User Console, or to require administrator approval before accounts are created and access is granted. In addition, some identity providers enable integration with social networks, such as Facebook, LinkedIn, Twitter, and others.

If the Organization component is enabled on your appliance, QIB can be enabled for the default organization only. To enable single sign on for multiple organizations, use the standard Active Directory method. See [Using Active Directory for single sign on](#).

Enabling and disabling single sign on

You can enable or disable single sign on in the K1000 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 or Quest Identity Broker.

- To configure single sign on for Active Directory, see [Configure Active Directory as the single sign on method](#)
 - To configure single sign on for the Quest Identity Broker, see [Configure Quest Identity Broker 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 K1000 Administrator Console, `http://K1000_hostname/admin`, then click **Settings**.
 - If the Organization component is enabled on the appliance, log in to the K1000 System Administration Console, `http://K1000_hostname/system`, or select **System** in the drop-down list in the top-right corner of the page, then click **Settings**.
 2. Click **Security Settings** to display the *Security Settings* page.
 3. In the *Single Sign On* section, select a single sign on method.
 - [Configure Active Directory as the single sign on method](#)
 - [Configure Quest Identity Broker as the single sign on method](#)

Disable single sign on

You can disable single sign on without removing the K1000 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 K1000 Administrator Console, `http://K1000_hostname/admin`, then click **Settings**.
 - If the Organization component is enabled on the appliance, log in to the K1000 System Administration Console, `http://K1000_hostname/system`, or select **System** in the drop-down list in the top-right corner of the page, then click **Settings**.
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 K1000 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 Internet Explorer and 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 K1000 Administrator Console and User Console without having to re-enter their logon credentials each time.

Before you connect the K1000 to an Active Directory server, verify that:

- Network and DNS settings are configured to enable the K1000 appliance to access the Active Directory server. See [Changing appliance network settings](#).
 - The time settings on the Active Directory server match the time settings on the K1000 appliance. For information on setting the time on the K1000 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 K1000 Administrator Console, http://K1000_hostname/admin, then click **Settings**.
 - If the Organization component is enabled on the appliance, log in to the K1000 System Administration Console, http://K1000_hostname/system, or select **System** in the drop-down list in the top-right corner of the page, then click **Settings**.
 2. In the *Single Sign On* section of the *Security Settings* page, select **Active Directory**, then provide the following information:

Option	Description
Domain	The hostname of the domain of your Active Directory® server, such as example.com.
Username	The username 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.

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 K1000 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 K1000 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 and Restart Services**.

When users are logged in to devices that are joined to the Active Directory domain, they can access the K1000 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 K1000 user account. See [Add or edit System-level user accounts](#).



NOTE: To use single sign on with Internet Explorer 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 Internet Explorer and Firefox browsers, users must configure their browser settings to use the appropriate authentication. The Chrome™ browser does not require any special configuration.

Configure Internet Explorer browser settings

To use Active Directory single sign on with the Internet Explorer, you must configure the browser's security settings.

1. In the Internet Explorer browser, click **Tools > Internet Options > Security**.
2. Select the appropriate security policy:
 - If the K1000 appliance is available on the Internet select **Trusted Sites**.
 - If the K1000 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, Internet Explorer cannot automatically log in to the Administrator Console or User Console even if single sign on is enabled on the K1000.

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 K1000 appliance. For example, `http://k1000.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 K1000 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 K1000 appliance in the browser address field. To identify the host name, see [Changing 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 K1000 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 K1000 Administrator Console, `http://K1000_hostname/admin`, then click **Settings**.
 - If the Organization component is enabled on the appliance, log in to the K1000 System Administration Console, `http://K1000_hostname/system`, or select **System** in the drop-down list in the top-right corner of the page, then click **Settings**.
2. Click **Security Settings** to display the *Security Settings* page.
3. In the *Single Sign On* section, 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.

Using Quest Identity Broker for single sign on

Quest Identity Broker (QIB) enables users to associate the credentials they use with third-party identity providers, such as your organization's Identity Provider or Microsoft Azure Active Directory. This association makes it possible to use a single sign on to access the Administrator Console or the User Console.

To use QIB to access the Administrator Console or User Console, users must enter the hostname of the K1000 appliance in the browser address field, then click **Login with Single Sign On** under the login credentials on the login page.



NOTE: QIB can be enabled for a single organization only. If the Organization component is enabled on your appliance, you can enable QIB for the default organization only. You cannot enable QIB for multiple organizations. To enable single sign on for multiple organizations, use Active Directory. See [Use Active Directory single sign on to access the Administrator Console or User Console](#)

Configure Quest Identity Broker as the single sign on method

You can use Quest Identity Broker (QIB) to enable users to log in to the Administrator Console and User Console using credentials from third-party identity providers, such as your organization's Identity Provider and Microsoft Azure™ Active Directory.

QIB can be enabled for a single organization only. If the Organization component is enabled on your appliance, you can enable QIB for the default organization only. To use single sign on with multiple organizations, use Active Directory authentication. 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 K1000 Administrator Console, `http://K1000_hostname/admin`, then click **Settings**.
 - If the Organization component is enabled on the appliance, log in to the K1000 System Administration Console, `http://K1000_hostname/system`, or select **System** in the drop-down list in the top-right corner of the page, then click **Settings**.
2. In the *Single Sign On* section of the *Security Settings* page, select **Quest Identity Broker**, then provide the following information:

Option	Description
Web Server Assertion Consuming Service URL	The URL associated with your K1000 appliance. This URL is created automatically during appliance configuration. To enable QIB, contact Quest Support and provide this URL to obtain the Relying Party Identifier for your appliance. IMPORTANT: If you enable or disable SSL for the appliance, this URL changes. As a result, you need to provide this URL to Quest Support and obtain a new <i>Relying Party Identifier</i> any time SSL settings are changed.
Relying Party Identifier	A unique identifier provided by Quest Support to enable QIB. This identifier determines which identity provider, such as your organization's Identity Provider or Microsoft Azure Active Directory, is

Option	Description
	used for authentication. You must provide your <i>Web Server Assertion Consuming Service URL</i> to Quest Support to receive this identifier.
Automatically approve user requests	Users requesting single sign on access are automatically granted access to the K1000 User Console if they are authenticated by the third-party identity provider. Accounts for these users are created automatically on the K1000 appliance.
Manually approve user requests	Administrators must approve access requests before users can access the K1000 Administrator Console or User Console. When users attempt to sign on to the K1000 using third-party credentials, the K1000 creates approval requests. When administrators log in to the Administrator Console, a notification stating that approval requests are pending appears on the information bar at the top of the <i>Dashboard</i> page. When administrators approve requests, user accounts are created on the K1000 appliance and users can access the K1000 Administrator Console or User Console.

- To specify identity provider settings, click **Advanced Settings**.



NOTE: Do not change these settings unless directed to do so by Quest Support.

Option	Description
Quest Identity BrokerURL	The URL of the identity provider.
Quest Identity BrokerIdentifier	The unique identifier of the identity provider.
Quest Identity BrokerCertificate	The certificate used to verify communications with the identity provider.

- Click **Save and Restart Services**.

Manage Quest Identity Broker user approval requests

Quest Identity Broker (QIB) user approval requests are created when users who do not have K1000 account credentials attempt to log in to the K1000 Administrator Console or User Console using identity providers, such as your organization's Identity Provider and Microsoft Azure Active Directory.

- QIB must be selected as the single sign on (SSO) method for the K1000 appliance. See [Configure Quest Identity Broker as the single sign on method](#).
- QIB must be configured to approve requests manually.
- QIB approval requests must be pending.



NOTE: When administrators log in to the Administrator Console or User Console, a message appears in the information bar at the top of the page if QIB approval requests are pending.

- Go to the *Approval Requests* list:

- a. Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 **Quest Identity Broker**.
2. To approve a single request from the *Approval Request Detail* page:
 - a. In the *Identity* column, click the linked name of a request to show the *Approval Request Detail* page.

The page shows attributes supplied by the identity provider, including *nameidentifier*, which identifies the user and the identity provider.

- b. Select one of the following options:

Option	Description
Create new account	Create an account on the K1000 for the user. When the account is created, the user can use single sign on to access the User Console only. If you want to grant access to the Administrator Console, you need to edit the user's permissions on the <i>User Detail</i> page.
Create new account and display editor	Create an account on the K1000 for the user and open the <i>User Detail</i> page for editing. This enables you to modify user access permissions for the K1000 User Console and Administrator Console as needed.
Map to existing account	Map the approval request to an existing user account. When you select this option, you need to choose the account you want to map to in the drop-down list. When you approve the request, the QIB request information is added to the <i>User Detail</i> page of the selected account.



NOTE: You can map multiple approval requests to user accounts.

- c. Click **Approve**. The request is approved, and an account is created for the user on the K1000. If the Organization component is enabled on your appliance, the account is created in the default organization.
3. To approve one or more requests:
 - a. On the *Approval Requests* page, select one or more check boxes next to the approval requests.
 - b. Select **Choose Action > Auto Create**.

The account is created with the default access permissions. If the Organization component is enabled on your appliance, the account is created in the default organization. To change permissions, edit the user account. See [Add or edit organization user accounts](#).

4. To reject approval requests, do one of the following:
 - To reject one or more requests from the *Approval Request* page, select the check boxes next to the request, then select **Choose Action > Reject**.
 - In the *Identity* column on the *Approval Request* page, click the linked name of a request to show the *Approval Request Detail* page, then click **Reject**.

Use single sign on through Quest Identity Broker

When Quest Identity Broker is enabled as the single sign on method, users can access the Administrator Console or User Console using credentials from identity providers, such as your organization's Identity Provider and Microsoft Azure Active Directory.

QIB must be selected as the single sign on (SSO) method for the K1000 appliance. See [Configure Quest Identity Broker as the single sign on method](#).

1. Go to the K1000 login page, http://K1000_hostname.
2. On the login page, click **Single Sign On** below the login information.
3. Provide valid third-party credentials.

If the appliance is configured to approve login requests automatically, the User Console is displayed. If the appliance is configured to approve login requests manually, a notification page appears. When the request is approved, return to the K1000 login page to access the Administrator Console or User Console.

Using Replication Shares

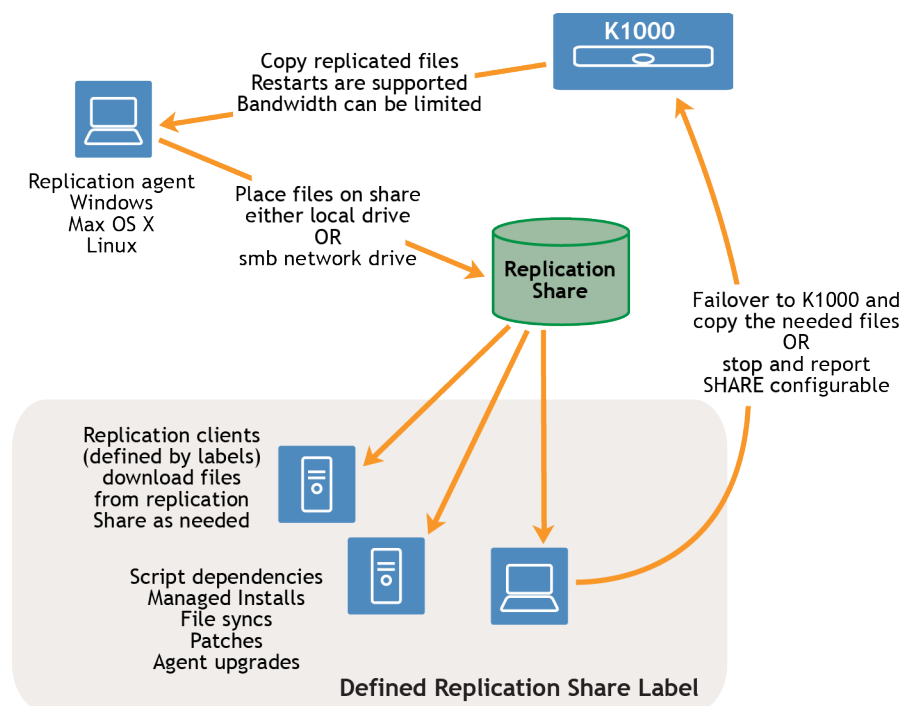
Replication Shares are devices that keep copies of files for distribution, and they are especially useful if your managed devices are deployed across multiple geographic locations.

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 K1000 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 7. 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 K1000 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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* section, select the **Enabled** check box.
3. **Optional:** Select **Failover To Appliance** to use the K1000 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** and **Include Dell Updates** check boxes to copy the patch and update files to the Replication Share.
 7. Specify the *Destination Share* settings:

Option	Description
Path	The path the Replication device uses for the Replication Share. Applications are copied from the K1000 to this location. For a local drive, use local drive syntax, for example: <code>C:\k1000share</code> For a network drive, use UNC format, for example: <code>\kaceRep\k1000share\</code>  NOTE: \$ notation, for example <code>\KaceRep\e\$</code>, is not supported.
Local Share or UNC	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 new credential to add credentials not already listed. See Add and edit User/Password credentials.

Option	Description
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 the *Download Share* settings:

Option	Description
Path	The path used by devices in the replication label to copy items from the replication drive. For example, a UNC path: <pre>\\fileservername\directory\k1000\</pre> 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 new credential to add credentials not already listed. See Add and edit User/Password credentials.

9. Specify the following settings in the *Schedule* section:

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 Light blue: Replication is on with low bandwidth Blue: Replication is on with high bandwidth

Option	Description
Copy Schedule From	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.

- Go to the *Replication* list:
 - Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
 - 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*, K1000 *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.

- 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 K1000 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 K1000 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 K1000 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 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 devices managed using Dell Mobility Management (DMM).

- 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 <i>Credentials Management</i> list

Option	Description
	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 <code>Domain\User</code> format might be required for some Windows configurations.
Password	The password required for the credential.
Show typing	Show the characters in the <i>Password</i> field on the <i>Add Credential</i> 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.
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 OAuth credentials

To streamline the management of Google OAuth credentials used in Inventory, Distribution, and Scripting, add those credentials to the *Credentials Management* page.

- 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](#).
- 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 <i>Credentials Management</i> 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 OAuth to specify credentials for Chrome devices.
Client ID	Your Google developer API Client ID.
Client Secret	Your Google developer API Client Secret.
Show typing	Show the characters in the <i>Client Secret</i> field on the <i>Add Credential</i> form. This option is available only when you are adding credentials. If you are editing existing credentials, the characters in the <i>Client Secret</i> field cannot be displayed.
Approval Code	The approval code for access. To obtain this code, provide your <i>Client ID</i> and <i>Client Secret</i> , then click Generate a new code .
Generate a new code	A link to the code-generator. To generate a new code: a. Click Generate a new code. b. Sign in with your Google Admin Account credentials on the Google sign-in page. If a Google sign-in page does not appear, your Google account credentials are already cached. If the cached account is not the preferred Admin Account, log out and log back in with the preferred Admin Account. c. Click Accept to generate a code that allows the K1000 access to view user and Chrome OS devices on the Google Domain. d. Copy the generated code and close the Google window. e. Paste the code into <i>Approval Code</i>.

Option	Description
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.

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.

- Go to the *Credentials Management* page:
 - Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
 - On the left navigation bar, click **Settings**, then click **Credentials**.
- Select **Choose Action > New**.
- On the *Add Credential* form, provide the following information:

Option	Description
Name	A unique name for the credential. This name appears on the <i>Credentials Management</i> 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.

Option	Description
Notes	Any additional information you want to provide about the credential.

- 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.
- Go to the *Credentials Management* page:
 - Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
 - On the left navigation bar, click **Settings**, then click **Credentials**.

The *In Use* column shows the components using the credentials.

- 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 K1000 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.

- Go to the *Credentials Management* page:
 - Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
 - On the left navigation bar, click **Settings**, then click **Credentials**.
- Select **Choose Action > Create Report**.
- On the *Report Detail* page, provide a name for the report.
- Select additional report settings, then click **Save**. See [Create reports from list pages](#).

The report appears on the Reports list.

- 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 K1000 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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](#).

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 <i>Assets</i> section.	In the <i>Inventory</i> 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 <i>Software Catalog</i> provides additional information about applications that are categorized as <i>Discovered</i> or <i>Not Discovered</i> .
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	Inventory information is automatically generated and overwritten each time managed devices report data to the appliance.

Item	Asset Component	Inventory Component
	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.	
How licenses are tracked	The Asset Management component enables you to manage software License Compliance as well as physical and logical assets.	On the <i>Software</i> page, inventory information includes the number of Software assets, but it does not show the number of licenses. On the <i>Software Catalog</i> 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 K1000 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
 - b. On the left navigation bar, 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 **Advanced Search** tab above the list on the right to display the *Advanced Search* 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.

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 **Advanced Search** tab above the list on the right to display the *Advanced Search* 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.

5. To create a custom view that uses the specified search criteria, click the **Custom View** tab above the list on the right, then save the view.

The custom view appears in the *View By* drop-down list. Custom views are user-specific. Users can access their own custom views, but they cannot access custom views created by other users.

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 *Assets* list:
 - a. Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
 - b. On the left navigation bar, click **Assets**.
 - c. Click the name of an asset.
2. On the *Asset Detail* page, in the list of 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
 - b. On the left navigation bar, click **Assets**.
2. In the *View By* drop-down list, select **Asset Type > Device**.
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.

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, Location, 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
 - b. On the left navigation bar, click **Assets**, 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, 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. If you want the instances of this asset type to use barcodes, specify one or more tags in the *Barcode Tags* area.

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**.
4. In the *Asset Fields* area, click .

A new line appears.
5. 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 <i>Type</i> 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 <i>Type</i> drop-down list, you must type one of the values given in the <i>Available Values</i> 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. • 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. • 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

Item	Description
	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	For subtypes of the device type asset only: The location, on the <i>Device Detail</i> page, where the field is reported. For example, if you are creating a printer Asset Subtype, with a field named <i>Toner Level</i>, you might select <i>Hardware</i> 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, 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
 - b. On the left navigation bar, click **Assets**, then click **Asset Types**.
 - c. Click the **Device** Asset Type.
2. 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 *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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
 - b. On the left navigation bar, click **Assets**, then click **Asset Types**.
 - c. Click the **Location** Asset Type.
2. 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
 - b. On the left navigation bar, 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
 - b. On the left navigation bar, click **Assets**, then click **Asset Types**.
2. Click the check box next to an Asset Type.
3. Select **Choose Action > Delete**, then click **Yes** to confirm.

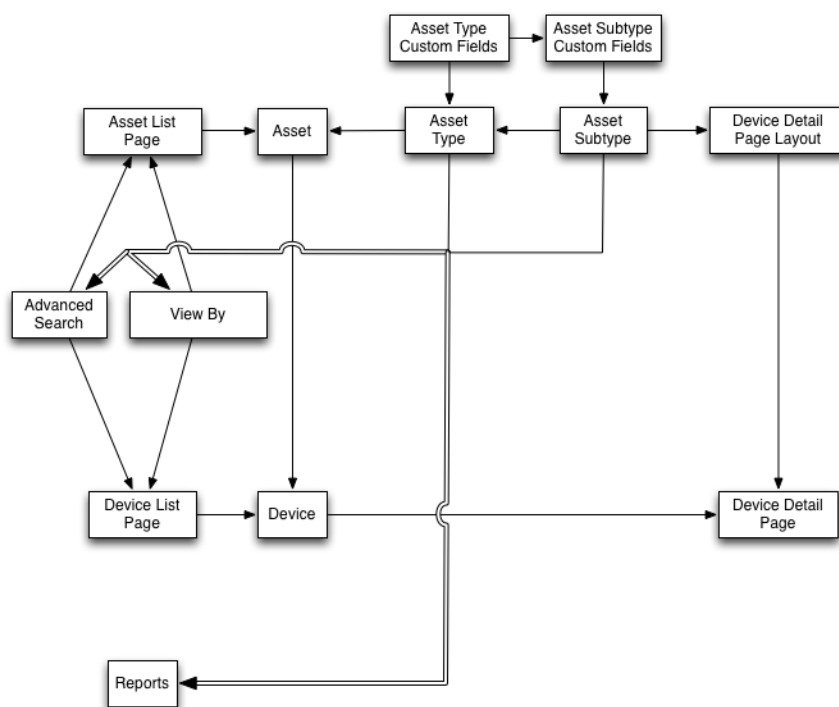
About Asset Subtypes, custom fields, and device detail preferences

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 K1000 inventory.

Asset Subtypes inherit the fields from the Asset Type, and you can add custom fields to enable the K1000 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 K1000 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
 - b. On the left navigation bar, click **Assets**, 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* section, click **Add Subtype**.
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.
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 <i>Asset Type Detail</i> 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 <i>Asset Detail</i> 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 <i>Type</i> 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 <i>Type</i> drop-down list, you must type one of the values given in the <i>Available Values</i> 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. • 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. • 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

Item	Description
	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 <i>Type</i> 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 <i>Device Detail</i> page, where the field is reported. For example, if you are creating a printer Asset Subtype, with a field named <i>Toner Level</i>, you might select <i>Hardware</i> 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 K1000 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
 - b. On the left navigation bar, click **Assets**, 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 **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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
 - b. On the left navigation bar, click **Assets**, 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* section 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the 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**, 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
 - b. On the left navigation bar, 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 K1000 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the 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 **Inventory** to display the *Devices* page.
3. To filter the list to show only those devices that are assigned to a subtype:
 - a. Click the **Advanced Search** tab above the list on the right to display the *Advanced Search* 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 K1000 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
 - b. On the left navigation bar, click **Assets**.
2. To filter the list to show only those assets that are assigned to a subtype:
 - a. Click the **Advanced Search** tab above the list on the right to display the *Advanced Search* 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 **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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
 - b. On the left navigation bar, 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
 - b. On the left navigation bar, click **Assets**, 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
 - b. On the left navigation bar, click **Assets**, 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
 - b. On the left navigation bar, click **Assets**.
 - c. Select **Choose Action > New > Software**.
2. Complete the asset fields as follows:

Option	Description
Subtype	The asset subtype, if applicable.
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.
Name	The asset name. For example, Office Pro SW Asset.
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 K1000 Inventory component automatically provides the Asset Management component with information about physical assets, such as devices, that report software and hardware inventory to the K1000. For physical and logical assets that do not report inventory to the K1000, 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
 - b. On the left navigation bar, click **Assets**, then click **Asset Types**.
 - c. Select **Choose Action > New**.
2. In the *Name* field, enter a descriptive name for the asset, such as Laptop.
3. Click the **Add** button on the right side of the page: **+**.

A new line appears.

4. 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.

5. 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**.

6. 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**.

7. 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**.

8. 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.

9. 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.

K1000 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 K1000 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the 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 the Assets list, select a device Asset. Select **Choose Action > Archive**.
 - On the 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 K1000 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 K1000 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
 - b. On the left navigation bar, click **Assets**, 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 move.
 - b. Select **Choose Action > Export**, and then choose the appropriate option.

For example, to export all locations to a CSV file, select **Choose Action > Export > Export 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
 - b. On the left navigation bar, click **Assets**, 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. 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
 - b. On the left navigation bar, click **Assets**, 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 <i>Location Detail</i> 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 <i>Type</i> 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

Option	Description
	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. • 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. • 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.

c. Click **Save**.

5. Click **Save**.

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 K1000 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 K1000 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 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 K1000 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
 - b. On the left navigation bar, click **Assets**, then click **Asset Types**.
2. In the *Name* column, click **License** to display the *Asset Type Detail* page.
3. In the *Name* field, type the name of the Asset Type.

The default for this type of asset is *License*.

4. **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.

5. 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.

License Mode Field:

License Mode ▲

Select Field...

License Mode

License Mode 2

License Mode 3

License Modes:

Select License Modes to Ignore...

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.

6. **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: .
7. 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 **Add New License** to display the *License Asset Detail* page.
4. Provide the following information:

Option	Description
Subtype	The Asset Subtype to associate with the license. See About Asset Subtypes, custom fields, and device detail preferences .
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 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 <i>Software Catalog</i> inventory and the <i>Software</i> 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 <i>License Compliance</i> page, select either <i>Enterprise</i> or <i>Unit License</i>. i NOTE: Most modes, including <i>Not Specified</i>, <i>Client License</i>, <i>Subscription</i>, <i>Shareware</i>, <i>Freeware</i>, <i>OpenSource</i>, <i>No Licensing</i>, and <i>Site License</i>, are not used for License Compliance.

Option	Description
	The license mode is used in these sections of the Administrator Console: - The <i>License Compliance</i> list. See View License Compliance information for Software Catalog applications. - The License Compliance chart that is displayed on the <i>Dashboard</i>. Values that are marked as ignored on the <i>Asset Detail</i> page are shown with a usage level of 100 percent. See About Dashboard widgets.
Product Key and Unit Cost	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 application. the <i>Vendor</i> 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 license was obtained. Click in the field, then select a date on the calendar.
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. 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 <i>Upgrade Software list</i> box. You can add one or more versions, as needed. To delete an item from

Option	Description
	the list, select it in the <i>Upgrade Software list</i> 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 K1000 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. 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 <i>Downgrade Software list</i> box. You can add one or more versions, as needed. To delete an item from the list, select it in the <i>Downgrade Software list</i> box, and click Remove. • No: If you do not want to grant downgrade rights to the selected software, select this option.
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

Option	Description
	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, <i>Unapproved Software Installation</i> . However, the K1000 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.
Notes	Any additional information you want to provide.
License Text	Any supplemental information about the license, such as a license number.
Custom Fields	Additional information. You can modify the License Asset Type to include as many additional fields as necessary to meet your business objectives.

5. Click **Save**.

The new asset appears on the *Assets* 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance 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 **Assets**. Select **Choose Action > New > License**.
 - 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. Provide the following information:

Option	Description
Subtype	The Asset Subtype to associate with the license. See About Asset Subtypes, custom fields, and device detail preferences .
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 Count	The number of installations or seats the license allows. For example, 50.
Applies to Cataloged Software	Leave this section blank. A software license cannot be associated with applications from the <i>Software</i> page inventory and the <i>Software Catalog</i> inventory at the same time. For more information on how to create license assets for cataloged software, see Add License assets for Software Catalog inventory .
Applies to Software	Applications in the <i>Software</i> page inventory to which the license applies. You can associate licenses with multiple applications on the <i>Software</i> page. If this field is blank, you need to create a Software asset as described in Adding Software assets.
License Mode	The mode of the License asset. For applications that require licenses, select either <i>Enterprise</i> or <i>Client Access License</i>.  NOTE: Most modes, including Not Specified, Unit 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 <i>License Compliance</i> list (Software Catalog inventory only). See View License Compliance information for Software Catalog applications. • The License Compliance chart that is displayed on the <i>Dashboard</i>. Values that are marked as ignored on the <i>Asset Detail</i> page

Option	Description
	are shown with a usage level of 100 percent. See About Dashboard widgets .
Product Key and Unit Cost	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 application. the <i>Vendor</i> drop-down list is empty unless you have added a Vendor asset. To search for a vendor, begin typing in the list. i NOTE: Assigning multiple vendors to a single software License asset is not recommended because it can result in inaccurate license compliance information. If you do assign multiple vendors to an asset, each vendor is assigned the total number of license seats specified in the <i>License Count</i> field.
Purchase Order Number	The purchase order number associated with the license.
Purchase Date	The date the license was obtained. Click in the field, then select a date on the calendar.
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. This setting, however, only applies to licenses for cataloged software. For non-cataloged software, set this option to No. For more information on how to create license assets for cataloged software, see Add License assets for Software Catalog inventory.
Includes Maintenance	Whether or not the license entitles users to upgrade or downgrade the version of the application.
Expiration Date	If the license includes maintenance, the expiration date of the maintenance period. The K1000 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.

Option	Description
	This setting, however, only applies to licenses for cataloged software. For non-cataloged software, set this option to No. For more information on how to create license assets for cataloged software, see Add License assets for Software Catalog inventory.
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 <i>Unapproved Software Installation</i>. However, the K1000 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.
Notes	Any additional information you want to provide.
License Text	Any supplemental information about the license such as the license number.
Custom Fields	Additional information. You can modify the License Asset Type to include as many additional fields as necessary to meet your business objectives.

3. Click **Save**.

The new asset appears on the *Assets* 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 K1000. 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. 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
- b. On the left navigation bar, click **Assets**, then click **Import Assets**.

5. Click **Browse** or **Choose File**, then select the CSV file.

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**.

The *Asset Type Selection* page appears.

7. Select the Asset Type and Asset Subtype:

- 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.

8. 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*=**Asset Name**
- *License Count*=**License Count**
- *Applies to Cataloged Software*=**Software Catalog**
- *License Mode*=**Mode**

9. 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.

10. 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.

Option	Description
Replace all asset barcodes with selected	Replace the existing barcodes with the specified barcodes.
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.

11. Click **Preview** to verify the data on the *Confirmation* page.

12. Click **Import** to complete the import process.

The *Result for Asset Import* page appears.

13. Click **Done** to return to the *Assets* page.

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.

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 K1000 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 **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 redisplay 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	The number of application installations that have been launched in the previous 90 days. A dash in this column indicates that metering is not enabled for the application.

Column name	Description
	 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	The number of application installations that have not been launched in the previous 90 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 .
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.

- 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: .

- 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](#).

- 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](#).

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 K1000 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 **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 redisplay 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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**.
 - c. On the *Control Panel*, click **General Settings**.

2. Scroll down to the *License Usage Warning Configurations* 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

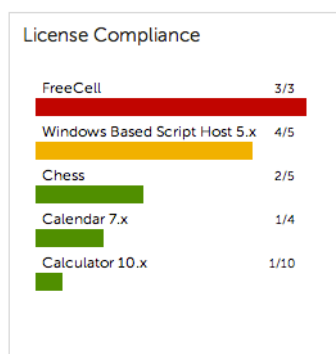
If you have set up License assets for applications, you can view License Compliance and Configuration information for those applications.

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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the 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.

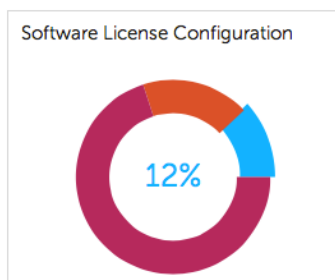


NOTE: The appliance updates the data in the *License Compliance* widget every eight hours. Clicking the **Refresh** button, however, does not update the data; it simply redisplay the data that has already been collected.

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, configuring ticket settings, and configuring 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 <i>Distribution</i> tab hidden, users in that organization, including the Admin user, cannot access the <i>Distribution</i> 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

Role	Description
	depends on the Organization Role assigned to the organization.
Administrator	The most powerful user role on the K1000 Management 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 <i>Tickets</i> 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 K1000 Management 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 K1000 Management Appliance. This role is useful for oversight personnel, such as supervisors. This role primarily interacts with the K1000 Management Appliance through the Administrator Console.
User ConsoleOnly	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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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

Category	Item	Permission level
Assets	All	HIDE
Distribution	All	HIDE
Scripting	All	HIDE
Security	All	HIDE
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](#).

- Go to the *Users* list:
 - Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
 - On the left navigation bar, click **Settings**, then click **Users**.
- Assign the Administrator role to your Service Desk administrators:
 - Select the check box next to one or more users.
 - Select **Choose Action > Apply Role > Administrator**.
By default, Administrator users have owner/submitter permissions.
- Assign the Service Desk Staff role to your team users:
 - 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 *Assign To Label* field, click **Edit**.
4. In the label window, drag the **All Ticket Owners** label to the *Assign To* 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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
Email	DefaultTicketOwners@mydomain.com
Password	Enter a password
Confirm Password	Enter the password again
Role	No Access
Assign 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 K1000 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. However, 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](#).
- 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 K1000 to receive email from POP3 servers.

To do so, you need to:

- Enable and configure an external SMTP server and POP3 in the appliance network settings. See [Use an external SMTP server or Secure SMTP server](#).
- Configure SMTP server and POP3 settings in Service Desk ticket queues. See [Configure ticket queues](#).

If you do not use a POP3 email server, you can use the K1000 appliance's built-in SMTP server to accept incoming email messages from your internal email server.



IMPORTANT: The K1000 Management 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. Go to the appliance *Control Panel*:
 - If the Organization component is not enabled on the appliance, log in to the K1000 Administrator Console, **`http://K1000_hostname/admin`**, then click **Settings**.
 - If the Organization component is enabled on the appliance, log in to the K1000 System Administration Console, **`http://K1000_hostname/system`**, or select **System** in the drop-down list in the top-right corner of the page, then click **Settings**.
 4. Click **Network Settings** to display the *Network Settings* page.
 5. Select **Enable SMTP Server** in the *Email Configuration* section, then specify the 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.
Port	Enter the port number to use for the 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	Enter the password of the specified account.

Option	Description
Enable Service Desk POP3 Server	Select this check box to use POP3 for Service Desk ticket email.

6. Click **Save** to restart the appliance.
7. Go to the Service Desk *Queue Detail* page:
 - a. Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 **Queues**.
 - d. To display the *Queue Detail* page, do one of the following:
 - Click the name of a queue.
 - Select **Choose Action > New**.
8. In the top section of the page, select **Configure SMTP Settings**.
9. Specify the following options:



NOTE: POP3 options are available only if *Service Desk POP3 Server* is enabled in the appliance Network Settings. See [Changing appliance network settings](#).

Option	Description
POP3 Server	Enter the name of the POP3 server you want to use for the queue. For example, <code>pop.gmail.com</code> .
POP3 User / Password	Enter the username and password of an account that has access to the POP3 server.
SMTP Server	Specify the SMTP server hostname or IP address, such as smtp.gmail.com . The SMTP server 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 SMTP server. For standard SMTP, use port 25. For secure SMTP, use port 587. If you leave this field blank, the appliance uses the settings specified on the <i>Network Settings</i> page.
SMTP User / Password	Enter the username and password of an account that has access to the SMTP server.

10. Click **Save**.
11. If you have multiple queues, repeat the preceding steps for each queue.

Configuring email triggers and email templates

You can set up triggers that automatically send email from the K1000 Management 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 K1000 Management Appliance users. Email templates determine the content of the messages.

Timing of email messages

The following email events trigger the K1000 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 K1000 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 **Queues**.
 - 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* section, 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.

Service Desk user (role)	Description
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 <i>Category Value</i> of the ticket. See Configure CC lists for ticket categories .

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 <i>Owner</i> field is changed.
Status Change	The ticket's <i>Status</i> field is changed.
Comment	Information, attachments, or screenshots are added to the ticket's <i>Comments</i> 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 <i>Any Change</i> notification is sent.
Approval Change	The ticket's approval status has changed.
Resolution Change	The ticket's resolution has changed.
Escalation	The ticket has not been resolved within the escalation time defined by the ticket priority.
SLA Violation	The ticket has not been resolved by its due date.
Ticket Closed	The ticket's <i>Status</i> 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.

- Click **Save**.

Related topics

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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 **Queues**.
 - 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* section, click **Customize Emails** to display the *Service Desk Email Notifications* page.
3. Change the following email templates as needed.



NOTE: If the default text for any of the templates is changed, the email messages will not be translated into different languages.

Ticket-related template	Description	Default recipients
Ticket 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	Used to acknowledge that a ticket has been created through email.	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 have been added to tickets.	Owners, submitters, approvers, the ticket CC list, and the ticket Category CC list

Ticket-related template	Description	Default recipients
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 <i>Email Ticket</i> action on <i>Ticket Detail</i> pages.  TIP: If you use HTML/Markdown, the <code>\$ticket_fields_visible</code> token must be enclosed in the <code><pre></code> tag to prevent formatting, such as line breaks, from being discarded. For example: <pre><pre> \$ticket_fields_visible</pre></pre>	Manually entered by the sender
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 <i>Queue Detail</i> 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.
\$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.
\$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 <i>Service Desk</i> 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 .
\$ticket_approver_email	The email address of the ticket approver. Having this address is especially useful for <i>Comments</i> 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.

Token	Description
\$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, <i>CUSTOM_5</i>, and that field is configured with the label <i>Location Name</i>, the system replaces <code>\$ticket_custom_5_label</code> with the text, <i>Location Name</i>. The token, <code>\$ticket_custom_5_value</code> is replaced with the ticket value that was saved for the <i>Location Name</i> field, such as, <i>Topeka</i> or <i>Albuquerque</i>. 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.
\$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 <code>\$ticket_fields_visible</code> token must be enclosed in the <code><pre></code> tag to prevent formatting, such as line breaks, from being discarded. For example: <pre><pre>\$ticket_fields_visible</pre></pre>
\$ticket_history	The complete history of the ticket.

Token	Description
	 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 <code>\$ticket_history_X</code> to limit the number of records to include.
<code>\$ticket_history_X</code>	A specified number of records in the ticket history. X indicates the number of records to include, beginning with the most recent.
<code>\$ticket_id</code>	A unique identifier assigned to the ticket, also called the ticket number. Using this identifier is the primary method for users to identify tickets.
<code>\$ticket_number</code>	A formatted version of the ticket ID. This version begins with <code>TICK</code> followed by a minimum of five digits. For example, a ticket with ID 4321 is displayed as <code>TICK:04321</code> . This format is especially useful in email Subject lines to make sure that email replies link to the correct tickets.
<code>\$ticket_owner_email</code>	The email address of the Service Desk administrator assigned to the ticket.
<code>\$ticket_owner_name</code>	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.
<code>\$ticket_owner_phone_home</code>	Contact information for the Service Desk administrator assigned to the ticket.
<code>\$ticket_owner_phone_mobile</code>	Contact information for the Service Desk administrator assigned to the ticket.
<code>\$ticket_owner_phone_pager</code>	Contact information for the Service Desk administrator assigned to the ticket.
<code>\$ticket_owner_phone_work</code>	Contact information for the Service Desk administrator assigned to the ticket.
<code>\$ticket_priority</code>	The priority assigned to the ticket. Default values include High, Medium, and Low.
<code>\$ticket_resolution</code>	Information about what was done to resolve the ticket as described in the ticket's <i>Resolution</i> field.
<code>\$ticket_status</code>	The status of the ticket. Defaults include New, Opened, Closed, Need More Info, Reopened,

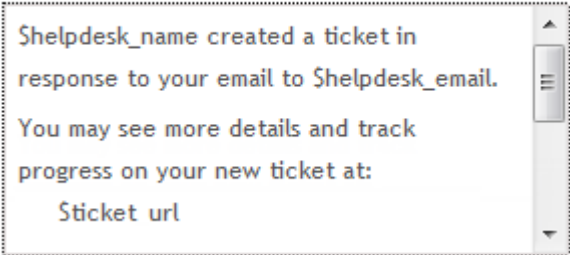
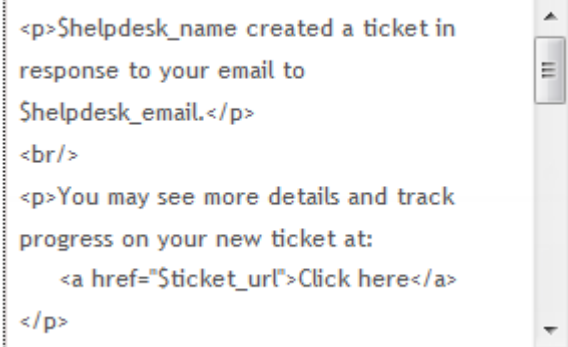
Token	Description
	Waiting Overdue, Waiting on Customer, and Waiting on Third Party.
\$ticket_submitter_email	The email address of the submitter.
\$ticket_submitter_name	The name of the submitter.  NOTE: The submitter name and contact information is derived from the USER record associated with the fields 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 <i>Ticket Detail</i> 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 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.

Token	Description
\$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.
4.	Optional: Select Use HTML/Markdown to use a simple HTML-based email instead of plain text.
	NOTE: To use HTML/Markdown feature, the email text must be fully formatted in HTML/Markdown. The default email text will not automatically convert to HTML/Markdown without the appropriate tags in the email text.

For example:

Default Email Notification	Email Notification with HTML
Message:  Shelpdesk_name created a ticket in response to your email to Shelpdesk_email. You may see more details and track progress on your new ticket at: Sticket url	Message:  <pre><p>Shelpdesk_name created a ticket in response to your email to Shelpdesk_email.</p>
 <p>You may see more details and track progress on your new ticket at: Click here </p></pre>

- 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.

- Go to the Service Desk *Queue Detail* page:
 - Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
 - On the left navigation bar, click **Service Desk**, then click **Configuration**.
 - On the **Configuration** panel, click **Queues**.

- 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* section, select all of the check boxes under the *Category CC* column. See [Configure email triggers](#).
3. Click **Save**.
4. In the *Ticket Defaults* section, click **Customize These Values**.
5. In the *Category Values* section, 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 a K1000 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 K1000 appliances running version 6.4 or later.

1. Go to the Service Desk *Settings* page:
 - a. Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 **Settings**.
2. In the *Inbound Email* section, 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 **Settings**.
2. In the *Inbound Email* section, click **Define 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 *Settings* page:
 - a. Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 **Settings**.
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* section, 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	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.

Option	Description
	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**.

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 a K1000 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 K1000 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 K1000 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 <i>Distribution</i> tab hidden, users in that organization, including the Admin user, cannot access the <i>Distribution</i> 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 K1000 Management 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.

Role	Description
	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 <i>Tickets</i> 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 K1000 Management 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 K1000 Management Appliance. This role is useful for oversight personnel, such as supervisors. This role primarily interacts with the K1000 Management 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.

- Go to the *Organization Role Detail* page:
 - Log in to the K1000 System Administration Console, http://K1000_hostname/system, or select **System** from the drop-down list in the top-right corner of the page.
 - On the left navigation bar, click **Organizations**, then click **Roles**.
 - 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.

- 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 K1000 System Administration Console, http://K1000_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.

Option	Description
Description	(Optional) Enter a description of the role.
4. To assign Administrator Console permissions:	
- In the Administrator Console <i>Permissions</i> 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 <i>Permissions</i> 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.

- Go to the *Roles* list:
 - Log in to the K1000 System Administration Console, http://K1000_hostname/system, or select **System** from the drop-down list in the top-right corner of the page.
 - On the left navigation bar, click **Organizations**, then click **Roles**.
- Select the check box next to one or more roles.
- 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 K1000 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](#).

- Go to the *Organization Detail* page:
 - Log in to the K1000 System Administration Console, http://K1000_hostname/system, or select **System** from the drop-down list in the top-right corner of the page.
 - On the left navigation bar, 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 K1000 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 <i>Client Drop Size</i> filter determines whether files uploaded to the organization's Client Drop location are displayed on the <i>Upload and Associate Client Drop File</i> list on the <i>Software Detail</i> page. For example, if the Client Drop Size filter is set to 1 GB, the <i>Upload and Associate Client Drop File</i> 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 <i>Software Detail</i> 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 <i>Backup Settings</i> page within five minutes. If you have multiple organizations, each organization has its own Client Drop location and Client Drop

Option	Description
	Size filter setting. See Copy files to the K1000 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 .
Locale	The language to use for the organization's Administrator Console and User Console.
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 K1000 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 <i>Client Drop Size</i> filter determines whether files uploaded to the organization's Client Drop location are displayed on the <i>Upload and Associate Client Drop File</i> list on the <i>Software Detail</i> page. For example, if the Client Drop Size filter is set to 1 GB, the <i>Upload and Associate Client Drop File</i> list shows files that are 1 GB in size or larger. Files that

Option	Description
	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 <i>Software Detail</i> 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 <i>Backup Settings</i> 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 K1000 Client Drop location.
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. In the *Communication Settings* section, specify the following settings:



NOTE: To reduce the load on the K1000 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 K1000 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 <i>Agent Logging</i> 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 <i>Agent Logging</i> .
Agent Inventory	12 hours	The frequency at which Agents on managed devices report inventory. This information is displayed in the <i>Inventory</i> section.
Agentless Inventory	1 Day	The frequency at which Agentless devices report inventory. This information is displayed in the <i>Inventory</i> section.

Option	Suggested Setting	Notes
Catalog Inventory	24 hours	The frequency at which managed devices report inventory to the <i>Software Catalog</i> page.
Metering	4 hours	The frequency at which managed devices report metering information to the K1000 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.
Disable Wait for Bootup Tasks	Disabled	If selected, this option stops the agent from executing bootup tasks.
Disable Wait for Login Tasks	Disabled	If selected, this option stops the agent from executing login tasks.

5. In the *Notify* section, specify the message to use for Agent communications:

Option	Suggested Setting	Notes
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 bootup splash logo.
Disable Login Splash	Disabled	If selected, this option stops the agent from displaying the login splash logo.
Agent Splash Page Message	Default text: KACE Systems Management Appliance (K1000) 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.

6. In the *Schedule* section, specify the *Communication Window* for Agent-managed devices:

Option	Suggested Setting	Notes
Communication Window	00:00 to 00:00 (+1 day)	The period of time during which Agents on managed devices are

Option	Suggested Setting	Notes
		allowed to connect with the K1000 appliance. For example, to allow Agents to connect between the hours of 01:00 and 06:00 only, select 01:00 from the first drop-down list, and 06:00 from the second drop-down list. You can set the communications window to avoid times when your devices are busiest.

7. In the *Agentless* section, specify communications settings for Agentless devices:

Option	Description
SSH/Telnet 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.
Maximum 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. 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://K1000_hostname/admin, where K1000_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](#)

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 K1000 System Administration Console, http://K1000_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**.
 - 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 K1000 System Administration Console, http://K1000_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 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 <i>Organization Filters</i> list.
Description	A description of the filter.

Option	Description
Order	The run order of the filter. Filters run according to the number specified. Low numbers run before high numbers.

3. Select filter criteria:

- a. Select a device attribute in the left-most drop-down list in the top row.

For example: **IP Address**.

- b. Select a condition in the second drop-down list.

For example: **contains**.

- 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 percent 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 no LDAP username is given, an anonymous bind is attempted. Each LDAP Filter might connect to a different LDAP server.

1. Go to the *Organization Filters Detail* page:

- a. Log in to the K1000 System Administration Console, http://K1000_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 <i>Organization Filters</i> list.
Description	A description of the filter.

Option	Description
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.



NOTE: To connect through SSL, use an IP address or hostname. For example: ldaps://hostname.

If you have a non-standard SSL certificate installed on your LDAP server, such as an internally-signed certificate or a chain certificate that is not from a major certificate provider such as VeriSign, contact Quest Support at <https://support.quest.com/contact-support> for assistance.

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: <pre>(&(objectCategory=Computer) (sAMAccountName=KBOX_COMPUTER_NAME))</pre>

LDAP Login	The credentials of the account the K1000 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 K1000 uses to log in to the LDAP server.

During the filter processing, the K1000 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_USERNAME
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 K1000 System Administration Console, http://K1000_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 K1000 System Administration Console, http://K1000_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**.
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 Advanced Search

If you need more granularity than keyword searches provide, you can use Advanced Search. Advanced Search 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 K1000 System Administration Console, http://K1000_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 K1000 System Administration Console, http://K1000_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 a K1000 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 K1000 appliances, 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the 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 K1000 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 Resources**.

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 K1000 System Administration Console, http://K1000_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 K1000 to network locations

If the Organization component is enabled on your appliance, you can move shared resources from the local K1000 to a network share.

1. Go to the *Shared Resources* list:

- a. Log in to the K1000 System Administration Console, http://K1000_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 K1000 System Administration Console, http://K1000_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 K1000 to manage devices, software, processes, and services in inventory.

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 K1000 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 K1000 Agent on devices.** The K1000 Agent can be installed on Windows, Mac®, Red Hat®, SUSE®, and Ubuntu® devices. See [Provisioning the K1000 Agent](#).
- **Enabling Agentless management for devices.** Agentless management is especially useful for devices that cannot have the K1000 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](#).
- **Third-party Discovery:** A different type of thorough discovery that is aimed at certain computer devices that are not Windows-, Mac Os X-, or Linux-based. See [Add a Discovery Schedule for a G Suite device](#) and [Add a Discovery Schedule for a Dell Mobility Management \(DMM\) 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 K1000 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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:

- **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 [G Suite, Dell Mobility Management, AirWatch].** *G Suite*, *Dell Mobility Management*, and *AirWatch* discovery options appear.
 - **Authenticated (WinRM, SNMP, SSH/Telnet).** *DNS Lookup*, *WinRM*, *SNMP*, and *SSH/Telnet* discovery options appear.
 - **Nmap.** *DNS Lookup* and *Nmap* discovery options appear.
 - **Custom.** *DNS Lookup*, *Ping*, *Nmap*, *WinRM*, *SNMP*, and *SSH/Telnet* 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 1-255 in the right-most box to scan for all IP addresses between 1 and 255 inclusive.
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.
	Timeout	The time, in seconds, after which a DNS lookup expires. If an address is not found during this time, the process "times out."
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 indicated as an approximate percentage instead of the number of devices scanned.
	Privileged User	The username of the administrator account on the Active

Option	Item	Description
		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
G Suite		Working with G Suite devices requires credentials that grant the K1000 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 K1000 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.
	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.

Option	Item	Description
		For more information, see Add and edit Google OAuth credentials .
	Auto Provision Devices	If selected, all Chrome and mobile devices discovered in the next scan are added to inventory. i NOTE: Use this option with care, to avoid expanding your inventory to an unexpected extent.
Dell Mobility Management		Dell Mobility Management (DMM) manages and provides access to smartphones and tablets
	Region	The region of the DMM Service, either US or EMEA .
	Credentials	The details of the admin account that is used to connect to the DMM Service. 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 DMM devices discovered in the next scan are added to inventory. i NOTE: Use this option with care, to avoid expanding your inventory to an unexpected extent.
AirWatch		VMware® AirWatch® 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 AirWatch administration console.
	REST API Key	The REST API key, available in the AirWatch administration console. The key must be provided to enable integration with AirWatch through API calls.

Option	Item	Description
	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 AirWatch devices discovered in the next scan are added to inventory. i NOTE: Use this option with care, to avoid expanding your inventory to an unexpected extent.
WinRM		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 K1000 network settings.
	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.
SNMP		SNMP (Simple Network Management Protocol) is a protocol for monitoring managed devices on a network.

Option	Item	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. i 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 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.
SSH/Telnet		Use SSH or Telnet protocols with authentication.

Option	Item	Description
		 IMPORTANT: After a Discovery Schedule is saved, you cannot change SSH and Telnet authentication 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).
	Try Telnet Connection	Enable the Telnet protocol for connecting to and communicating with devices. Use Telnet for devices that are not SSH-enabled or devices that have port 22 blocked. Telnet communications are not encrypted.
	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.
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

Option	Item	Description
		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 <i>Timeout</i> value to 10 minutes to decrease the likelihood of erroneous results. Do not combine this scan with the <i>Fast Scan</i> 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 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 <i>Timeout</i> value to 30 minutes to decrease the likelihood of erroneous results. Do not combine this scan with the <i>Fast Scan</i> option. Doing so results in only 100 commonly used ports being scanned.

Option	Item	Description
		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 minutes/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.
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.

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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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/Telnet]**. *DNS Lookup*, *WinRM*, *SSH/Telnet*, and *SNMP* 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 1-255 in the right-most box to scan for all IP addresses between 1 and 255 inclusive.
 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.
	Timeout	The time, in seconds, after which a DNS lookup expires. If an address is not found during this time, the process "times out."
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.
	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		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

Option	Item	Description
		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 K1000 network settings.
	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/Telnet		Use SSH or Telnet protocols with authentication.  NOTE: After a Discovery Schedule is saved, you cannot change SSH and Telnet authentication 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).
	Try Telnet Connection	Enable the Telnet protocol for connecting to and communicating with devices. Use Telnet for devices that are not SSH-enabled or devices that have port 22 blocked. Telnet communications are not encrypted.
	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

Option	Item	Description
		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 minutes/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.
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.

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 K1000 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 K1000 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 K1000 is enabled to import device information about devices and users from a Google Apps Domain when the K1000 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 K1000 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 K1000 for Chrome device discovery.

Add a Third Party Discovery Schedule to scan your network for Chrome devices and capture information about those devices. See [Add a Discovery Schedule for a G Suite device](#).

Add a Discovery Schedule for a G Suite device

To scan your network for G Suite devices and capture information about those devices, add a Third Party Discovery 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](#).
1. Go to the *Discovery Schedule Detail* page:
 - a. Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 [G Suite, Dell Mobility Management, AirWatch]*.
3. In the *Name* field, enter a name for the scan.

This name appears on the *Discovery Schedules* page.

4. Expand *G Suite* 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 G Suite 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. i 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 OAuth credentials.
Auto Provision Devices	If selected, all Chrome devices discovered in the next scan are added to inventory. i 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 minutes/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
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.

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 Dell Mobility Management (DMM) device

If you use Dell Mobile Management to manage and provision access to smartphones and tablets, you can discover managed mobile devices using discovery scheduling, and can provision discovered devices into K1000 inventory and asset management. To scan your network for DMM devices and capture information about those devices, you add a Third Party Discovery Schedule.

1. Go to the *Discovery Schedule Detail* page:
 - a. Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 *Third Party [Chrome, Dell Mobility Management]*.
3. In the *Name* field, enter a name for the scan.
This name appears on the *Discovery Schedules* page.
4. Expand *Dell Mobility Management* and select the Discovery options.

Option	Description
Region	The region of the Dell Mobility Management Service, either US or EMEA .
Credentials	The details of the admin account that is used to connect to the Dell Mobility Management Service. 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 DMM devices discovered in the next scan are added to inventory.

Option	Description
	 NOTE: Use this option with care, to avoid expanding your inventory to an unexpected extent.
5. Optional: In the <i>Notify</i> 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 minutes/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.
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.

- 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 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 K1000 to connect to devices, run commands, and capture Discovery information.

 **NOTE:** After a Discovery Schedule is saved, you cannot change SNMP authentication to SSH and Telnet authentication.

- Go to the *Discovery Schedule Detail* page:
 - Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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/Telnet]*.

The following options appear before the *Notify* section:

- *DNS Lookup*
- *WinRM*
- *SSH/Telnet*
- *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 1-255 in the right-most box to scan for all IP addresses between 1 and 255 inclusive.
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.
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 *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. i 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.

Option	Description
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 .
7. Optional: In the <i>Notify</i> section, enter an email address for being notified of when the discovery scan completes. The email includes the name of the discovery schedule. 8. 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 minutes/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.
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.

9. 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 AirWatch device

VMware® AirWatch® is an enterprise-level mobility management platform that allows you to manage a wide range of different device types. You can integrate with AirWatch to collect discover devices managed with AirWatch using REST API calls.

- Go to the *Discovery Schedule Detail* page:
 - Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
 - 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 [Chrome, Dell Mobility Management, AirWatch]*.
3. In the *Name* field, enter a name for the scan.
This name appears on the *Discovery Schedules* page.
4. Expand *AirWatch* and select the Discovery options.

Option	Description
Host	The host name of the AirWatch administration console.
REST API Key	The REST API key, available in the AirWatch administration console. The key must be provided to enable integration with AirWatch 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 AirWatch 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 minutes/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.
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.

7. 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](#).



NOTE: To run Device Actions, you must have the Administrator Console open in Internet Explorer, because ActiveX is required to start these programs on the local device. Other browsers do not support ActiveX.

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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 **Advanced Search** 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 K1000 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 K1000 to manage devices. Devices managed by the K1000 are referred to as device inventory.

About managing devices

Managing devices is the process of using the K1000 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 K1000 inventory, you can:

- **Install the K1000 Agent on devices.** Devices are automatically added to inventory after the Agent is installed on them and the Agent reports inventory to the K1000. See [Provisioning the K1000 Agent](#).
- **Enable Agentless management for devices.** Agentless management is especially useful for devices that cannot have the K1000 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 K1000 license agreement entitles you to manage a specified number of devices that are classified as Managed Computers, Assets, and Monitored Servers. 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 K1000 license information](#).

For information about the K1000 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, AIX®, CentOS™, Debian®, FreeBSD®, HP-UX, Oracle® Enterprise Linux, Red Hat Enterprise Linux, SUSE, Solaris®, and Ubuntu.

Table 9. K1000 features available to managed devices

Feature or component	Agent	Agentless				WSAPI manual
	Win, Mac, Linux	Win	Non-Win	Chrome Devices	SNMP	
Home						
Dashboard: Includes device information where appropriate. See About Dashboards .	X	X	X	X	X	
Label Management: Labels can be assigned to devices. See About labels .	X	X	X	X	X	X
Search: Devices included in results. See Searching for information and filtering lists .	X	X	X	X	X	X
Inventory						

Feature or component	Agent	Agentless			WSAPI manual	
	Win, Mac, Linux	Win	Non-Win	Chrome Devices	SNMP	
Devices: List includes devices. See Managing inventory information .	X	X	X	X	X	X
Devices > Force Inventory. See Forcing inventory updates .	X	X	X	X	X	
Devices > MIA settings. See Managing MIA devices .	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			
Software Catalog page: List	X Windows and Mac only					

Feature or component	WSAPI manual				
	Agent	Agentless			
	Win, Mac, Linux	Win	Non-Win	Chrome Devices	SNMP
includes software from devices. See Viewing Software Catalog information .					
Metering: Metering can be enabled for devices. See Using software metering .	X Windows and Mac only				
Blacklisting 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	X	X			

Feature or component	Agent	Agentless				WSAPI manual
	Win, Mac, Linux	Win	Non-Win	Chrome Devices	SNMP	
service inventory.						
Discovery Schedules: Devices can be discovered. See About Device Discovery and device management.	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	
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	X					

Feature or component	Agent	Agentless			WSAPI manual
	Win, Mac, Linux	Win	Non-Win	Chrome Devices	SNMP
custom inventory rules.					
Monitoring					
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:	X	X	X		

Feature or component	Agent	Agentless			WSAPI manual	
	Win, Mac, Linux	Win	Non-Win	Chrome Devices	SNMP	
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 .						
Assets						
Assets: Can be created for devices. See About managing assets .	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
Locations: Can be defined for devices, users, and assets. See	X	X	X	X	X	X

Feature or component						WSAPI manual
	Win, Mac, Linux	Win	Non-Win	Chrome Devices	SNMP	
Managing locations.						
Import Assets: Can be imported for devices. See Importing license data in CSV files.	X					
Distribution						
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 Synchronizations.	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	X					

Feature or component	WSAPI manual				
	Agent	Agentless			
	Win, Mac, Linux	Win	Non-Win	Chrome Devices	SNMP
Replication Shares.					
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				
Configuration Policies: Can be used to configure devices.	X Windows and Mac only				

Feature or component	WSAPI manual				
	Agent	Agentless			
	Win, Mac, Linux	Win	Non-Win	Chrome Devices	SNMP
See About configuration policy templates .					
Security Policies: Can be used to configure devices. See About security policy templates .	X Windows and Mac only				
Mac Profiles: Can be used to configure user-level and system-level policies and settings on Mac OS X devices. See Managing Mac profiles .	X Mac only				
Security					
Patch Management: Can be used to patch devices. See About patch management .	X Windows and Mac only				
OVAL Scans: Devices included in tests. See About OVAL security checks .	X Windows only				
SCAP scans: Devices included in	X Windows only				

Feature or component						WSAPI manual
	Agent Win, Mac, Linux	Agentless Win	Non-Win	Chrome Devices	SNMP	
scans. See About SCAP .						
Dell Updates: Can be used to update devices. See Managing Dell devices with Dell 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	
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	
Announcements: Can create announcements that appear on the User		X	X	X	X	

Feature or component	Agent	Agentless			WSAPI manual
	Win, Mac, Linux	Win	Non-Win	Chrome Devices	SNMP
Console home page. See Add, edit, hide, or delete User Console announcements.					
Configuration. X See Setting up Service Desk.		X	X	X	X
Reporting					
Reports: X Device information available for reports. See Creating reports.	X	X	X	X	X
Report Schedules: X View report schedules that have been created. See Scheduling reports.	X	X	X	X	X
Notifications: X Devices can be included in notifications. See Scheduling notifications.	X	X	X	X	X
Settings: Control Panel					
Device Actions: X Actions can be performed	X	X	X		X

Feature or component	Agent	Agentless			WSAPI manual
	Win, Mac, Linux	Win	Non-Win	Chrome Devices	SNMP
on devices. See Run actions on devices .					
License Usage Warning levels: Available for applications on devices. See Assign threat levels to applications .	X	X	X	X	X
History: Device information can be tracked. See Managing asset history .	X	X	X	X	X
Logs: Device information available. See View appliance logs .	X	X	X	X	X
Backup and restore: Device information included. See About appliance backups .	X	X	X	X	X
Organizations					
Filters: Organization filters can be assigned to devices. See Managing	X	X	X	X	X

Feature or component	Agent	Agentless				WSAPI manual
	Win, Mac, Linux	Win	Non-Win	Chrome Devices	SNMP	
organization filters.						
Redirect Devices: Devices can be reassigned to organizations. See Redirect devices.	X	X	X	X	X	X
Filtering Devices: Devices can be filtered and reassigned to organizations. See Filter devices.	X	X	X	X	X	
Organization settings: Inventory intervals configurable. See Schedule inventory data collection for managed devices.	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 K1000 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 K1000 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 K1000 Administrator Console, `http://K1000_hostname/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 K1000 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 K1000 System Administration Console, `http://K1000_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.

The *Organization Detail* page appears.

- If the Organization component is not enabled on your appliance, select **Settings > Provisioning**. Then click **Communication Settings** on the *Provisioning* panel.

The *Communication Settings* page appears.

2. In the *Communications Settings* section, specify the following settings:



NOTE: To reduce the load on the K1000 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 K1000 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 <i>Agent Logging</i> 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 <i>Agent Logging</i> .

Option	Suggested Setting	Notes
Agent Inventory	12 hours	The frequency at which Agents on managed devices report inventory. This information is displayed in the <i>Inventory</i> section.
Agentless Inventory	1 Day	The frequency at which Agentless devices report inventory. This information is displayed in the <i>Inventory</i> section.
Catalog Inventory	24 hours	The frequency at which managed devices report inventory to the <i>Software Catalog</i> page.
Metering	4 hours	The frequency at which managed devices report metering information to the K1000 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: Quest 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 *Schedule* section, specify the *Communication Window* for Agent-managed devices:

Option	Suggested Setting	Notes
Communication Window	00:00 to 00:00 (+1 day)	The period during which Agents on managed devices are allowed to connect with the K1000 appliance. For example, to allow Agents to connect between the hours of 01:00 and 06:00 only, select 01:00 from the first drop-down list, and 06:00 from the second drop-down list.

5. In the *Agentless* section, specify communications settings for Agentless devices:

Option	Description
SSH/Telnet 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.

6. 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.
Current Load Average	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 Load Average is not more than 10.0 and the Last Task Throughput Update time is more than 15 minutes.

7. Click **Save**.
The changes take effect when Agents check in to the appliance.
8. 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.

- Go to the *Device Detail* page:
 - Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
 - On the left navigation bar, click **Inventory**.

- 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 OVAL security checks](#)

[About SCAP](#)

[About the Asset Management component](#)

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](#).

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 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.	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: <i>Agent Device</i> , <i>Agentless Device</i> , or <i>Manually Entered Record</i> . 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
System 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 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

Item	Description	Database field
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 K1000 Agent installed on the device.	CLIENT_VERSION
Device Timezone	The timezone used by the K1000 Agent installed on the device.	TZ_AGENT
Source	The source of the collected device details. For Agent-managed devices, this field is set to Agent. For Agentless devices, this field reflects the connection type. For example, VMware.	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 (AMP) service on the device connected to the K1000 appliance and the current connection status (available for Agent-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.	KBSYS.SMMP_CONNECTION
Agentless Connection	The time the Agentless device connected to the K1000 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.	N/A

Item	Description	Database field
	 : Agentless management is enabled for the device, but the device is not currently reachable.	
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
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 AMP 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

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
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 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	VIRTUAL

Section or Item	Description	Database field
	displayed for physical devices, such as laptops and servers.	
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
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 <i>Days Left</i> column, which indicates the number of days remaining in the warranty	DELL_WARRANTY

Section or Item	Description	Database field
	period, and <i>Last Updated</i> column, which indicates the last time the warranty information was refreshed. To update Dell Service information, click Refresh .	
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
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
Printers	The printers that the device is configured to use.	PRINTERS
Network Interfaces	The type of network interface, such as IP address or MAC address, and whether DHCP is enabled or disabled.	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 <i>Authenticated</i> device discovery type to perform a Full Walk. This section does not appear if discovery was made with a Bulk GET.	
Chrome OS	Chrome-related information.	N/A

Section or Item	Description	Database field
	 NOTE: Chrome values are in the MACHINE_CHROMEOS_DETAIL table, not the MACHINE table.	
Device ID	The unique ID of the Chrome device.	DEVICE_ID
Serial Number	The Chrome device serial number	SERIAL_NUMBER
Status	The status of the Chrome device: ACTIVE, DEPROVISIONED, INACTIVE, RETURN_APPROVED, RETURN_REQUESTED, SHIPPED, UNKNOWN.	STATUS
Last Sync	The date and time the device was last synchronized with the policy settings in the Google Admin console.	LAST_SYNC
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
Annotated User	The user of the device as noted by the administrator.	ANNOTATED_USER
Annotated Location	The address or location of the device as noted by the administrator.	ANNOTATED_LOCATION
Notes	Notes about this device added by the administrator.	NOTES
MEID	The Mobile Equipment Identifier (MEID) for the 3G mobile card in a mobile device.	MEID
Order Number	The device's order number. Only devices directly purchased from Google have an order number.	ORDER_NUMBER
OS Version	The Chrome device's operating system version.	OS_VERSION
Platform Version	The Chrome device's platform version.	PLATFORM_VERSION

Section or Item	Description	Database field
Firmware Version	The Chrome device's firmware version.	FIRMWARE_VERSION
MAC Address	The device's wireless MAC address.	MAC_ADDRESS
Boot Mode	The boot mode for the device.	BOOT_MODE
Last Enrollment Time	The date and time the device was last enrolled with the Google Admin console.	LAST_ENROLLMENT_TIME
Org Unit Path	The full parent path with the Google organization unit's name associated with the device.	ORG_UNIT_PATH
Mobile Information	Information from devices managed by Dell Mobility Management (DMM) and AirWatch®	N/A
UDID	The device's Unique Device Identifier. For iOS devices only.	UDID
Device type	DMM devices only. The type of mobile device. Examples include iPhone, iPad, iPod, Android Phone, and Android Tablet.	DEVICE_TYPE
ICCID	DMM devices only. The unique serial number for the device's SIM card.	ICCID
IMEI	DMM devices only. International Mobile Equipment Identity number for the device.	IMEI
Phone Number	DMM devices only. Phone number associated with the device.	PHONE_NUMBER
Mobile Operator	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	DMM devices only. Amount of battery charge at last update, in percent.	BATTERY_LEVEL

Section or Item	Description	Database field
Last Check-in	The time stamp of when the device information was last updated.	LAST_CHECK_IN
Enrolled	AirWatch devices only. The date and time the device was last enrolled with the AirWatch console.	IS_ENROLLED
Compliant	AirWatch devices only. Indicates if the device meets pre-configured AirWatch compliance rules.	IS_COMPLIANT
Current Mobile Network	AirWatch devices only The name of the mobile network associated with the AirWatch device.	N/A
Agent	Agent-related information.	N/A
Agent Version	The version number of the K1000 Agent installed on the device.	CLIENT_VERSION
Version	The version of Agent Messaging Protocol (AMP) used to connect the device to the K1000 appliance.	AMP_VERSION
Connected	The time the Agent Messaging Protocol (AMP) service on the device connected to the K1000 appliance.	CONNECT_TIME
Disconnected	If disconnected, the time the Agent Messaging Protocol (AMP) service on the device disconnected from the K1000 appliance.	DISCONNECT_TIME
KACE ID	The character string used to identify the device in the K1000 database.	KUID
Database ID	The unique number used to identify the device in the K1000 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: <i>Agent</i>	N/A

Section or Item	Description	Database field
	<i>Device, Agentless Device, or Manually Entered Record.</i> Click Edit to change connection protocols.	
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 K1000 appliance. For Agentless devices, the time the K1000 appliance last connected to the device and collected inventory.	LAST_SYNC
Last Agent Update	The time of the most recent update to the K1000 Agent, if any.	LAST_CLIENT_UPDATE
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

Section or Item	Description	Database field
Number	The number of the operating system.	OS_NUMBER
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
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.	

Section or Item	Description	Database field
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
FileVault	Configuration and status information about Mac OS X FileVault 2.	N/A
Location	Information from devices managed by AirWatch.	N/A
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 is selected, this group lists the virtual machines running on the ESXi host. Some of the information in this list is only available if VMware tools are installed on the virtual machines. If some columns are not populated, this is because VMware tools are not installed on that virtual machine.	
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 K1000 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

Section or Item	Description	Database field
IP Address	The primary IP address assigned to the virtual machine.	IP
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
Hypervisors	When a vCenter is selected, this group lists the ESXi hosts managed by the vCenter.	
Hostname	The host name assigned to the ESXi host. If an ESXi 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 monitored ESXi device.	N/A
IP Address	The IP address assigned to the ESXi host.	N/A

Section or Item	Description	Database field
Status	The ESXi host status.	N/A

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 K1000 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 <i>upload a file</i> 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	N/A

Section	Description	Database field
	next to the heading. Click Show Changes to view only those items that have changed. Click Hide Changes to view all items.	
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. 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
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

Section	Description	Database field
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 to add configurations, click Manage Associated SNMP Configurations .	N/A

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	N/A

Section	Description	Database field
	can click Reset Tries to reset the number of patch attempts to the maximum allowed.	
Threat Level 5 List	Threats that are harmful to applications, processes, startup items, or services on the device.	N/A
OVAL Vulnerabilities	The results of OVAL (Open Vulnerability Assessment Language) vulnerability tests that have been run on this device. Only tests that failed on this device are listed by the OVAL ID and marked as <i>Vulnerable</i> . Tests that passed are grouped and marked as <i>Safe</i> .	N/A
SCAP Configuration Scans	The results of FDCC/SCAP Configuration Scans that have been run on this device.	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
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 K1000 using Dell Command | Monitor, see [About Dell Command | Monitor](#).

Dell Updates group

Information regarding updates and inventory (for Dell devices only).

Section	Description	Database field
Dell Update Schedules	The Dell updates that are scheduled to run on this device, and the time they are scheduled to run.	N/A
Dell System Inventory Report	The Dell devices that are installed on this device.	N/A

Section	Description	Database field
Dell Update Catalog Comparison Report	A list of Dell devices, installed on this device, that have drivers in the Dell catalog feed. If the installed version does not match the version in the Dell catalog feed, an icon indicates that the device needs to be upgraded.	N/A
Dell Update History	A list of the updates, such as driver updates, that have been performed on this device.	N/A

Logs 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.

Section	Description	Database field
Agent Logs	The logs for the K1000 Agent. A question mark indicates that its status is unknown.	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

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	N/A

Section	Description	Database field
	modified; the Asset Type, such as device; and the name of the asset.	
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 K1000 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 K1000 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 10. 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 11. 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 <i>Protected</i> and <i>Unprotected</i> . Values of <i>Locked</i> or <i>Unknown</i> 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 12. 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 <i>VendorProtected</i> , which indicates DDP E or BitLocker.	PROTECTION_REASON

BitLocker

BitLocker is a full disk encryption feature included with Windows.

Table 13. 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 14. BitLocker information displayed on the Device Detail page

Item	Description	MACHINE_BITLOCKER_VOLUME 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
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

Item	Description	MACHINE_BITLOCKER_VOLUME Database field
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 15. Supported OSs for FileVault 2

Operating system	Versions
Mac OS X	10.8, 10.9, 10.10

Table 16. 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 <i>Pending Conversion</i> , <i>Converting</i> ,	CONVERSION_STATUS

Item	Description	MACHINE_FILEVAULT_VOLUME Database field
	<i>Encryption Paused, and Complete.</i>	
Conversion Percentage	The extent of conversion, shown as a percentage.	CONVERSION_PERCENTAGE
Encryption Status	Status of the encryption. For example, <i>Locked</i> or <i>Unlocked</i> .	ENCRYPTION_STATUS
Encryption Type	Type of encryption used. For example, <i>AES-XTS</i> .	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 17. Supported OSs for TPM

Operating system	Versions
Windows	Vista, 7, 8, 8.1
Windows Server	2008, 2008 R2, 2012, 2012 R2

Table 18. 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	PHYSICAL_PRESENCE_VERSION _INFO

Item	Description	MACHINE_TPM Database field
	operations that require physical presence.	
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 K1000 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 K1000 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 K1000 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 K1000 file system.

i **NOTE:** After you set the registry key, the DDP|E service requires a full policy update schedule before the K1000 is able to collect inventory.

- Go to the *Script Detail* page for the *K1000 Enable Detailed DDPE Inventory (Windows)* script.
 - Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
 - On the left navigation bar, click **Scripting**.
 - From the list, select **K1000 Enable Detailed DDPE Inventory (Windows)**.
- In the *Configure* section, specify script settings:

Option	Description
Name	<i>K1000 Enable Detailed DDPE Inventory (Windows)</i> , 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.

Option	Description
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* section specify deployment options:

Option	Description
All Devices	Deploy to all devices. Clear the check box to limit the deployment to specific labels or devices.
Labels	Limit deployment to devices that belong to specified labels. To select labels, click Edit, drag labels to the <i>Limit Deployment to</i> 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.
Operating Systems	Limit deployment to devices that have the specified operating systems. Leave the Operating Systems field blank to deploy the script to all operating systems.
Select Specific Operating Systems	Limit deployment to devices that have specific versions of operating systems. If this check box is cleared, the script runs on all versions of specified operating systems.

4. In the *Schedule* section, specify run options:

Option	Description
None	Run in combination with an event rather than on a specific date or at a specific time.
Every nth minutes/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 or on a specific month at HH:MM	Run on the same day every month, or a specific month, at the specified time.
Custom Schedule	Run according to a custom schedule. Use standard 5-field cron format (extended cron format is not supported): <pre>* * * * * +-----day of week (0-6) (Sun=0) +-----month (1-12) +-----day of month (1-31) +-----hour (0-23) +-----minute (0-59)</pre> 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:
Also run once at next device checkin (for offline KScripts only)	Runs the offline KScript once when new scripts are downloaded from the appliance.
Also Execute 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 Execute after login (before desktop loads) (for offline KScripts only)	Runs the offline KScript after users enter Windows login credentials.

Option	Description
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 offline 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.

5. Skip the *Dependencies* and *Tasks* sections.
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 K1000 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 K1000 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 K1000 collects using Dell Command | Monitor. See [About Dell Command | Monitor](#).

Intel AMT resources and K1000 requirements

For information from the Dell Tech Center, go to <http://en.community.dell.com/techcenter/enterprise-client/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 K1000 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 19. 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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: To run Device Actions, you must have the Administrator Console open in Internet Explorer, because ActiveX is required to launch these programs on the local device. Other browsers do not support ActiveX.

1. Go to the *Device Detail* page for a device:
 - a. Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 **Advanced Search** tab above the list on the right to display the *Advanced Search* 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 <i>Software Detail</i> 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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.

Provisioning the K1000 Agent

Agent provisioning is the task of installing the K1000 Agent on devices you want to add to K1000 inventory using the Agent.

About the K1000 Agent

The K1000 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 K1000 appliance through AMP (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 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 K1000 Agent

You have a number of ways to deploy the K1000 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 K1000 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 K1000 Agent using email or logon scripts.

Related topics

[Provisioning the K1000 Agent using the GPO Provisioning Tool for Windows devices](#)

[Provisioning the K1000 Agent using onboard provisioning](#)

[Manually deploying the K1000 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 K1000 System Administration Console, http://K1000_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**.
 - c. On the *Control Panel*, click **Security Settings**.
2. In the *Samba* section, 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

Option	Description
	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 to appliance file shares	Enable NTLMv2 authentication for the K1000 files shares. When this setting is enabled, managed devices connecting to the K1000 File Shares require support for NTLMv2 and authenticate to the K1000 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 K1000 Agent. See Manually deploying the K1000 Agent .
Require NTLMv2 to off-board file shares	Force certain K1000 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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**.
 - c. On the *Control Panel*, click **General Settings**.
2. Select **Enable File Sharing** in the *Samba Share Settings* section.

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 Samba Settings**.
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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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**.
 - c. On the *Control Panel*, click **Security Settings**.
2. In the *Samba* section, select **Enable File Sharing**.
3. **Optional:** Select authentication options:

Option	Description
Require NTLMv2 to authenticate appliance file shares	Enable NTLMv2 authentication for the K1000 files shares. When this setting is enabled, managed devices connecting to the K1000 File Shares require support for NTLMv2 and authenticate to the K1000 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 K1000 Agent. See Manually deploying the K1000 Agent .
Require NTLMv2 authentication to off-board file shares	Force certain K1000 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 K1000 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 K1000 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 K1000 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 Vista and higher:** Remote Server Administration Tools (RSAT) enables IT administrators to remotely manage roles and features in Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 or Windows Server 2008 R2 from a computer that is running Windows 8.1, Windows 8, Windows 7, or Windows Vista.

Go to <http://social.technet.microsoft.com/wiki/contents/articles/2202.remote-server-administration-tools-rsat-for-windows-client-and-windows-server-dsforum2wiki.aspx>.

- **For Windows XP:** Install and enable the Group Policy Console for your Windows operating system.

Go to <http://microsoft.com/en-us/download/details.aspx?id=21895>.

- **.NET Framework 3.5.**
- **Windows Server 2008 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 K1000 Agents using the K1000 GPO Provisioning Tool

You can install the K1000 Agent on a single device, or on multiple devices by using the K1000 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 K1000 appliance to work in the Windows Group Policy Management Console or the Windows Administrative Tools using the K1000 GPO Provisioning Tool before returning to the appliance.

1. Go to the Agent Provisioning Assistant:
 - a. Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 K1000 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 K1000 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 K1000 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 K1000 Agent using onboard provisioning

You can install the K1000 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 K1000 to identify the devices and set up a provisioning schedule.

Preparing to install the K1000 Agent

Before you install the K1000 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 K1000 Agent installation

Before you install the K1000 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:

- Go to <https://documents.quest.com/KACE-Systems-Management-Appliance/Technical-Specifications-for-Physical-Appliances>.
- See [Verifying port settings, NTP service, and website access](#).

Prepare Windows devices to have the Agent installed

Before you install the K1000 Agent on Windows devices, you must configure file sharing and User Account Control (UAC) properly.

- **Prepare a Windows Vista™, Windows 7, or Windows 8 device**

Provide Administrator credentials for each device. To install the K1000 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 Vista, go to **Control Panel > User Accounts > User Accounts > Turn User Account Control on or off**. 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 a Windows XP device**

Turn off Simple File Sharing. For instructions, go to <http://support.microsoft.com/kb/304040> on the Microsoft Support website.



NOTE: If Simple File Sharing is enabled, logon failures occur. This failure is because Simple File Sharing does not support administrative file shares and the associated access security required for provisioning. Therefore, Simple File Sharing must be turned off during Agent provisioning.

- **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 52230 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 K1000 Agent on a device or multiple devices

You can install the K1000 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 K1000 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 K1000 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 K1000 appliance to periodically check devices in a specified IP address range and install, reinstall, or uninstall the K1000 Agent as needed.

For provisioning Windows devices, you can also use the K1000 GPO Provisioning Tool. Using the tool minimizes the pre-configuration that must happen on the target device. See [Provisioning the K1000 Agent using the GPO Provisioning Tool for Windows devices](#).

1. Go to the Agent Provisioning Assistant:

- a. Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 <i>Provisioning Schedules</i> 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.
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 hostnames of the target devices. The Help me pick devices link enables you to add devices to the <i>Target IP addresses or Hostnames</i> list: • Provisioning IP Range: Use hyphens to specify individual IP address class ranges. For example: 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 minutes/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.
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.

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.
- 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 K1000 generates a new KUID for the asset, and it appears as a new device in the K1000.

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 K1000 Agent using the GPO Provisioning Tool for Windows devices](#)

[Manually deploying the K1000 Agent](#)

Managing provisioning schedules

To streamline the Agent installation process, you can add provisioning schedules that specify how and when to install the K1000 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 <i>Provisioning Schedule Detail</i> page).

Option	Description
Targeted	The total number of target devices in the configuration (links to the <i>Provisioning Results</i> page).
Running	The total number of target devices on which provisioning is running (links to the <i>Provisioning Results</i> page).
Pending	The total number of target devices on which provisioning has not yet started (links to the <i>Provisioning Results</i> page).
Succeeded	The total number of target devices on which provisioning has succeeded (links to the <i>Provisioning Results</i> page).
Failed	The total number of target devices on which provisioning has failed (links to the <i>Provisioning Results</i> 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: Everyn 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 K1000 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 (Internet Explorer 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 *K1000 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 K1000 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 K1000 System Administration Console, http://K1000_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.

The *Organization Detail* page appears.

- If the Organization component is not enabled on your appliance, select **Settings > Provisioning**. Then click **Communication Settings** on the *Provisioning* panel.

The *Communication Settings* page appears.

2. In the *Communications Settings* section, specify the following settings:

To reduce the load on the K1000 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 K1000 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 <i>Agent Logging</i> 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 <i>Agent Logging</i> .
Agent Debug Trace	Enabled	If selected, this option allows you to record the Agent's debug trace. This information allows

Option	Suggested Setting	Notes
		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 <i>Inventory</i> section.
Agentless Inventory	1 day	The frequency at which Agentless devices report inventory. This information is displayed in the <i>Inventory</i> section.
Catalog Inventory	1 day	The frequency at which managed devices report inventory to the <i>Software Catalog</i> page.
Metering	4 hours	The frequency at which managed devices report metering information to the K1000 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.
Disable Wait for Bootup Tasks	Disabled	If selected, this option stops the Agent from executing boot-up tasks.
Disable Wait for Login Tasks	Disabled	If selected, this option stops the agent from executing login tasks.

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 (K1000) 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.

Option	Suggested Setting	Notes
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.

4. In the *Schedule* section, specify the *Communication Window*:

Option	Suggested Setting	Notes
Communication Window	00:00 to 00:00 (+1 day)	The period during which Agents on managed devices are allowed to connect with the K1000 appliance. For example, to allow Agents to connect between the hours of 01:00 and 06:00 only, select 01:00 from the first drop-down list, and 06:00 from the second drop-down list. You can set the communications window to avoid times when your devices are busiest.

5. In the *Agentless Settings* section, specify communications settings for Agentless devices:

Option	Description
SNMP Timeout	The time, in seconds or minutes, after which the connection is closed if there is no activity.
SSH/Telnet Timeout	The time, in seconds, after which the connection is closed if there is no activity.
WinRM Timeout	The time, in seconds or minutes, after which the connection is closed if there is no activity.
Maximum Attempts	The number of times the connection is attempted.

6. If the Organization component is not enabled on your appliance, specify *Agent* settings.



NOTE: If the Organization component is enabled on your appliance, these *Agent* settings are located on the appliance K1000 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 Load Average	The value in this field depicts the load on an appliance at any given time. For the appliance to run

Option	Description
	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 Load Average is not more than 10.0 and the Last Task Throughput Update time is more than 15 minutes.

- Click **Save**.

The changes take effect when Agents check in to the appliance.

- 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.

- Go to the appliance *Control Panel*:
 - If the Organization component is not enabled on the appliance, log in to the K1000 Administrator Console, `http://K1000_hostname/admin`, then click **Settings**.
 - If the Organization component is enabled on the appliance, log in to the K1000 System Administration Console, `http://K1000_hostname/system`, or select **System** in the drop-down list in the top-right corner of the page, then click **Settings**.
- On the left navigation bar, click **Support** to display the *Support* page.
- 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.

Column	Description
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.

- 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.

- Go to the appliance *Control Panel*:
 - If the Organization component is not enabled on the appliance, log in to the K1000 Administrator Console, `http://K1000_hostname/admin`, then click **Settings**.
 - If the Organization component is enabled on the appliance, log in to the K1000 System Administration Console, `http://K1000_hostname/system`, or select **System** in the drop-down list in the top-right corner of the page, then click **Settings**.
- On the left navigation bar, click **Support** to display the *Support* page.
- 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 K1000.

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 <i>Run Process</i> .
Command	The content and information contained in the message.
Expiration	The date and time when the message expires, also called <i>Keep Alive</i> time. Messages are deleted from the queue automatically when they expire.
Status	The status of the message, such as <i>Completed</i> or <i>Received</i> .

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 K1000 Administrator Console, `http://K1000_hostname/admin`, then click **Settings**.
 - If the Organization component is enabled on the appliance, log in to the K1000 System Administration Console, `http://K1000_hostname/system`, or select **System** in the drop-down list in the top-right corner of the page, then click **Settings**.
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 K1000 Agent on managed devices

The K1000 appliance automatically checks with Quest for K1000 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 K1000 appliance, provided that the appliance is connected to the Internet, and an alert appears on the *Home* page of the K1000 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 K1000 Agent updates

You can view K1000 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 K1000 Administrator Console, `http://K1000_hostname/admin`, then click **Settings**.
 - If the Organization component is enabled on the appliance, log in to the K1000 System Administration Console, `http://K1000_hostname/system`, or select **System** in the drop-down list in the top-right corner of the page, then click **Settings**.
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 K1000 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 **Update Agents**.

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 K1000 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 K1000 Agent installed. If this option is selected, the <i>Devices</i> and <i>Labels</i> 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 .
Manage Associated Labels	Display the <i>Edit Labels</i> 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 K1000 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

Upload Agent updates manually

In most cases, Agent updates are automatically downloaded to the K1000 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 K1000 Administrator Console, `http://K1000_hostname/admin`, then click **Settings**.
 - If the Organization component is enabled on the appliance, log in to the K1000 System Administration Console, `http://K1000_hostname/system`, or select **System** in the drop-down list in the top-right corner of the page, then click **Settings**.
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 Update** 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 K1000 Administrator Console, `http://K1000_hostname/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 **Update Agents**.
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 K1000 Agent

Manual deployment is useful when automated Agent provisioning is not practical or when you want to deploy the K1000 Agent using email, logon scripts, GPO (Group Policy Objects), or Active Directory.

- **Email:** To deploy K1000 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 K1000 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 K1000 Agent installers for Windows, Mac OS X, and Linux devices on the K1000 appliance in the following directory:

```
\\k1000_hostname\client\agent_provisioning
```



NOTE: File sharing must be enabled to access the installers. See [Enable file sharing at the System level](#).

Manually deploying the K1000 Agent on Windows devices

You can manually deploy the K1000 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\Dell\KACE\
- Window 64-bit devices: C:\Program Files (x86)\Dell\KACE\

The Agent configuration files, logs, and other data are stored in:

- Windows 32-bit devices: C:\Documents and Settings\All Users\Dell\KACE
- Window 64-bit devices: C:\ProgramData\Dell\KACE

Manually deploy the K1000 Agent on Windows devices using the installation wizard

You can manually deploy the K1000 Agent on Windows devices by running the installation wizard on devices.

1. Go to the shared directory of the appliance:

```
\\k1000_hostname\client\agent_provisioning\windows_platform
```

2. Copy the `ampagent-6.x.xxxxx-x86.msi` file to the device.
3. Double-click the file to start the installation and follow the instructions in the installation wizard.

The device information appears in the appliance Inventory within a few minutes. See [Managing applications on the Software page](#).

Manually deploy the K1000 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 20. Command line parameters for the Agent

Description	Parameter
Windows Installer Tool	<code>msiexec</code> or <code>msiexec.exe</code>
Install flag	<code>/i</code> Example: <code>msiexec /i ampagent-6.x.xxxxx-x86</code>
Uninstall flag	<code>/x</code> Example: <code>msiexec /x ampagent-6.x.xxxxx-x86</code>
Silent install	<code>/qn</code> Example: <code>msiexec /qn /i ampagent-6.x.xxxxx-x86</code>
Log verbose output	<code>/L*v log.txt</code> Example: <code>msiexec /qn /L*v C:\temp\log.txt /i ampagent-6.x.xxxxx-x86</code>
Auto set hostname: Rename the installation file to the name of the server name, which automatically sets the hostname	<code>rename agent_installer.msi_hostname.msi</code> Example: <code>msiexec /qn /i ampagent-6.x.xxxxx-x86_k1000.example.com.msi</code>
Set properties	<code>PROPERTY=value</code> (Must use ALL CAPS) Example: <code>msiexec /qn /i ampagent-6.x.xxxxx-x86.msi HOST=k1000.example.com</code>
Set server name	<code>set KACE_SERVER=k1000name</code> Must be followed by an <code>msiexec</code> call to install Example:

Description	Parameter
	<pre>set KACE_SERVER=kboxmsiexec /i ampagent-6.x.xxxxx-x86</pre>
Prevent the installation of logon or bootup hooks, and preserve existing userinit.exe files	NOHOOKS=1 Example: <pre>msiexec /qn /i ampagent-6.x.xxxxx- x86.msi HOST=k1000.example.com NOHOOKS=1</pre>
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: <pre>msiexec /qn /i ampagent-6.x.xxxxx- x86.msi HOST=k1000.example.com CLONEPREP=yes</pre>
Set the debug level for the Agent when it generates logs	DEBUG=true/all Example: <pre>msiexec /qn /i ampagent-6.x.xxxxx- x86.msi HOST=k1000.example.com DEBUG=true</pre>
Force the Agent to communicate through HTTPS only. It cannot fall back to HTTP if HTTPS is unavailable	SSLREQUIRED=true Example: <pre>msiexec /qn /i ampagent-6.x.xxxxx- x86.msi HOST=k1000.example.com SSLREQUIRED=true</pre>

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

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.

Manually deploying and upgrading the K1000 Agent on Linux devices

You can manually deploy or upgrade the K1000 Agent on Linux devices as needed.

Manually deploy the K1000 Agent on Linux devices

You can manually deploy the K1000 Agent on Linux devices by copying the Agent installation files to the devices and running installation commands.

1. Copy the K1000 Agent installation file to the device.

See [Obtaining Agent installation files](#).

2. Open a terminal window from **Applications > System Tools**.
3. At the command prompt, set the name of the server and install the Agent:

```
sudo KACE_SERVER=k1000name rpm -Uvh ampagent-6.x.xxxxx-x.i386.rpm
```

The Agent is installed in the following directories:

- /opt/dell/kace/bin/ where the Agent executable files are installed.
- /var/dell/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 K1000 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=k1000name
```

The `export` call must precede the call to the installer. For example: `export KACE_SERVER=k1000name rpm -Uvh k1000agent-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



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 K1000 Agent on Linux devices

You can manually upgrade the K1000 Agent on Linux devices by running commands on the devices.

1. Copy the K1000 Agent installation file to the device. See [Obtaining Agent installation files](#).
2. Open a terminal window from **Applications > System Tools**.
3. At the command prompt, enter:

```
rpm -uvh k1000agent-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/dell/kace/bin/AMPTools start
```

3. To stop the Agent, enter:

```
/opt/dell/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/dell/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/dell/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 K1000 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 K1000 Agent on Mac OS X devices. Additional options are described in [Use shell scripts to deploy the K1000 Agent](#).



NOTE: Some commands must be run as **root**.

NOTE: Proceed with `su` or `sudo` as required.

Deploy or upgrade the K1000 Agent to Mac devices using the Agent installer

You can manually deploy the K1000 Agent on Mac devices by copying the Agent installation files to the devices and running the installer.

1. Copy the K1000 Agent installation file to the device.

See [Obtaining Agent installation files](#).

2. Double-click **ampagent-6.x.build_number.dmg**.
3. Double-click **AMPAgent.pkg**.
4. Follow the instructions in the installer.

Be sure to enter the name of your K1000 appliance.

The installer creates the following directories on your device:

- `/Library/Application Support/Dell/KACE/bin` where the Agent executable files are installed.
- `/Library/Application Support/Dell/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 K1000 Agent on Mac devices by copying the Agent installation files to the devices and running commands.

1. Copy the K1000 Agent installation file to the device.
See [Obtaining Agent installation files](#).
2. Open a terminal window from **Applications > Utilities**.
3. At the command prompt, enter the following commands to set the name of the server and install the Agent:

```
hdiutil attach ./ampagent-6.x.xxxxx-all.dmg

sudo sh -c 'KACE_SERVER=k1000name installer -pkg /Volumes/Dell_KACE/
AMPAgent.pkg -target /'

hdiutil detach '/Volumes/Dell_KACE'
```

Use shell scripts to deploy the K1000 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=k1000name installer -pkg`
- `/Volumes/Dell_KACE/AMPAgent.pkg -target /'`
- `hdiutil detach '/Volumes/Dell_KACE'`

i **NOTE:** The export call must proceed the install call. For example: `sudo export KACE_SERVER=k1000name 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

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/Dell/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/Dell/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/Dell/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/Dell/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](#).

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 K1000 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 K1000 Agent software on those devices.

Agentless management uses SSH, Telnet, SNMP, and other methods to connect to Agent-intolerant devices, such as printers, network devices, and storage devices, and report inventory in the K1000 Administrator Console. Using Agentless management is useful for operating system versions and distributions that are not supported by the K1000 Agent, and where Agentless management is preferred over installing the Agent.

In version 6.4 of the K1000, 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
AIX
CentOS
Chrome OS
Debian
Fedora
FreeBSD
HP-UX
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 K1000 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 K1000 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 K1000 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 K1000 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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/Telnet, 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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**.
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/Telnet 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 K1000 inventory. See About Asset Subtypes , custom fields , and device detail preferences .
Connection Type	The connection method to use to connect to the device and obtain inventory information, in this case, SSH or Telnet.
Protocol	The protocol to use during connections. When SSH/Telnet is selected, options include: Use SSH2 if you want device communications to be more secure (recommended). Use Telnet for devices that are not SSH-enabled or devices that have port 22 blocked. Telnet communications are not encrypted.
Port	The port number the appliance uses to connect to the device. No input is required for the following default port numbers: • SSH: 22 • Telnet: 23

Option	Description
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. Credentials are not required for SNMPv1 and SNMPv2c. 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 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 and Telnet connections .
Log Level	The level of information to display on the <i>Device Detail</i> 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.

- 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 K1000 inventory. See About Asset Subtypes, custom fields, and device detail preferences .

Option	Description
Connection Type	The connection method to use to connect to the device and obtain inventory information, in this case, SNMP. 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 K1000 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
Read Community	(SNMP v1, SNMP v2c) The community string to query. The default is Public. The Public String is required if authentication is not required. When authentication is required, the scan returns SNMP enabled with no system data.
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 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 <i>Device Detail</i> page.

Option	Description
	 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 <i>Device Detail</i> 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.

- 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 K1000 inventory. See About Asset Subtypes , custom fields , and device detail preferences .
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.

Option	Description
	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 K1000 network settings.
Log Level	The level of information to display on the <i>Device Detail</i> 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.

- 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 .

Option	Description
	 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 <i>Device Detail</i> 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.

- Click **Test Connection**.

The connection status appears.

- 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 and Telnet connections

Operating systems vary in their support of shells used for SSH and Telnet connections between the appliance and managed devices.

The following table shows the shells available for SSH and Telnet connections for each operating system.

Table 21. Shell support for SSH and Telnet connections by operating system

Operating system	Default shell	Supported shells
AIX (IBM®)	ksh	bash, ksh, sh
CentOS	bash	bash, sh

Operating system	Default shell	Supported shells
Debian Linux	bash	bash, sh
Fedora	bash	bash, sh
FreeBSD	csch	bash, csch, sh
HP-UX	sh	ksh, 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.

- Go to the *Devices* list:
 - Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
 - On the left navigation bar, click **Inventory**.
- Click the name of an Agentless device that was entered manually to display the *Device Detail* page.
- In the *Summary* section, click **Edit** in the *Device Entry Type* row to display the *Agentless Device Connection Details* page.
- 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**.

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 K1000 enables you to map SNMP OIDs (Object Identifiers) to particular fields in the K1000 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 K1000 Agentless Inventory uses to extract data for inventory and integration into the K1000. The K1000 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 K1000 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 K1000 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 K1000, 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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**.
 - 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 K1000 inventory table so that their information can be integrated into inventory. See [Map Object Identifiers to fields in the K1000 inventory table](#).

Map Object Identifiers to fields in the K1000 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 K1000, 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 K1000. 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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.

i | **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 a K1000 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 K1000 inventory table](#).

i | **NOTE:** You can apply SNMP Inventory Configurations only to SNMP-managed Agentless devices.

1. Go to the *Devices* page:
 - a. Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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](#)

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 K1000 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 K1000 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 K1000 inventory, you can:

- **Install the K1000 Agent on devices.** Devices are automatically added to inventory after the Agent is installed on them and the Agent reports inventory to the K1000. See [Provisioning the K1000 Agent](#).
- **Enable Agentless management for devices.** Agentless management is especially useful for devices that cannot have the K1000 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 K1000 license agreement entitles you to manage a specified number of devices that are classified as Managed Computers, Assets, and Monitored Servers. 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 K1000 license information](#).

For information about the K1000 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 K1000 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 K1000 inventory manually by entering device information on the *Device Detail* page.

Once created, manual records are not touched or modified by the K1000 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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**.
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
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 K1000 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

Item	Description	Database field
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
Manufacturer	The device manufacturer.	CS_MANUFACTURER
CSP ID Number	Information used to identify the device.	BIOS_SERIAL_NUMBER
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
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
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

Item	Description	Database field
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
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 K1000 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
Version	The version number of the operating system.	OS_VERSION
Build	The build number of the operating system.	OS_BUILD
Number	The number of the operating system.	OS_NUMBER
Major Version	The number that identifies the major version of the operating system.	OS_MAJOR

Item	Description	Database field
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
Architecture	The architecture of the device operating system, such as x86 or x64.	OS_ARCH
Family	The product family of the operating system.	OS_FAMILY
Domain	The domain of the device.	CS_DOMAIN
Installed Date	The date the operating system was installed.	OS_INSTALLED_DATE
Last Reboot	The length of time the operating system has been running.	LAST_REBOOT
Last Startup	The last time the operating system was turned off.	LAST_REBOOT
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

9. In the *Other* section, provide additional information related to the device:

Item	Description	Database field
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
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
WMI Status	The status of the Windows Management Instrumentation	WMI_STATUS

Item	Description	Database field
	(WMI) service (Windows Devices only).	

10. 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 K1000 manually by creating an XML file and uploading that file to the K1000 using the API (application programming interface). Adding devices in this way is useful for devices that might not be able to run the K1000 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 K1000 appliance license limit. See [View K1000 license 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://K1000_hostname/service/wsapi.php`, where K1000_hostname is the hostname of your appliance.

Enable inventory API access

API inventory access enables you to upload inventory data using the API. This access is useful if you want to import inventory information from devices that do not have the K1000 Agent installed.

1. Go to the appliance *Control Panel*:
 - If the Organization component is not enabled on the appliance, log in to the K1000 Administrator Console, `http://K1000_hostname/admin`, then click **Settings**.
 - If the Organization component is enabled on the appliance, log in to the K1000 System Administration Console, `http://K1000_hostname/system`, or select **System** in the drop-down list in the top-right corner of the page, then click **Settings**.
2. Click **Security Settings** to display the *Security Settings* page.
3. Select **Enable Inventory API access**.
4. In the *API password* field, enter the password you want to use for API access.

This password is used only for API access and it does not need to match any other passwords.
5. Click **Save**.

After the appliance restarts, you can use external API commands to upload inventory information.

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.



NOTE: To submit inventory information using the API, you must enable inventory API access. See [Enable inventory API access](#).

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 K1000. 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);
}
# -----
# K1000 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 K1000 ...
# -----
$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 K1000 (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 K1000 ...
# -----
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 $uuid to K1000 ($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 XP Professional</OS_NAME>
  <OS_NUMBER>5.1.2600</OS_NUMBER>
  <OS_MAJOR>5</OS_MAJOR>
  <OS_MINOR>1</OS_MINOR>
  <SERVICE_PACK>Service Pack 2</SERVICE_PACK>
  <USER>Administrator</USER>
  <USER_FULLNAME>Tom Silver</USER_FULLNAME>
  <DOMAIN>WORK</DOMAIN>
  <OS_VERSION>5.1.2600</OS_VERSION>
  <OS_BUILD>2600</OS_BUILD>
  <OS_INSTALLED_DATE>2011-08-30 14:22:39 -0400</OS_INSTALLED_DATE>
  <LAST_REBOOT>2011-08-30 14:25:05 -0400</LAST_REBOOT>
  <LAST_SHUTDOWN>2011-08-30 14:25:05 -0400</LAST_SHUTDOWN>
  <UPTIME>4 days </UPTIME>
  <SYSTEM_DIRECTORY>C:\WINDOWS</SYSTEM_DIRECTORY>
  <SYSTEM_DESCRIPTION>XP Machine</SYSTEM_DESCRIPTION>
  <RAM_TOTAL>512.00MB</RAM_TOTAL>
  <RAM_USED>180MB</RAM_USED>
  <CS_MANUFACTURER>VMware, Inc.</CS_MANUFACTURER>
  <CS_MODEL>VMware Virtual Platform</CS_MODEL>
  <CHASSIS_TYPE>Other</CHASSIS_TYPE>
  <USER_LOGGED>Tom</USER_LOGGED>
  <CS_DOMAIN>WORK</CS_DOMAIN>
  <USER_NAME>Administrator</USER_NAME>
  <USER_DOMAIN>Work</USER_DOMAIN>
  <BIOS_NAME>PhoenixBIOS 4.0 Release 5.5 </BIOS_NAME>
  <BIOS_VERSION>INTEL - 6040000</BIOS_VERSION>
  <BIOS_MANUFACTURER>Phoenix Technologies LTD</BIOS_MANUFACTURER>

```



```

<BIOS_DESCRIPTION>PhoenixBIOS 4.0 Release 5.5 </BIOS_DESCRIPTION>
<BIOS_SERIAL_NUMBER>VMware-56 4d bd d3 5e 4f a5 4e-6a ce a0 d3 39 bd ae 02
  </BIOS_SERIAL_NUMBER>
<MOTHERBOARD_PRIMARY_BUS>PCI</MOTHERBOARD_PRIMARY_BUS>
<MOTHERBOARD_SECONDARY_BUS>ISA</MOTHERBOARD_SECONDARY_BUS>
<PROCESSORS>CPU Chip Count: 1
CPU Core Count: 0
CPU0: Intel Celeron processor (0 cores) </PROCESSORS>
  <SOUND_DEVICES>Creative AudioPCI (ES1371,ES1373) (WDM)
</SOUND_DEVICES>
  <CDROM_DEVICES>TSSTcorp DVD+-RW TS-U633F
</CDROM_DEVICES>
  <VIDEO_CONTROLLERS>VMware SVGA II
</VIDEO_CONTROLLERS>
  <REGISTRY_SIZE>1MB</REGISTRY_SIZE>
  <REGISTRY_MAX_SIZE>86MB</REGISTRY_MAX_SIZE>
  <DISK_DRIVES>
    <DiskDrive>
      <NAME>Drive C: (Physical Disk) FileSystem: NTFS Used: 2.08GB Total: 39.99GB</NAME>
      <DISK_SIZE>39.9906</DISK_SIZE>
      <DISK_USED>2.07966</DISK_USED>
      <DISK_FREE>37.9109</DISK_FREE>
      <PERCENT_USED>5.2</PERCENT_USED>
    </DiskDrive>
  </DISK_DRIVES>
  <NETWORK_INTERFACES>
    <NetworkInterface>
      <NIC>AMD PCNET Family PCI Ethernet Adapter - Packet Scheduler
Miniport</NIC>
      <MAC>00:0C:29:BD:AE:03</MAC>
      <IP>192.168.220.132</IP>
      <DHCP_ENABLED>True</DHCP_ENABLED>
    </NetworkInterface>
  </NETWORK_INTERFACES>
  <PRINTERS></PRINTERS>
  <STARTUP_PROGRAMS>
    <StartupProgram>
      <NAME>desktop</NAME>
    </StartupProgram>
    <StartupProgram>
      <NAME>VMware Tools</NAME>
      <COMMAND_EXE>C:\Program Files\VMware\VMware Tools\VMwareTray.exe</COMMAND_EXE>
      <COMMAND_ARGS />
      <FILE_INFO>
        <FILE_NAME>VMwareTray.exe</FILE_NAME>
        <FILE_DESCRIPTION>VMware Tools tray application</FILE_DESCRIPTION>
        <FILE_VERSION>8.4.6.16648</FILE_VERSION>
        <PRODUCT_NAME>VMware Tools</PRODUCT_NAME>
        <PRODUCT_VERSION>8.4.6 build-385536</PRODUCT_VERSION>
        <COMPANY_NAME>VMware, Inc.</COMPANY_NAME>
      </FILE_INFO>
    </StartupProgram>
    <StartupProgram>
      <NAME>VMware User Process</NAME>
      <COMMAND_EXE>C:\Program Files\VMware\VMware Tools\VMwareUser.exe</COMMAND_EXE>
      <COMMAND_ARGS />
      <FILE_INFO>
        <FILE_NAME>VMwareUser.exe</FILE_NAME>
        <FILE_DESCRIPTION>VMware Tools Service</FILE_DESCRIPTION>
        <FILE_VERSION>8.4.6.16648</FILE_VERSION>

```

```

        <PRODUCT_NAME>VMware Tools</PRODUCT_NAME>
        <PRODUCT_VERSION>8.4.6 build-385536</PRODUCT_VERSION>
        <COMPANY_NAME>VMware, Inc.</COMPANY_NAME>
    </FILE_INFO>
</StartupProgram>
</STARTUP_PROGRAMS>
<PROCESSES>
    <MachineProcess>
        <NAME>AMPAgent.exe</NAME>
        <COMMAND_EXE>C:\Program Files\Dell\KACE\AMPAgent.exe</COMMAND_EXE>
        <COMMAND_ARGS />
        <FILE_INFO>
            <FILE_NAME>AMPAgent.exe</FILE_NAME>
            <FILE_DESCRIPTION>AMP Service</FILE_DESCRIPTION>
            <FILE_VERSION>5.2.38916</FILE_VERSION>
            <PRODUCT_NAME>KACE Agent</PRODUCT_NAME>
            <PRODUCT_VERSION>5.2.38916</PRODUCT_VERSION>
            <COMPANY_NAME>Quest Software Inc.</COMPANY_NAME>
        </FILE_INFO>
    </MachineProcess>
</PROCESSES>
<NT_SERVICES>
    <NtService>
        <NAME>Alerter</NAME>
        <DISPLAY_NAME>Alerter</DISPLAY_NAME>
        <STATUS>SERVICE_STOPPED</STATUS>
        <STARTUP_TYPE>SERVICE_DISABLED</STARTUP_TYPE>
        <DESCRIPTION />
        <LOGON_AS_USER>NT AUTHORITY\LocalService</LOGON_AS_USER>
        <CAN_INTERACT_WITH_DESKTOP>False</CAN_INTERACT_WITH_DESKTOP>
        <COMMAND_EXE>C:\WINDOWS\system32\svchost.exe</COMMAND_EXE>
        <COMMAND_ARGS> -k LocalService</COMMAND_ARGS>
        <FILE_INFO>
            <FILE_NAME>svchost.exe</FILE_NAME>
            <FILE_DESCRIPTION>Generic Host Process for Win32 Services</FILE_DESCRIPTION>
            <FILE_VERSION>5.1.2600.2180 (xpsp_sp2_rtm.040803-2158)</FILE_VERSION>
            <PRODUCT_NAME>Microsoft® Windows® Operating System</PRODUCT_NAME>
            <PRODUCT_VERSION>5.1.2600.2180</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>20110830</INSTALL_DATE>
        <PUBLISHER>Quest Software Inc.</PUBLISHER>
        <UNINSTALL_STRING />
        <URLINFO_ABOUT />
        <DISPLAY_NAME>Quest KACE Agent</DISPLAY_NAME>
    </software>
</INSTALLED_software>
    <CLIENT_VERSION>6.0.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 K1000 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 K1000 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 K1000 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\Dell\KACE`
 - Windows 64-bit systems: `C:\Program Files (x86)\Dell\KACE`
 - Mac OS X systems: `/Library/Application Support/Dell/KACE/bin`
 - Linux systems: `/opt/dell/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 K1000 Administrator Console, go to the *Devices* list:
 - a. Log in to the K1000 Administrator Console, `http://K1000_hostname/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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**.
 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 K1000 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.

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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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**.
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\Dell\KACE\`
 - On 64-bit systems: `C:\Program Files (x86)\Dell\KACE\`



NOTE: For Windows Vista and later, use *Run as Administrator* when running the command.

3. Enter the following command:

```
runkbot -s 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/Dell/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/dell/kace/bin/
```

3. Enter the following command:

```
sudo ./runkbot 2 0
```

Inventory information is updated.

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 K1000 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 K1000 license 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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**.
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 <i>Automatically Relete MIA Devices</i> is selected. Managed devices that do not communicate with the appliance for the specified number of days are automatically deleted or archived, as specified.
Archive MIA Asset-Devices	Select this option to archive the MIA devices after the specified number of days.

Option	Description
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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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**.
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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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**.
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, K1000 Agents installed on managed devices communicate with the appliance using HTTP over ports 80, 443, and 52230. 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=myk1000
```

Mac OS X

```
hdiutil attach ampagent-6.x.xxxxx-all.dmg
sudo sh -c 'KACE_SERVER=myk1000 installer -pkg /Volumes/Dell_KACE/AMPAgent.pkg
-target /'
hdiutil detach /Volumes/Dell_KACE
```

Linux (RHEL and SLES)

```
export KACE_SERVER=myk1000
export KACE_SERVER=myk1000sudo 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\Dell\KACE\AMPTools" host=myk1000

64-bit systems: "C:\Program Files (x86)\Dell\KACE\AMPTools" host=myk1000

Mac OS X

/Library/Application\ Support/Dell/KACE/bin/AMPTools host=myk1000

Linux

/opt/dell/kace/bin/AMPTools host=myk1000

3. Verify that you are able to ping the appliance, and reach it through a web browser at http://k1000_hostname.
4. Verify that Internet Options are not set to use proxy. Verify that proxy is excluded for the local network or k1000_hostname.
5. Verify that no firewall or anti-spyware applications are blocking communication between the appliance and any of the Agent components, including:

Table 22. K1000 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 AMPctl

Operating system	Agent components
	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 K1000 periodically runs a background service that gathers and updates Dell warranty information on the Dell devices that are in your K1000 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 K1000 appliance](#).

Obtain Dell warranty information on a single Dell device instantly

You can obtain warranty information for any managed Dell device in your K1000 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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**.
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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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**.
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 K1000 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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**.
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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 K1000 *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 K1000 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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.
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 <i>Add/Remove Programs</i> 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: <pre>RegistryValueGreaterThan(HKEY_LOCAL_MACHINE \Software\Network Associates\TVD \Shared Components\VirusScan Engine \4.0.xx,szDatVersion,4.0.44)</pre> 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
 - b. On the left navigation bar, 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 K1000 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.



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 K1000 Client Drop location

You can upload large files, such as application files and backup files, to the K1000 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 K1000:
 - In Windows Explorer, enter a UNC path with the K1000 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 K1000 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 Advanced Search

Advanced Search 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 Advanced Search 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 K1000 *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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the 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 K1000 inventory as needed.

Add a manual label. See [Add manual software labels](#).

1. Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the 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.
 - 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 the ITNinja feed

The ITNinja feed enables you to view systems-management content from ITNinja in the Administrator Console. You enable and disable the ITNinja feed by changing your data sharing settings.

Sponsored by Quest KACE, ITNinja.com (formerly AppDeploy.com) is a product-agnostic IT-focused community website. It is the Internet's leading destination for IT professionals to share information and ask questions about system-management related topics. The website provides a question and answer section and a blogging platform. If you choose to share anonymous usage data with ITNinja, the ITNinja feed appears on pages such as the software, Managed Installation, and File Synchronization detail pages in the Administrator Console. The feed is not available on *Software Catalog* detail page. See [Enable the ITNinja feed](#).

Enable the ITNinja feed

To enable the ITNinja feed, configure the appliance settings to share anonymous usage data with Quest.

1. Go to the appliance *Control Panel*:
 - If the Organization component is not enabled on the appliance, log in to the K1000 Administrator Console, `http://K1000_hostname/admin`, then click **Settings**.
 - If the Organization component is enabled on the appliance, log in to the K1000 System Administration Console, `http://K1000_hostname/system`, or select **System** in the drop-down list in the top-right corner of the page, then click **Settings**.
2. Click **General Settings**.
3. In the *Share With Quest* section, select the *Share summary usage data...* and *Share detailed usage data...* check boxes.
4. Click **Save**.

For more information on K1000 General Settings, see [Configure appliance General Settings with the Organization component enabled](#).

Viewing ITNinja information

If the ITNinja feed is enabled, you can view ITNinja information related to Managed Installations, File Synchronizations, and software on detail pages in the Administrator Console.

See [Enable the ITNinja feed](#).



NOTE: ITNinja information is available for software on the *Software* page, but it is not available for software on the *Software Catalog* page.

View ITNinja information for software

You can view ITNinja information on the *Software Detail* page.

The ITNinja feed must be enabled. See [Enable the ITNinja feed](#).

1. Log in to the K1000 Administrator Console, `http://K1000_hostname/admin`. Or, if the *Show organization menu in admin header* option is enabled in the 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 name of an application to display the *Software Detail* page.
4. Scroll down to the ITNinja section.

View ITNinja information for Managed Installations

You can view ITNinja information for Managed Installations.

The ITNinja feed must be enabled. See [Enable the ITNinja feed](#).

1. Log in to the K1000 Administrator Console, `http://K1000_hostname/admin`. Or, if the *Show organization menu in admin header* option is enabled in the 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 **Distribution** to display the *Managed Installations* page.
3. Click the name of a Managed Installation to display the *Managed Installation Detail* page.
4. Scroll down to the ITNinja section.

View ITNinja information for File Synchronizations

You can view ITNinja information for File Synchronizations.

The ITNinja feed must be enabled. See [Enable the ITNinja feed](#).

1. Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the 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 **Distribution > File Synchronizations** to display the *File Synchronizations* page.
3. Click the name of a File Synchronization to display the *File Synchronization Detail* page.
4. Scroll down to the ITNinja section.

Disable the ITNinja feed

To prevent the ITNinja feed from being displayed in the Administrator Console, change the appliance settings that share data with Quest. This disables the ITNinja feed.

1. Go to the appliance *Control Panel*:
 - If the Organization component is not enabled on the appliance, log in to the K1000 Administrator Console, http://K1000_hostname/admin, then click **Settings**.
 - If the Organization component is enabled on the appliance, log in to the K1000 System Administration Console, http://K1000_hostname/system, or select **System** in the drop-down list in the top-right corner of the page, then click **Settings**.
2. Click **General Settings**.
3. In the *Share With Quest* section, clear the *Share detailed usage data...* check box.
4. Click **Save**.

For more information on K1000 General Settings, see [Configure appliance General Settings with the Organization component enabled](#).

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 K1000 appliances 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 K1000 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 K1000 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 K1000 inventory, the Not Discovered application list cannot be exported in CSV format.

Uncataloged applications

Uncataloged applications are executables that are in the K1000 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 K1000 inventory (Discovered applications) and applications that do not appear in K1000 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 K1000 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 blacklisted from running 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 K1000 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 K1000 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 K1000 inventory information with Quest KACE and the ITNinja community.

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 K1000. Managed devices that are running Agent version 5.4 and lower report inventory only to the <i>Software</i> page; they do not report inventory to the <i>Software Catalog</i> page. Managed devices that are running Agent version 5.5 and higher report inventory to both the <i>Software</i> page and the <i>Software Catalog</i> page.	Uses an inventory collection process introduced in version 5.5 of the K1000. 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 <i>Software Catalog</i> page.
Viewing software inventory information	The <i>Software</i> page displays information about all of the applications found on managed devices or added to K1000 inventory manually or through WSAPI.	Software inventory information is presented on the <i>Software Catalog</i> 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 K1000 manually or through WSAPI is not available under the <i>Software Catalog</i> page.
Metering applications	Not available.	Enabled for each application separately on the <i>Software Catalog</i> page or on the <i>Software Catalog Detail</i> page.

Task	Software page	Software Catalog 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 <i>License Compliance</i> page.	Enabled by creating a License asset and associating it with an application in the Software Catalog. License information appears on both the <i>License Compliance</i> 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 <i>Software Catalog Detail</i> page. See Mark applications and suites as Not Allowed .
Adding digital assets to applications	Available on <i>Software Detail</i> 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.
View ITNinja tips and information	Available on <i>Software Detail</i> pages. See Managing the ITNinja feed .	Not available.
Viewing summary license information	Available on the <i>License Compliance</i> and <i>Software License Configuration</i> chart on the <i>Dashboard</i> page. See About Dashboard widgets .	Available on the <i>License Compliance</i> and <i>Software License Configuration</i> chart on the <i>Dashboard</i> page. See About Dashboard widgets .
Setting threat levels for software	Available on the <i>Software</i> list. See Using software threat levels and categories .	Not available.
Setting software categories	Available on <i>Software Detail</i> 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 K1000 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 K1000 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 K1000 inventory, the Not Discovered application list cannot be exported in CSV format.

1. Go to the *Software Catalog* list:
 - a. Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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.

Item	Description
Recently Removed	The number of devices from which the application has been removed in the past seven days.

- 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.

- 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 K1000 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.

- Go to the *Software Catalog* list:
 - Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
 - On the left navigation bar, click **Inventory**, then click **Software Catalog**.
- 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.
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.

- 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 K1000 appliance, are referred to as Locally Cataloged applications. Locally cataloged applications can be metered, marked as Not Allowed, and associated with License assets.

- Go to the *Software Catalog* list:
 - Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
 - On the left navigation bar, click **Inventory**, then click **Software Catalog**.
- 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

- 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.
Publisher	The application's publisher. This information is normalized to ensure accurate reporting. For

Item	Description
	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.

- 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](#).

- Go to the *Software Catalog* list:
 - Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
 - On the left navigation bar, click **Inventory**, then click **Software Catalog**.
- 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	Whether the suite or application is marked as Not Allowed. Marking applications as Not Allowed prevents them from running on Agent-managed devices.
Metered	Whether 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.

Item	Description
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	Whether 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.

Item	Description
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.
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 is 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 <i>Dashboard</i> of the Administrator Console. Values

Item	Description
	that are marked as ignored on the <i>Asset Detail</i> 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 <i>Vendor</i> 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.
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 K1000 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 K1000 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 K1000 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 K1000 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 K1000 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 K1000 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 K1000 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 K1000, 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 **Add New License** to display the *License Asset Detail* page.
4. Provide the following information:

Option	Description
Subtype	The Asset Subtype to associate with the license. See About Asset Subtypes, custom fields, and device detail preferences .
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 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

Option	Description
	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 <i>Software Catalog</i> inventory and the <i>Software</i> 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 <i>License Compliance</i> page, select either <i>Enterprise</i> or <i>Unit License</i>. i NOTE: Most modes, including <i>Not Specified</i>, <i>Client License</i>, <i>Subscription</i>, <i>Shareware</i>, <i>Freeware</i>, <i>OpenSource</i>, <i>No Licensing</i>, and <i>Site License</i>, are not used for License Compliance. The license mode is used in these sections of the Administrator Console: • The <i>License Compliance</i> list. See View License Compliance information for Software Catalog applications. • The License Compliance chart that is displayed on the <i>Dashboard</i>. Values that are marked as ignored on the <i>Asset Detail</i> page are shown with a usage level of 100 percent. See About Dashboard widgets.
Product Key and Unit Cost	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 application. the <i>Vendor</i> drop-down list is empty unless you have added a Vendor asset. To search for a vendor, begin typing in the list. i 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 license was obtained. Click in the field, then select a date on the calendar.
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

Option	Description
	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. 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 <i>Upgrade Software list</i> box. You can add one or more versions, as needed. To delete an item from the list, select it in the <i>Upgrade Software list</i> 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 K1000 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. 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

Option	Description
	downgraded. When you click an entry in the list, your selection appears in the <i>Downgrade Software list</i> box. You can add one or more versions, as needed. To delete an item from the list, select it in the <i>Downgrade Software list</i> box, and click Remove. • No: If you do not want to grant downgrade rights to the selected software, select this option.
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, <i>Unapproved Software Installation</i> . However, the K1000 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.
Notes	Any additional information you want to provide.
License Text	Any supplemental information about the license, such as a license number.
Custom Fields	Additional information. You can modify the License Asset Type to include as many additional fields as necessary to meet your business objectives.

5. Click **Save**.

The new asset appears on the *Assets* 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
 - b. On the left navigation bar, 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.

Using software metering

You can manage software metering information using the KACE Systems Management Appliance (K1000).

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 K1000 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 K1000 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 K1000 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization 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 <i>Device Inventory</i> check box. You can select additional label types as needed, but Metering can be enabled only if the <i>Devices</i> label type is selected.

Option	Description
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. 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 <i>Label Group</i> 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 <i>Licenses</i> . 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**.

The *Devices* page appears.

- b. Select the check box next to one or more devices.
- c. Select **Choose Action > Label > 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 K1000 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization 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**.

The screenshot shows the 'Smart Label' configuration panel. It has a header with 'Choose Action', 'Advanced Search', 'Smart Label', and 'Notification'. The main area is titled 'Smart Label' and contains two criteria rows. The first row has 'Name' in a dropdown, 'contains' as the operator, and 'Windows' in a text field. The second row has 'Disk % Capacity' in a dropdown, '>' as the operator, and '95' in a text field. To the right of each row are 'AND' and 'OR' operator dropdowns, and 'Add Line' and 'Add Group' buttons. At the bottom, there is a 'Choose label:' dropdown, a 'Test' button, a 'Save' button, and a 'Metering Enabled' checkbox.

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 below 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.
 - 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**.

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 K1000 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

Icon	Description
	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.

- Go to the *Software Catalog* list:
 - Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
 - On the left navigation bar, click **Inventory**, then click **Software Catalog**.
- Select the check box next to an application that is Discovered, or Not Discovered.
- 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 K1000 appliance database.

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

- Do one of the following:
 - If the Organization component is enabled on your appliance, log in to the K1000 System Administration Console, http://K1000_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.

The *Organization Detail* page appears.

- If the Organization component is not enabled on your appliance, select **Settings > Provisioning**. Then click **Communication Settings** on the *Provisioning* panel.

The *Communication Settings* page appears.

2. In the *Communication Settings* section, specify the following settings:

Option	Suggested Setting	Notes
Agent Logging	Enabled	Whether the K1000 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 <i>Agent Logging</i> 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 <i>Agent Logging</i> .
Agent Inventory	12 hours	The frequency at which Agents on managed devices report inventory. This information is displayed in the <i>Inventory</i> section.
Agentless Inventory	1 Day	The frequency at which Agentless devices report inventory. This information is displayed in the <i>Inventory</i> section.
Catalog Inventory	24 hours	The frequency at which managed devices report inventory to the <i>Software Catalog</i> page.
Metering	4 hours	The frequency at which managed devices report metering information to the K1000 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**.

4. To configure data retention settings for metering, go to the Admin-level *General Settings* page:

- a. Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 K1000 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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.
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.

Column name	Description
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.

View metering information on the Device Detail page

You can view metering information for Software Catalog applications on the *Device Detail* page.

- Go to the *Devices* list:
 - Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
 - On the left navigation bar, click **Inventory**.
- Click the name of a managed device that has metering enabled to display the *Device Detail* page.
- In the *Software* section, 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.
Launches	The number of times the application has been launched on the device in the past seven days.

Column name	Description
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.

- Go to the *Software Catalog* list:
 - Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
 - On the left navigation bar, click **Inventory**, then click **Software Catalog**.
- Select the check box next to an application.
- Select **Choose Action > Disable Metering**.

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.

- Go to the *Labels* list:
 - Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
 - On the left navigation bar, in the **Home** section, click **Label Management**.
 - On the Label Management panel, click **Labels**.
- Select the check box next to a metering label.
- 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.

- Go to the *Smart Label Detail* page:

- a. Log in to the K1000 Administrator Console, `http://K1000_hostname/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization 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 K1000 System Administration Console, `http://K1000_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.

The *Organization Detail* page appears.

- If the Organization component is not enabled on your appliance, select **Settings > Provisioning**. Then click **Communication Settings** on the *Provisioning* panel.

The *Communication Settings* page appears.

2. In the *Communication Settings* section, specify the following settings:

Option	Suggested Setting	Notes
Agent Logging	Enabled	Whether the K1000 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 <i>Agent Logging</i> 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 <i>Agent Logging</i> .
Agent Inventory	12 hours	The frequency at which Agents on managed devices report inventory. This information is displayed in the <i>Inventory</i> section.

Option	Suggested Setting	Notes
Agentless Inventory	1 Day	The frequency at which Agentless devices report inventory. This information is displayed in the <i>Inventory</i> section.
Catalog Inventory	24 hours	The frequency at which managed devices report inventory to the <i>Software Catalog</i> page.
Metering	4 hours	The frequency at which managed devices report metering information to the K1000 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 blacklist 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 blacklisting 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 blacklisting applications

Application Control requirements must be met for applications to be blacklisted.

To block applications and prevent them from being launched on managed devices, you must:

- **Install the K1000 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 K1000 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 blacklisted.** 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 blacklisted

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 blacklisting 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 blacklisted

Some applications, such as plug-ins to other applications, cannot be blacklisted.

The following applications can be marked as Not Allowed but they cannot be blacklisted 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 blacklisted or prevented from running on the devices.

1. Go to the *Devices* list:

- a. Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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**.
2. Select the check boxes next to one or more devices.
3. Select **Choose Action > Apply Labels**.
4. Select the **ApplicationControlDevices** label.

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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 K1000 has the Organization component enabled, and you want to access a System-level report:

Log in to the K1000 System Administration Console, http://K1000_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 K1000 components.

- If your K1000 does not have the Organization component enabled, or if you want to access an organization-level report, log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the 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 K1000 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.

Option	Description
Subtopic	Device
4. Click Next to display the <i>Fields to Display</i> 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 <i>Column Order</i> 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 <i>Sort and Breaks</i> page.	
8. Select Sort and Break options, then click Next to display the <i>Filters</i> 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 <i>Reports</i> list appears with the new report listed. the <i>View By</i> 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 <i>Generate Report</i> 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.

- Go to the *Software Catalog* list:
 - Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
 - On the left navigation bar, click **Inventory**, then click **Software Catalog**.
- Select the check box next to one or more applications.
- 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 K1000 appliances 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 K1000 Administrator Console, http://K1000_hostname/admin, then click **Settings**.
 - If the Organization component is enabled on the appliance, log in to the K1000 System Administration Console, http://K1000_hostname/system, or select **System** in the drop-down list in the top-right corner of the page, then click **Settings**.
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 K1000 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 K1000 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 blacklist processes. However, you can blacklist 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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
Assign 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: a. Safe b. Fairly Safe c. Unknown d. Could be harmful e. 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 **Save**.

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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 K1000 appliance does not enforce policies based on threat levels.

1. Go to the *Processes* list:
 - a. Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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
Assign 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: a. Safe b. Fairly Safe c. Unknown d. Could be harmful e. 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 K1000 appliance does not enforce policies based on threat levels.

1. Go to the *Startup Programs* list:

- a. Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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
Assign To Label	(Optional) the label associated with the item.

Option	Description
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: a. Safe b. Fairly Safe c. Unknown d. Could be harmful e. Harmful

3. Click **Save**.

Add labels for services

Add manual labels to manage services in inventory as a group.

1. Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 K1000 appliance does not enforce policies based on threat levels.

1. Go to the *Services* list:
 - a. Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 K1000 Agent.

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 K1000 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 K1000 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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.

Option	Description
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 <i>Add/Remove Programs</i> 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: <pre>RegistryValueGreaterThan(HKEY_LOCAL_MACHINE\Software\Network Associates\TVD\ Network Associates\TVD\Shared Components\ VirusScanEngine\4.0.xx,szDatVersion,4.0.44)</pre> - Next to <i>Upload and Associate File</i>, 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. - 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. Optional: Select a <i>Category</i> and <i>Threat Level</i> for the software. - 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 K1000 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\Microsoft\Internet Explorer\
Version Vector, IE, 10.000)
RegistryValueEquals (HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\
Version Vector,IE,10.000)
```

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 registry 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 > Software > Custom_item: Detail* page.

Conditional rule reference

The following table describes which data types can be used for comparison.

Table 23. 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

Conditional rule	Data types supported for comparison functions
	Equals, GreaterThan, LessThan
FileVersion	TEXT
PlistValue	NUMBER, TEXT
ProductVersion	TEXT
RegistryValue	TEXT

The following table describes how comparisons are made.

Table 24. 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 K1000 database uses the 24-hour clock (0 – 24 hours). - The timestamp listed in the K1000 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 25. 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.
FileVersionEqual (path, version)	X			Verifies that the Version > File Version property of the file specified in the path matches the TEXT value you entered.
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

Syntax	Win	RHEL	OS X	Description
				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.
RegistryValueGreaterThan (registryPath, valueName, value)	X			Verifies that the registry entry is higher than the

Syntax	Win	RHEL	OS X	Description
valueName, value)				value you specify. Value is a TEXT.
EnvironmentalVarXableExists (var)		X	X	Verifies that an environment variable with the name you specify exists.
EnvironmentalVarXableGreaterThan (var, type, value)		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.
EnvironmentalVarXableLessThan (var, type, value)		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.
EnvironmentalVarXableEquals (var, type, value)		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.

Syntax	Win	RHEL	OS X	Description
<code>PlistValueLessThan</code> (fullpath, entry, type, value)			X	Verifies that the named value is a NUMBER or TEXT lower than the value you specified.
<code>PlistValueEquals</code> (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 `FilenameMatchingRegex`, 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 K1000 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: Testing Internet Explorer version

To verify that the Internet Explorer is version 10.0.9200.17148:

```
FileVersionEquals(C:\Program Files\Internet Explorer\iexplore.exe, 10.0.9200.17148)
```

Specifying the version as 10.0.9 would return false. The version argument in a `Equals` function must be precise. A partial number will fail when the full version is longer.

Example: Detecting Windows XP Service Pack 2

Windows XP Service Pack 2 appears in *Add/Remove programs* for devices that were originally on SP1 then upgraded to SP2 only. The default application inventory for this item does not reflect devices that are already on SP2 because they were originally imaged at the SP2 level.

When using the appliance to deploy Windows XP Service Pack 2, 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, SP1 devices that have been upgraded, as well as devices originally imaged with SP2).

Comparing device values (Greater Than and Less Than rules)

Functions whose names end with `GreaterThan` and `LessThan` compare values as listed in [Table 23](#).

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 than 10

To verify that the product version is higher than 10:

```
ProductVersionGreaterThan(C:\Program Files\Internet Explorer\iexplorer.exe, 10)
```

To verify that the production version is 10 (that is equal to 10) or higher, enter the following:

```
ProductVersionEquals(C:\Program Files\Internet Explorer\iexplorer.exe, 10)  
OR ProductVersionGreaterThan(C:\Program Files\Internet Explorer\iexplorer.exe,  
10)
```

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\Internet Explorer\iexplorer.exe, 9)  
AND ProductVersionLessThan(C:\Program Files\Internet Explorer\iexplorer.exe, 10)
```



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 K1000 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 Windows Internet Explorer product version

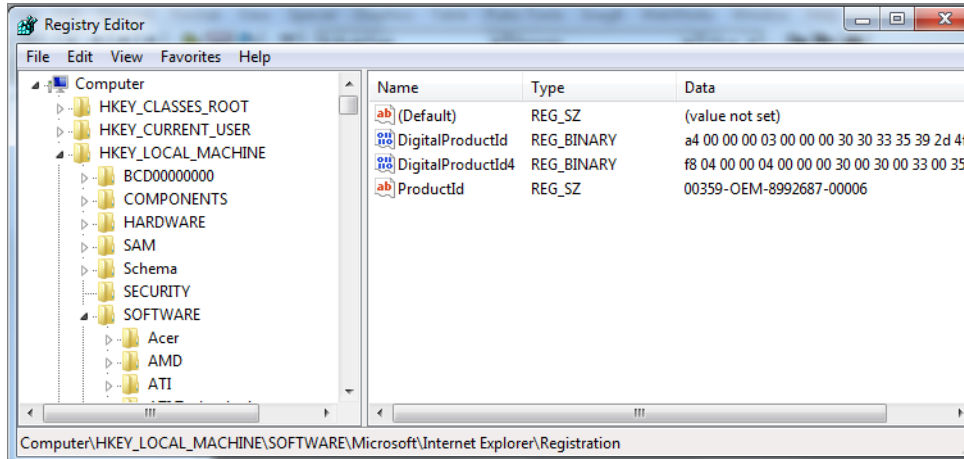
The following example sets the *Custom Inventory Field* for the Internet Explorer Product Version as a NUMBER:

In the *Custom Inventory Field*, enter the following:

```
FileInfoReturn(C:\Program Files\Internet Explorer\iexplore.exe,ProductVersion,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 Internet Explorer ProductID key

To set the ProductID registry key as a *Custom Inventory Field*:

```
RegistryValueReturn (HKEY_LOCAL_MACHINE\application\Microsoft\Internet Explorer\
Registration, ProductId, 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 native 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 K1000 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 K1000 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.	.*\.txt\$	abcFile.xls Example.jpg File.doc Myabc.txt	Myabc.txt

Character	Description	Example Expression	Target Files	Files Matched
	For more information, go to http://rexegg.com/regex-capture.html .		MyFile.abc	
^	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

Character	Description	Example Expression	Target Files	Files Matched
()	Parentheses enclosing characters create a back reference and match the preceding characters and/or the enclosed characters. For more information, go to http://rexegg.com/regex-capture.html .	(p) \1	a.log1 afile.txt3 app.log appconf.log11 mylog.log10	app.log appconf.log11
{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
<code>FileNamesMatchingRegexExist (fullpath, regex)</code>	X	X	X	Returns true if any files in the specified directory match the filename you entered using a regular expression.
<code>FileNamesMatchingRegexGreaterThan (fullpath, regex, value)</code>	X	X	X	True if the number of files that match is more than the value.
<code>FileNamesMatchingRegexLessThan (fullpath, regex, value)</code>	X	X	X	True if the number of files that match is less than the value.
<code>FileNamesMatchingRegexEqual (fullpath, regex, value)</code>	X	X	X	True if the number of files that match is the same as the value.

Syntax	Win	RHEL	OS X	Description
<code>FileNamesMatchingRegexReturn (fullpath, regex, type)</code>	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 K1000 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 K1000 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 K1000 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.
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.

Attribute	Type	Description
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.
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

Attribute	Type	Description
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 K1000 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 K1000 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 K1000 Agent installed.
2. Enter the following command: `kdeploy -custominventory`

The Agent contacts the K1000 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 K1000 appliance.

Distributing software and using Wake-on-LAN

You can distribute applications, updates, and files from the K1000 Management Appliance to managed devices. In addition, you can use Wake-on-LAN to power on devices remotely.

About software distribution

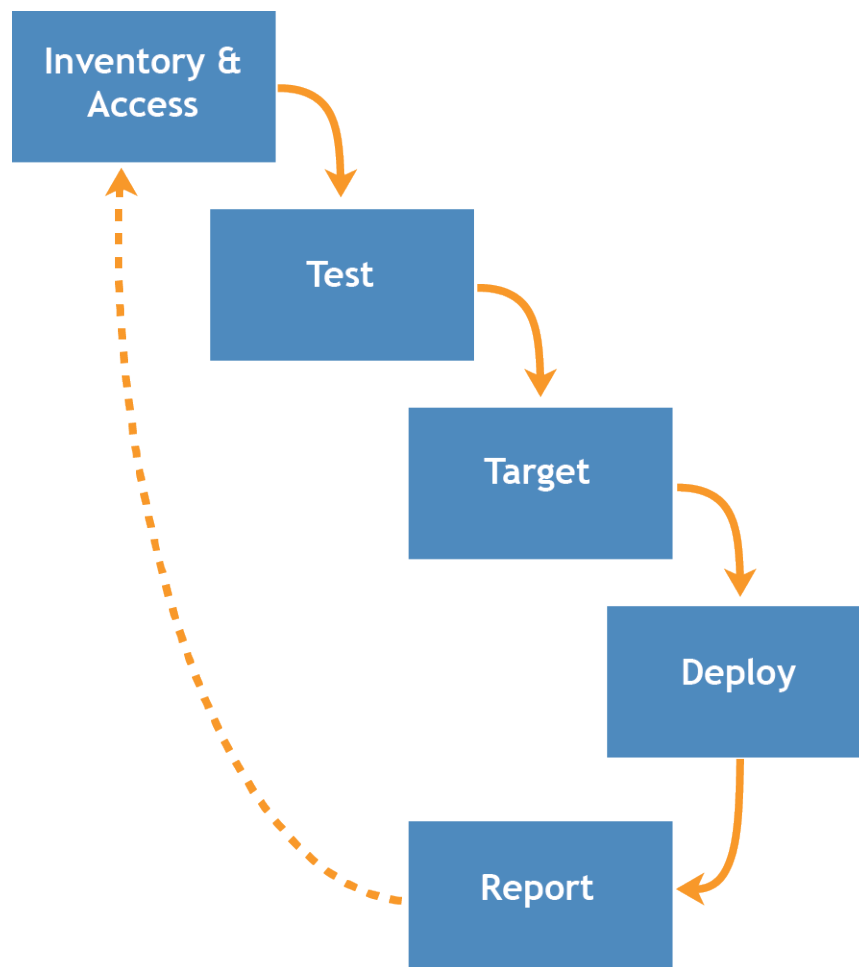
Software can be distributed from the K1000 appliance to Agent-managed Windows, Mac, and Linux devices.



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 8. 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 Synchronizations](#).
- **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 [Add MSI Installer scripts](#).

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 K1000 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 a K1000 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 K1000 Agent always looks to the appliance for distribution files if:

- No Replication Share is specified for any label applied to a device.
- More than one Replication Share is identified.

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 K1000 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 K1000. In this way, the K1000 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.

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 Mac OS 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 K1000 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 K1000 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 a 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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**.

c. Select **Choose Action > New**.

2. In the *Configure* section, provide the following information:

Option	Description
Name	A name that identifies the Managed Installation. This name appears on the <i>Managed Installations</i> 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 K1000 Agent reports inventory information to the appliance. • At bootup: Deploy the package the next time the device starts up. i 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. • While user logged in: Deploy the package while the user is logged on. • While 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 <i>Software</i> or <i>Cataloged Software</i> field. • 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.

Option	Description
Alternate Location	Specify a location from which files can be downloaded for a specific Managed Installation. Path: Enter the location where the K1000 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, <code>\fileserver_one\software\adobe.exe</code>). You can create the checksum using any tool, including <code>KDeploy.exe</code>, which is installed with the K1000 Agent. To create the checksum using KDeploy.exe: - On a device with the K1000 Agent installed, open a command prompt or terminal window. - Go to the Quest KACE installation directory. For example: Windows 32-bit devices: <code>C:\Program Files\Dell\KACE</code> Windows 64-bit devices: <code>C:\Program Files (x86)\Dell\KACE</code> Mac OS X devices: <code>/Library/Application Support/Dell/KACE/bin</code> - Enter the following command: <code>KDeploy -hash=filename</code> Where filename is the UNC path to the file. If the path contains spaces, enclose the entire path in double quotation marks. - 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 new credential to add credentials not already listed. See Add and edit User/Password credentials. i 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.

Option	Description
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 msixexec.exe: Prevent the appliance from adding <code>msixexec.exe</code> to the beginning of the file.
Delete Downloaded Files	Delete the files when the deployment is complete.
ITNinja	Deployment tips from ITNinja. These tips are available only if you share usage data. See Configure data sharing preferences .

3. Specify deployment settings:

Option	Description
All Devices	Deploy to all devices. Clear the check box to limit the deployment to specific labels or devices.
Labels	Limit deployment to devices that belong to specified labels. To select labels, click Edit, drag labels to the <i>Limit Deployment to</i> 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

Option	Description
	characters in the <i>Devices</i> field. The number next to the field indicates the number of devices available.

4. Specify the user notification settings:

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.
- **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 Schedule options:

Option	Description
Deployment Window Start End	The time, in 24-hour clock format, for package deployment to start and end. The <i>Deployment Window</i> time affects all <i>Action</i> options. Also, the run intervals defined in the appliance <i>Settings</i> 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.
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.

- 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 K1000 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the 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**.
 - 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 *Run 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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**.
 - 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 K1000 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.

i **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 K1000 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 K1000 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 <i>Managed Installations</i> page.
Execution	Select the most appropriate time for this package to be deployed. For the Linux platform, the options are Execute 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 <i>Software</i> or <i>Cataloged Software</i> field. - 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 K1000 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, <code>\fileserver_one\software\adobe.exe</code>). You can create the checksum using any tool, including KDeploy.exe, which is installed with the K1000 Agent. To create the checksum using KDeploy.exe: - On a device with the K1000 Agent installed, open a command prompt or terminal window. - Go to the Quest KACE installation directory. For example: Windows 32-bit devices: <code>C:\Program Files\Dell\KACE</code> Windows 64-bit devices: <code>C:\Program Files (x86)\Dell\KACE</code> Mac OS X devices: <code>/Library/Application Support/Dell/KACE/bin</code> - Enter the following command: <code>KDeploy -hash=filename</code> Where filename is the UNC path to the file. If the path contains spaces, enclose the entire path in double quotation marks.

Option	Description
	d. 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 new credential to add credentials not already listed. See Add and edit User/Password credentials. i 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.
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" Run Parameters: (Optional) If you select Use Default, specify the parameters to use. Run 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: <pre>rpm -ivh --replacepkgs package.rpm</pre>
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 <i>Full Command Line</i> field, the command runs. Otherwise, the K1000 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.

Option	Description
Delete Downloaded Files	Delete the files when the deployment is complete.
ITNinja	Deployment tips from ITNinja. These tips are available only if you share usage data. See Configure data sharing preferences .
4. Specify deployment settings:	
Option	Description
All Devices	Deploy to all devices. Clear the check box to limit the deployment to specific labels or devices.
Labels	Limit deployment to devices that belong to specified labels. To select labels, click Edit, drag labels to the <i>Limit Deployment to</i> 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 <i>Devices</i> field. The number next to the field indicates the number of devices available.
5. Specify the user notification settings:	
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. • 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.

Option	Description
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 Schedule options:

Option	Description
Deployment Window	The time, in 24-hour clock format, for package deployment to start and end. The <i>Deployment Window</i> time affects all <i>Action</i> options. Also, the run intervals defined in the appliance <i>Settings</i> interact with or override the deployment window of specific packages.
Start	
End	
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.
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 K1000 Administrator Console, `http://K1000_hostname/admin`. Or, if the *Show organization menu in admin header* option is enabled in the 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**.
 - 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 *Run 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 K1000 Agent automatically runs deployment packages with RPM extensions.

Create Managed Installations for Mac OS X devices

You can create Managed Installations for Mac OS 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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**.
 - c. Select **Choose Action > New**.
2. Select the application in the *Software* drop-down list.

By default, the K1000 Agent attempts to install the PKG file using the following command:

```
installer -pkg packagename.pkg -target / [Run Parameters]
```

If you have selected a ZIP, TGZ, or TAR.GZ file, 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 <i>Managed Installations</i> 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 K1000 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. • While user logged in: Deploy the package while the user is logged on. • While user logged off: Deploy the package only when the device is running and the user is logged off.

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 <i>Software</i> or <i>Cataloged Software</i> field. - 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 K1000 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, <code>\fileserver_one\software\adobe.exe</code>). You can create the checksum using any tool, including KDeploy.exe, which is installed with the K1000 Agent. To create the checksum using KDeploy.exe: - On a device with the K1000 Agent installed, open a command prompt or terminal window. - Go to the Quest KACE installation directory. For example: Windows 32-bit devices: <code>C:\Program Files\Dell\KACE</code> Windows 64-bit devices: <code>C:\Program Files(x86)\Dell\KACE</code> Mac OS X devices: <code>/Library/Application Support/Dell/KACE/bin</code> - Enter the following command: <code>KDeploy -hash=filename</code> Where filename is the UNC path to the file. If the path contains spaces, enclose the entire path in double quotation marks.

Option	Description
	d. 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 new credential to add credentials not already listed. See Add and edit User/Password credentials. i 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: <pre>installer -pkg packagename.pkg - target / [Run Parameters]</pre> or <pre>ditto -rsrc packagename.app / Applications/theapp</pre> 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. • Uninstall: Uninstall the application from the command line. • Run Command Only (do not download file): Run the command line only. • Don't Prepend msixexec.exe: Prevent the appliance from adding <code>msixexec.exe</code> to the beginning of the file.
Delete Downloaded Files	Delete the files when the deployment is complete.

Option	Description
ITNinja	Deployment tips from ITNinja. These tips are available only if you share usage data. See Configure data sharing preferences .



NOTE: User notification messages are not available on Mac OS X devices.

4. Specify deployment settings:

Option	Description
All Devices	Deploy to all devices. Clear the check box to limit the deployment to specific labels or devices.

Labels	Limit deployment to devices that belong to specified labels. To select labels, click Edit, drag labels to the <i>Limit Deployment to</i> 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 <i>Devices</i> field. The number next to the field indicates the number of devices available.

5. Select Schedule options:

Option	Description
Deployment Window	The time, in 24-hour clock format, for package deployment to start and end. The <i>Deployment Window</i> time affects all <i>Action</i> options. Also, the run intervals defined in the appliance <i>Settings</i> interact with or override the deployment window of specific packages.
Start	
End	

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.

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 Synchronizations

Using File Synchronizations, you can push out any type of file to Agent-managed devices.

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.

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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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
Enabled	Enable the File Synchronization. When the K1000 Agents on selected devices check in to the appliance, the file is distributed.
Name	A name that identifies the File Synchronization. This name appears on the <i>File Synchronizations</i> page.
Path	The directory location, on target devices, to which you want to save the file.
Create Path	Create the location specified in the <i>Path</i> 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 new 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.

Option	Description
Persist	Confirm that the file does not already exist on target devices before attempting to distribute it.
Create Shortcut	Create a desktop shortcut to the file location on the device.
Name	The display name for the desktop shortcut.
Delete Temporary Files	Delete the files when the deployment is complete.
ITNinja	Deployment tips from ITNinja. These tips are available only if you share usage data. See Configure data sharing preferences .

3. Specify deployment settings:

Option	Description
All Devices	Deploy to all devices. Clear the check box to limit the deployment to specific labels or devices.
Labels	Limit deployment to devices that belong to specified labels. To select labels, click Edit, drag labels to the <i>Limit Deployment to</i> 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 <i>Devices</i> field. The number next to the field indicates the number of devices available.
Initial Message	Display a message on devices before installation.
Completion Message	Display a message on devices after the installation is complete.
Blackout Window	The time during which Agents on managed devices are prevented from performing File Synchronizations.
Alternate Location	Specify a location from which files can be downloaded for a specific Managed Installation. Path: Enter the location where the K1000 Agent can retrieve digital installation files. Checksum: Enter an alternate checksum (MD5) that matches the MD5 checksum on the remote

Option	Description
	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, <code>\fileserver_one\software\adobe.exe</code>). You can create the checksum using any tool, including <code>KDeploy.exe</code>, which is installed with the K1000 Agent. To create the checksum using KDeploy.exe: - On a device with the K1000 Agent installed, open a command prompt or terminal window. - Go to the Quest KACE installation directory. For example: Windows 32-bit devices: <code>C:\Program Files\Dell\KACE</code> Windows 64-bit devices: <code>C:\Program Files (x86)\Dell\KACE</code> Mac OS X devices: <code>/Library/Application Support/Dell/KACE/bin</code> - Enter the following command: <code>KDeploy -hash=filename</code> Where filename is the UNC path to the file. If the path contains spaces, enclose the entire path in double quotation marks. - 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 new credential to add credentials not already listed. See Add and edit User/Password credentials. i 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.
4. Click Save .	i TIP: To distribute files previously deployed after the deployment window has closed, go to the <i>File Synchronization Detail</i> 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 K1000 appliance regardless of whether the devices have the K1000 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 K1000 broadcasts UDP traffic on your network on port 7. The K1000 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.

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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 *IP Address* field, specify the IP address of a device.
 - In the *Manual 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.

1. Go to the *Wake-on-LAN Schedules* list:
 - a. Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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. 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 devices by operating system, select the operating systems of the devices you want to wake in the *Operating Systems* field. Otherwise, leave the *Operating Systems* field blank to wake devices with any operating system.
4. In the *Schedule* section, specify the schedule settings:

Option	Description
None	Run in combination with an event rather than on a specific date or at a specific time.
Run every 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.

5. 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://support.intel.com/support/network/sb/cs-008459.htm>.

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 [Configuring Agent settings](#).



NOTE: This type of alert is generated at the K1000, to be broadcast to Agent-managed devices. The other type of alert is the monitoring alert, which comes into the K1000 from your server devices if you have enabled monitoring on them to perform basic performance monitoring. See [Monitoring servers](#).

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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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:

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 K1000 Agents are connected to the appliance.
Devices	Display the message on specified devices. Use Ctrl-click or Command-click to select multiple devices.
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 K1000, 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 K1000, the alert message is sent to the Agent Command Queue, and it remains there until the device connects to the K1000. When the target device connects, the message appears regardless of whether the *Expiration* time has elapsed.

3. In the *Schedule* section, 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.
Custom	Run according to a custom schedule. Use standard 5-field cron format (extended cron format is not supported): <pre>* * * * * +-----day of week (0-6) (Sun=0) +-----month (1-12) +-----day of month (1-31) +-----hour (0-23) +-----minute (0-59)</pre> 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:

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 K1000 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 26. Default scripts

Script Name	Description
Defragment the C: drive	Defragments drive C on the device.
Force Check-In	Forces Windows devices with the K1000 Agent installed to take inventory and sync with the K1000. WARNING: 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 K1000 Agent installed to take inventory and sync with the K1000. WARNING: 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.

Script Name	Description
Issue a DOS Command Example	Issues the <code>DOS-Dir</code> command on a Windows device. Used as an example for how to run a DOS command.
Issue a Mac Command Example	Issues the <code>AppDir.txt</code> 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 Agent Debug Log Disable (Mac/Linux)	On Mac and Linux devices, disables the debug switch used with the K1000 Agent debug logs.
K1000 Agent Debug Log Disable (Windows)	On Windows devices, disables the debug switch used with the K1000 Agent debug logs.
K1000 Agent Debug Log Enable (Mac/Linux)	On Mac and Linux devices, if the K1000 Agent is checking in, but something is still not quite right, this script enables the debug flag. This option provides additional debugging information for Agent-related activities such as AMP, Inventory, and Scripting, and sends the output back to the K1000. It does not enable debugging of the scheduling service.
K1000 Agent Debug Log Enable (Windows)	On Windows devices, if the K1000 Agent is checking in, but something is still not quite right, this script enables the debug flag. This option provides additional debugging information for Agent-related activities such as AMP, Inventory, and Scripting, and sends the output back to the K1000. It does not enable debugging of the scheduling service.
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 K1000 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.
Message Window Script Example	Illustrates the use of the Message Window. Your script must have properly paired create/destroy

Script Name	Description
	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. i 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 <code>ResetKUIDRunOnce</code> 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 <code>-t</code> 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 or online KScripts](#).



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 27. 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: <code>\$(KACE_DATA_DIR)packages\kbots\xxx</code> 5.1: <code>\$(KACE_INSTALL)packages\kbots\xxx</code>
\$(KACE_INSTALL) \$(KACE_DEPENDENCY_DIR) \$(KACE_INSTALL_DIR) \$(KBOX_INSTALL_DIR)	Installation directory for executables, scripts, packages, and so on. All are synonymous. Preferred: \$(KACE_INSTALL) 5.2 or higher, Win7/Vista: <code>C:\ProgramData\Dell\KACE</code> 5.2 or higher, XP: <code>C:\Documents and Settings\All Users\Dell\KACE</code> 5.2 or higher, Mac OS X: <code>/Library/Application Support/Dell/KACE/bin</code> 5.2 or higher, Linux: <code>/opt/dell/kace/bin</code> 5.1 Windows: <code>C:\Program Files\KACE\KBOX</code>
\$(KACE_SYS_DIR) \$(KBOX_SYS_DIR)	Agent device's system directory. Both are synonymous. Preferred: \$(KACE_SYS_DIR) . Windows: <code>C:\Windows\System32</code> Mac OS X: <code>/</code> Linux: <code>/</code>
\$(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) (<code>http://kace.kbox.com:80</code>). Both are synonymous. Preferred: \$(KACE_IP_ADDRESS)
\$(KACE_SERVER_URL)	Combination of server, port, and URL prefix. (<code>http://kace.kbox.com:80</code>)
\$(KACE_SERVER)	Hostname of K1000 server. (kbox)

Item	Description
\$(KACE_SERVER_PORT)	Port to use when connecting to the K1000 server. (80/433)
\$(KACE_SERVER_URLPREFIX)	Web protocol to use when connecting to the K1000 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. For older Agents this is mapped to \$(KACE_INSTALL) . 5.2 or higher, Windows: C:\Program Files\Dell\KACE or C:\Program Files (x86)\Dell\KACE 5.2 or higher, Mac OS X: /Library/Application Support/Dell/KACE/bin 5.2 or higher, Linux: /opt/dell/kace/bin 5.1: \$(KACE_INSTALL)
\$(KACE_DATA_DIR)	Installation directory for executables, scripts, packages, and so on. For older Agents this is mapped to \$(KACE_INSTALL) . 5.2 or higher, Win7/Vista: C:\ProgramData\Dell\KACE 5.2 or higher, XP: C:\Documents and Settings\All Users\Dell\KACE 5.2 or higher, Mac OS X: /Library/Application Support/Dell/KACE/data 5.2 or higher, Linux: /var/dell/kace 5.1: \$(KACE_INSTALL)
\$(KACE_AGENT_VERSION)	Substitutes the version number of the installed Agent. "6.0.12345". 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.

Item	Description
\$(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 or online KScripts

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*.

- Go to the *Script Detail* page:
 - Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
 - On the left navigation bar, click **Scripting**.
 - Select **Choose Action > New**.
- In the *Configure* section, specify script settings:

Option	Description
Name	A meaningful name for the script that distinguishes it from others on the <i>Scripts</i> list.
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.
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

Option	Description
	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.
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.
Description	(Optional) A brief description of the actions the script performs. This field helps you to distinguish one script from another on the <i>Scripts</i> list.
Notes	Any additional information you want to provide.

3. In the *Deploy* section specify deployment options:

Option	Description
All Devices	Deploy to all devices. Clear the check box to limit the deployment to specific labels or devices.
Labels	Limit deployment to devices that belong to specified labels. To select labels, click Edit, drag labels to the <i>Limit Deployment to</i> 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.
Operating Systems	Limit deployment to devices that have the specified operating systems. Leave the Operating Systems field blank to deploy the script to all operating systems.
Select Specific Operating Systems	Limit deployment to devices that have specific versions of operating systems. If this check box is cleared, the script runs on all versions of specified operating systems.

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.  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.

- In the *Notify* section, specify user alert settings. Alerts are available only for online KScripts and online shell scripts on Windows and Mac devices running the K1000 Agent version 5.1 and higher:

Option	Description
Alert 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 <i>Snooze Duration</i>. If the time specified in the <i>Timeout</i> elapses without a user response, the script runs at that time. Interaction with <i>Run As</i>: - Only the console user can see the alert dialog, and therefore choose to Snooze or Cancel, regardless of the <i>Run As</i> setting. - Enabling an alert prompts the console user even if the script is set to run as all users or another user.

Option	Description
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 <i>Timeout</i> 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* section, specify run options:

Option	Description
None	Run in combination with an event rather than on a specific date or at a specific time.
Every nth minutes/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 or on a specific month at HH:MM	Run on the same day every month, or a specific month, at the specified time.
Custom Schedule	Run according to a custom schedule. Use standard 5-field cron format (extended cron format is not supported): <pre>* * * * * +-----day of week (0-6) (Sun=0) +-----month (1-12) +-----day of month (1-31) +-----hour (0-23) +-----minute (0-59)</pre> 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

Option	Description
	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:
Also run once at next device checkin (for offline KScripts only)	Runs the offline KScript once when new scripts are downloaded from the appliance.
Also Execute 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. i 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 Execute after login (before desktop loads) (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

Option	Description
	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.

7. 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.

i **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.

8. In the *Tasks* section, click **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 <i>Verify</i> 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 .

9. 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.

1. Go to the *Script Detail* page:
 - a. Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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**.
 - 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 or online KScripts](#).
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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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**.
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 K1000 Administrator Console, `http://K1000_hostname/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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**.
 - 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="" type="policy" id="0" 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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**.
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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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**.
 - 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 K1000 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.
- *Mac Profile Detail*: Using the **Run Now** command on the *Mac Profile Detail* page runs a script that installs or removes the selected Mac profile on target devices that have an Agent connection to the K1000 appliance.
- *Mac Profiles*: Selecting **Choose Action > Run** on the *Mac Profiles* page runs scripts that install or remove multiple Mac profiles at the same time, provided that target devices have an Agent connection to the K1000 appliance.

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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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
All Devices	Deploy to all devices. Clear the check box to limit the deployment to specific labels or devices.
Labels	Limit deployment to devices that belong to specified labels. To select labels, click Edit, drag labels to the <i>Limit Deployment to</i> 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.

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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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**.
 - 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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**.
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 K1000 Agent from listening on port 52230.

The **Run Now** command communicates over port 52230. Scripts might fail to deploy if firewall settings block the K1000 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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.

About configuration policy templates

Configuration policy templates enable you to create policy-related scripts. These scripts can be deployed to configure policies on managed devices.

This section includes descriptions of the settings for each of the scripts you can create.

The Windows templates include:

- [Add Automatic Update scripts](#)
- [Add Dell Command | Monitor scripts](#)
- [Add Desktop Wallpaper scripts](#)
- [Add Desktop Shortcuts scripts](#)
- [Add Event Log Reporter scripts](#)
- [Add MSI Installer scripts](#)
- [Add Power Management scripts](#)
- [Add Registry scripts](#)[Add Registry scripts](#)
- [Add Remote Desktop Control Troubleshooter scripts](#)
- [Add UltraVNC scripts](#)
- [Add Uninstaller scripts](#)

The Mac OS X templates include:

- [Add Active Directory scripts](#)
- [Add Power Management scripts](#)
- [Add VNC scripts](#)

Using Windows configuration policies

You can create configuration policies or scripts to run on Windows devices using configuration policy templates.



NOTE: If you edit a template-based policy, keep the *Run As* setting as local system.

About starting Windows Automatic Updates on Windows devices

There are several ways to start Windows Automatic Updates on Windows managed devices.

To start Windows Automatic Updates, do one of the following:

- Enable the Windows Automatic Updates Settings policy of the appliance. See [Add Automatic Update scripts](#).
- Enable the local policy for Windows Automatic Updates on the device.
- Modify the registry key for Windows Automatic Updates on the device.
- Set up the Group Policy on the domain for Windows Automatic Updates on the device.

If you use K1000 patching to automatically deploy Windows updates on a device, you must disable Windows Automatic Updates on the device by any other process to avoid conflicts among the different deployment processes.

Add Automatic Update scripts

Use the Automatic Update template to create scripts that control how managed devices use the Windows Update process.

Windows Update is a Microsoft feature that automatically updates Windows devices with security and other important patches from Microsoft. Using the Windows Automatic Update policy, you can specify how and when Windows updates are downloaded to managed devices so that you can control the update process.

For more information about Windows Update, go to: <http://support.microsoft.com/kb/328010>.

1. Go to the *Windows Automatic Update* page:
 - a. Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 **Configuration Policies**.
 - c. On the *Configuration Policies* panel, in the *Windows* section, click **Automatic Updates**.
2. Provide the following information:

Option	Description
Name	A name that identifies the script. This name appears on the <i>Scripts</i> page.
(Recommended) Automatically download...	Enable the automatic downloading of Windows Updates.
Download updates for me, but let the end user choose when to install patches	Download updates, and provide installation options instead of installing updates automatically.
Notify the end user but do not automatically download or install patches	Receive notifications when updates are available, but prevent the appliance from downloading or installing updates.



IMPORTANT: This setting might make your network more vulnerable to attack if you neglect to retrieve and install the updates on a regular basis.

Option	Description
Turn off Automatic Updates	Prevent the device from using Windows Automatic Updates. This setting is recommended if you want to use the appliance patching feature to manage Windows patch updates.
Remove Admin Policy and let end user configure	Provide users with control over the updates downloaded.  IMPORTANT: Your network might be vulnerable to attacks if you select this option.
Reschedule Wait Time	The interval, in minutes, to wait before rescheduling an update if the update fails.
Do not reboot device while user logged in	Prevent automatic reboots when users are logged in.
SUS Server	The name of the server used for the Windows Server® Update Service.
SUS Statistics Server	The name of the statistics server used for the Windows Server Update Service.

3. Click **Save** to display the *Script Detail* page.
4. Select options for configuration, deployment, and scheduling. See [Add offline KScripts or online KScripts](#).
5. To edit the raw XML used in the script, click **Edit XML** below the *Schedule* section.
6. Click **Save**.

About Dell Command | Monitor

Dell Command | Monitor is the monitoring tool of the Dell Command Suite. With it, a remote management application such as the K1000 appliance can perform management and monitoring activities.

Using Dell Command | Monitor gives the K1000 the following abilities for certain Dell devices:

- Gain access to management information.
- Monitor device status.
- Change the state of enterprise client systems.

Earlier versions of Dell Command | Monitor were named Dell OpenManage™ Client Instrumentation (OMCI). The K1000 supports only Dell Command | Monitor 9.0 or higher.

Supported physical hardware

Dell Command | Monitor is available for the following Dell hardware.

- Dell Venue 11 Pro
- Dell OptiPlex™
- Dell Precision Workstation™
- Dell Latitude™

Supported Microsoft operating systems

The following operating systems are supported for Dell Command | Monitor.

- Microsoft Windows 8.1 (32-bit and 64-bit), Microsoft Windows 8.1 Professional (32-bit and 64-bit), and Enterprise (32-bit and 64-bit)
- Microsoft Windows 8 (32-bit and 64-bit), Microsoft Windows 8 Professional (32-bit and 64-bit), and Enterprise (32-bit and 64-bit)
- Microsoft Windows 7, Windows 7 Service Pack 1 (SP1), Professional, Enterprise, and Ultimate x86 (32-bit) and x64 (64-bit) editions
- Microsoft Windows Vista Business SP1 x86 (32-bit) and x64 (64-bit) editions
- Microsoft Windows Vista Ultimate SP1, and SP2 x86 (32-bit) and x64 (64-bit) editions
- Microsoft Windows Vista Enterprise SP1, and SP2 x86 (32-bit) and x64 (64-bit) editions

Classes and properties queried for information

The K1000, using Dell Command | Monitor, queries the following DCIM Windows Management Instrumentation (WMI) classes and properties.

The information returned from the queries appears in the *Dell Command | Monitor* group on the *Device Detail* page for the Dell hardware device in inventory.

You can create custom reports that collect any combination of the properties, using the report wizard. See [Create reports using the report wizard](#).

Class	Properties	Report wizard <i>Fields to Display</i> group	Report wizard <i>Fields to Display</i> item name
DCIM_FlatPanel	N/A	Dell Command Monitor - Flat Panel Display	Aspect Ratio
	DisplayType		Display Type
	HorizontalResolution		Horizontal Resolution
	PrimaryStatus		Primary Status
	VerticalResolution		Vertical Resolution
DCIM_DesktopMonitor	N/A	Dell Command Monitor - Monitor	Aspect Ratio
	CurrentResolutionH		Current Horizontal Resolution
	CurrentResolutionV		Current Vertical Resolution
	Description		Description
	InputDisplayPort		Supports DisplayPort
	InputDVI		Supports DVI
	InputHDMI		Supports HDMI

Class	Properties	Report wizard <i>Fields to Display</i> group	Report wizard <i>Fields to Display</i> item name
	ManufactureDate		Manufacture Date
	N/A		Physical Diagonal Size (cm)
	N/A		Physical Diagonal Size (in)
	PhysicalSizeH		Physical Horizontal Size (cm)
	PhysicalSizeV		Physical Vertical Size (cm)
	PrimaryStatus		PrimaryStatus
	SerialNumber		Serial Number
	StandbyModeSupported		Supports Standby Mode
	SuspendModeSupported		Supports Suspend Mode
	VeryLowPowerSupported		Supports Very Low Power Mode
DCIM_VProSettings	VProCharacteristics	Dell Command Monitor - vPro Settings	vPro Characteristics
DCIM_AMTSettings	AMTSupported	Dell Command Monitor - AMT Settings	AMT Supported
	IDEREnabled		IDE-R Enabled
	SOLEnabled		SOL Enabled
DCIM_PhysicalMemory	BankLabel	Dell Command Monitor - Physical Memory	Bank Label
	Capacity		Capacity (bytes)
	ElementName		Name
	ManufactureDate		Manufacture Date
	Manufacturer		Manufacturer
	MemoryType		Memory Type
	Model		Model

Class	Properties	Report wizard <i>Fields to Display</i> group	Report wizard <i>Fields to Display</i> item name
	PartNumber		Part Number
	PrimaryStatus		Primary Status
	SerialNumber		Serial Number
	Speed		Speed (MHz)
DCIM_Processor	Caption	Dell Command Monitor - Processor	Caption
	CurrentClockSpeed		Current Clock Speed (MHz)
	ElementName		Name
	MaxClockSpeed		Max Clock Speed (MHz)
	NumberOfEnabledCores		Number of Cores Enabled
	PrimaryStatus		Primary Status
	Stepping		Stepping
DCIM_ProcessorCapabilities	NumberOfHardwareThreads		Hardware Threads
	NumberOfProcessorCores		Number of Cores
DCIM_Battery	N/A	Dell Command Monitor - Battery	Charge Health (%)
	Chemistry		Chemistry
	DesignCapacity		Design Capacity (mWh)
	DesignVoltage		Design Voltage (mV)
	ExpectedLife		Expected Life (minutes)
	FullChargeCapacity		Full Charge Capacity (mWh)
	HealthState		Health State
	Name		Name
	PrimaryStatus		Primary Status
	RechargeCount		Recharge Count

Class	Properties	Report wizard <i>Fields to Display</i> group	Report wizard <i>Fields to Display</i> item name
DCIM_LogEntry	CreationTimeStamp	N/A	N/A
	RecordData		
	RecordFormat		

Hardware alerts available in reports from Dell Command | Monitor

The following settings determine how much alert information is included in a report created with the report wizard.

Report wizard <i>Fields to Display</i> group	Report wizard <i>Fields to Display</i> item name
Dell Command Monitor - Hardware Alerts	Category
	Description
	Severity
	Timestamp

Add Dell Command | Monitor scripts

Dell Command | Monitor is the monitoring tool of the Dell Command Suite. With it, a remote management application such as the K1000 appliance can perform management and monitoring activities. Using the *Dell Command | Monitor* page, you can name and save a Managed Installation for deploying or removing Dell Command | Monitor from K1000 managed devices that support the tool.

You have devices with supported Dell hardware and Microsoft operating systems. See [About Dell Command | Monitor](#).

You have downloaded Dell Command | Monitor from the Dell TechCenter at <http://en.community.dell.com/techcenter/enterprise-client/w/wiki/7531.dell-command-monitor>.



NOTE: Although this topic refers to installation, you can also use the *Dell Command | Monitor* page to remove Dell Command | Monitor from a device.

- Go to the *Windows Dell Command | Monitor* page:
 - Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
 - On the left navigation bar, click **Scripting**, then click **Configuration Policies**.
 - On the *Configuration Policies* panel, in the *Windows* section, click **Dell Command | Monitor**.
- Optional:** Change the name if you require a more precise name than the default.
- Set the *Action*, either keep the default **Install**, or change it to **Uninstall**.
- Click **Save** to display the *Managed Installation Detail* page with the configuration information filled in for the action you have chosen.

The K1000 automatically populates the *Name*, *Software*, *Associated Software*, and *Full Command Line* fields.

Complete filling out the needed information on the *Managed Installation Detail* page. See [Create Managed Installations for Windows devices](#).

Add Desktop Wallpaper scripts

Use this template to build scripts that control the desktop wallpaper settings of Windows devices.

The recommended format for wallpaper files is bitmap (BMP). The specified wallpaper file is distributed to devices when the script runs.

1. Go to the *Desktop Wallpaper* page:
 - a. Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 **Configuration Policies**.
 - c. On the *Configuration Policies* panel, in the *Windows* section, click **Desktop Wallpaper**.
2. Provide the following information:

Option	Description
Name	A name that identifies the script. This name appears on the <i>Scripts</i> page.
Use wallpaper	Display the wallpaper file on the desktop of target devices.
Wallpaper bitmap file	Click Browse or Choose File to select and upload the file to use for the wallpaper. The file must be in BMP or JPG format.
Position	Select an option in the <i>Position</i> drop-down list: • Stretch: Stretch the image so that it covers the entire screen. • Center: Display the image in the center of the screen. • Tile: Repeat the image over the entire screen.

3. Click **Save** to display the *Script Detail* page.
4. Select options for configuration, deployment, and scheduling. See [Add offline KScripts or online KScripts](#).
5. To edit the raw XML used in the script, click **Edit XML** below the *Schedule* section.
6. Click **Save**.

Add Desktop Shortcuts scripts

Use this template to create scripts that add Internet shortcuts to the Desktop or *Start* menu of Windows devices.

For example, you could use this script to add a shortcut to a company website or any other URL.

1. Go to the *Windows Desktop Shortcuts* page:
 - a. Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 **Configuration Policies**.
 - c. On the *Configuration Policies* panel, in the *Windows* section, click **Desktop Shortcuts**.
2. Provide the following information:

Option	Description
Name	A name that identifies the script. This name appears on the <i>Scripts</i> page.
3. Click Add Shortcut .	
4. Specify shortcut settings:	
Option	Description
Name	The text label that appears below or next to the shortcut.
Target	The full path to the application, file, or URL to be launched when the shortcut is selected. For example: To create shortcut for explorer.exe, use this format: C:\WINDOWS\explorer.exe To create a shortcut from the UNC share for explorer.exe, use this format: \\192.168.1.1\WINDOWS\explorer.exe or \\HostName\WINDOWS\explorer.exe
Parameters	The command line parameters required for the shortcut. For example: /S /IP=123.4
Working Directory	The changes to the current working directory. For example: C:\Windows\Temp
Location	The location where you want the shortcut to appear. Options include: Desktop and Start Menu.

- Click **Save Changes** to save the shortcut.
- Click **Add Shortcut** to add more shortcuts. To edit or delete a shortcut, hover over a shortcut and click the **Edit** button or the **Delete** button:  .
- Click **Save** to display the *Script Detail* page.
- Select options for configuration, deployment, and scheduling. See [Add offline KScripts or online KScripts](#).
- To edit the raw XML used in the script, click **Edit XML** below the *Schedule* section.
- Click **Save**.

Add Event Log Reporter scripts

Use this template to create scripts that query the Windows Event Log and upload the results to the appliance.

- Go to the *Windows Event Log Reporter* page:
 - Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
 - On the left navigation bar, click **Scripting**, then click **Configuration Policies**.
 - On the *Configuration Policies* panel, in the *Windows* section, click **Event Log Reporter**.
- Provide the following information:

Option	Description
Name	A name that identifies the script. This name appears on the <i>Scripts</i> page.
Output File Name	The name of the log file created by the script.
Log File	The type of log you want to query: Software, System, or Security.
Event Type	The type of event you want to query: Information, Warning, or Error.
Source Name	(Optional) The names of sources to which the query is restricted.

3. Click **Save** to display the *Script Detail* page.
4. Select options for configuration, deployment, and scheduling. See [Add offline KScripts or online KScripts](#).
5. To edit the raw XML used in the script, click **Edit XML** below the *Schedule* section.
6. Click **Save**.
7. To view the event log of a device, click **Inventory**, then click a device name.
8. In *Scripting Logs*, under *Currently Deployed Jobs and Policies*, click the **View logs** link next to *Event Log*.

Add MSI Installer scripts

Use this template to create scripts that set the basic command-line arguments for running MSI-based installers on Windows devices.

For command-line options, go to the Microsoft MSI Command-Line documentation: <http://msdn.microsoft.com/en-us/library/windows/desktop/aa367988%28v=vs.85%29.aspx>.

1. Go to the *Windows MIS Installer* page:
 - a. Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 **Configuration Policies**.
 - c. On the *Configuration Policies* panel, in the *Windows* section, click **MSI Installer**.
2. Provide the following information:

Option	Description
Name	A name that identifies the script. This name appears on the <i>Scripts</i> page.
Action	The task to be performed. Tasks include Install , Uninstall , Repair missing files , and Reinstall all files .
Software	The application to use for the script. To search for an application, begin typing in the field.
MSI Filename	The MSI filename (required if the file is a ZIP archive).

Option	Description
User Interaction	How the installation appears to users. Options include: Default , Silent , Basic UI , Reduced UI , and Full UI .
Install Directory	The directory on the target device where the application is to be installed.
Additional Switches	Any additional installer switches. Additional switches are inserted between the <code>msiexec.exe</code> and the <code>/i foo.msi</code> arguments.
Additional Properties	Any additional properties. These properties are inserted at the end of the command line. For example: <pre>msiexec.exe /s1 /switch2 /i patch123.msi TARGETDIR=C:\patcher PROP=A PROP2=B</pre>
Feature List	The features to install. Use commas to separate features.
Store Config per device	Whether to store configuration information for individual devices.
After install	The action to be performed after installation.
Restart Options	The action to be performed after the device restarts.
Logging	The information to record in the installation log. Use Ctrl-click or Command-click to select multiple items.
Log File Name	The name of the log file.

3. Click **Save** to display the *Script Detail* page.
4. Select options for configuration, deployment, and scheduling. See [Add offline KScripts or online KScripts](#).
5. To edit the raw XML used in the script, click **Edit XML** below the *Schedule* section.
6. Click **Save**.

About power management and power consumption

To get an overview of device power consumption, you can run power management reports for a set time, such as a month.

For more information about the *Power Management* category of reports, see [Creating reports](#).

You can also configure the amount of time that device uptime information is retained. See [Configure appliance General Settings with the Organization component enabled](#). This option is one of the last configuration options.

To collect information about the power use of desktop devices:

- Create a Smart Label in inventory for the chassis type.
- Create reports grouping devices by the chassis type.
- Make a Smart Label in inventory for **Uptime since last reboot** that contains time period in which you are interested.

Add power management scripts for Windows devices

Use this template to create energy management profiles for Windows devices. Power usage settings are a trade-off between CPU usage and power usage.

This template enables you to create a script that configures power management settings. On Windows XP devices, the script created by this template installs the EZ GPO utility if that utility is not already running. EZ GPO is a free power-saving utility that was developed for the Environmental Protection Agency. The utility overcomes a flaw in Windows XP power settings that makes power settings per-user instead of per-device. For more information on EZ GPO, go to <http://www.energystar.gov>.

On Windows 7 and Vista devices, power management is configured using the built-in **powercfg** command. EZ GPO is not required for Windows 7 and Vista devices.

1. Go to the *Windows Power Management* page:
 - a. Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 **Configuration Policies**.
 - c. On the *Configuration Policies* panel, in the *Windows* section, click **Power Management**.
2. On the *Configuration Policy: Windows Power Management* page, select your target operating system.
3. Do one of the following:
 - For Windows XP, select power and other settings:

Option	Description
Power Settings	Each timeout setting can be set to a range of 0-300 minutes where 0 means never. Hibernation should be higher than System Standby or set to 0; it should never be equal to System Standby. Hibernation must be enabled on each device in order for the Hibernate Timeout to work. This template accepts any value in minutes. However the Windows power options dialog boxes display only preset values in minutes such as 1, 2, or 3. When a value is entered that is not one of the preset values, it is correctly applied to the Windows device, but the Windows UI can appear blank for that particular setting.
Other Settings	
Hide Power Options	Hide Power Options: Remove the icon from the Control Panel for all users.

Option	Description
Reboot after applying settings	A reboot is required for the power settings to take effect. The user can be prompted to continue, snooze, or cancel the reboot.
For Windows Vista or Windows 7, select a profile: Balanced, High Performance, Power Saver, or Custom.	
4. Click Save to display the <i>Script: Edit Detail</i> page.	
5. Select options for configuration, deployment, and scheduling, then click Save . See Adding and editing scripts .	

Add Registry scripts

Use this template to create scripts that enforce registry settings on Windows devices.

1. Use `regedit.exe` to locate and export the values from the registry that you are interested in.
2. Open the `.reg` file that contains the registry values you want with `notepad.exe` and copy the text.
3. Go to the *Windows Registry* page:
 - a. Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 **Configuration Policies**.
 - c. On the *Configuration Policies* panel, in the *Windows* section, click **Registry**.
4. Provide the following information:

Option	Description
Name	A name that identifies the script. This name appears on the <i>Scripts</i> page.
Registry File	The registry values to apply when the script runs.

5. Click **Save** to display the *Script Detail* page.
6. Select options for configuration, deployment, and scheduling. See [Add offline KScripts or online KScripts](#).
7. To edit the raw XML used in the script, click **Edit XML** below the *Schedule* section.
8. Click **Save**.

A new script is created, which checks that the values in the registry file match the values found on the target devices. Any missing or incorrect values are replaced.

Add Remote Desktop Control Troubleshooter scripts

Use this template to create a troubleshooting script for the Remote Desktop Control feature on Windows devices.

This script tests the following:

- **Terminal Services:** To access a Windows XP Professional device using Remote Desktop, Terminal Services must be running. This script verifies that Terminal Services is running.
 - **Firewall Configuration:** If the Windows XP SP2 Firewall is running on the device, the script tests for configurations that might block Remote Desktop Control requests.
1. Go to the *Remote Desktop Control Troubleshooter* page:

- a. Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 **Configuration Policies**.
- c. On the *Configuration Policies* panel, in the *Windows* section, click **Remote Desktop Control Troubleshooter**.

2. Provide the following information:

Option	Description
Name	A name that identifies the script. This name appears on the <i>Scripts</i> page.
Firewall Configuration	Specify the settings to apply when the script runs.

3. Click **Save** to display the *Script Detail* page.
4. Select options for configuration, deployment, and scheduling. See [Add offline KScripts or online KScripts](#).
5. To edit the raw XML used in the script, click **Edit XML** below the *Schedule* section.
6. Click **Save**.

Add UltraVNC scripts

Use this template to create a script to distribute UltraVNC to Windows devices. UltraVNC is a free application that enables administrators to log in to devices remotely.

For more information on UltraVNC, go to <http://www.uvnc.com>.

1. Go to the *Windows Ultra VNC* page:
 - a. Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 **Configuration Policies**.
 - c. On the *Configuration Policies* panel, in the *Windows* section, click **UltraVNC**.
2. Provide the following information:

Option	Description
Name	A name that identifies the script. This name appears on the <i>Scripts</i> page.
Install Mirror Driver	Install the optional UltraVNC Mirror Video Driver. Mirror Video Driver is a driver that allows faster and more accurate updates. It also makes a direct link between the video driver framebuffer memory and UltraWinVNC server. Using the framebuffer directly eliminates the use of the CPU for intensive screen blitting, which can boost speed and reduce CPU load.
Install Viewer	Install the optional UltraVNC Viewer. Viewer is a tool used to connect to VNC servers and remotely view desktops. Install Viewer only if you need to initiate remote sessions from the managed device.

Option	Description
Disable tray icon	Prevent the UltraVNC tray icon from appearing on the device.
Disable client options in tray icon menu	Prevent client options from appearing in the tray icon menu on devices. This option is available only if Disable Tray Icon is enabled.
Disable properties panel	Disable the UltraVNC properties panel on devices.
Block end user from closing UltraVNC	Prevent device users to shut down WinVNC.
Password and Read Only Password	Provide password for authentication.
Require Windows Logon	Use Windows Logon authentication and export the ACL from your VNC® installation. Use <code>MSLogonACL.exe /e acl.txt</code> . Copy and paste the contents of the text file into the <i>ACL</i> field.
Encryption Key	Use key-based encryption. To use key-based encryption, create and upload a key: a. In the UltraVNC Viewer, select the MSRC4Plugin from the DSPlugin list. b. Click Config, then enter the full path where the key file will be placed. c. Click Gen Key, then upload the key file.

3. Click **Save** to display the *Script Detail* page.
4. Review the script generated by the template to verify the output.
5. Select options for configuration, deployment, and scheduling. See [Add offline KScripts or online KScripts](#).
6. To edit the raw XML used in the script, click **Edit XML** below the *Schedule* section.
7. Click **Save**.

Add Uninstaller scripts

Use this template to create scripts that manage applications and processes on Windows devices. Scripts can run uninstall commands, stop processes, and delete directories.

1. Go to the *Windows Uninstaller* page:
 - a. Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 **Configuration Policies**.
 - c. On the *Configuration Policies* panel, in the *Windows* section, click **Uninstaller**.
2. Provide the following information:

Option	Description
Name	A name that identifies the script. This name appears on the <i>Scripts</i> page.

Option	Description
Software	The application to use for the script. To search for an application, begin typing in the field.
File	The command information. When you select the application, the template attempts to provide the uninstall command directory, file, and parameters. Verify that the values are correct.
Parameters	
Directory	
Delete Directory	The full name of the directory to be deleted after the uninstall command runs. For example: C:\Program Files\Example_App\.
Kill Process	The full name of the process to be stopped before the uninstall command runs. For example: notepad.exe.

3. Click **Save** to display the *Script Detail* page.
4. Select options for configuration, deployment, and scheduling. See [Add offline KScripts or online KScripts](#).
5. To edit the raw XML used in the script, click **Edit XML** below the *Schedule* section.
6. Click **Save**.

Using Mac OS X configuration policies

You can create scripts that configure policies on Mac OS X devices using configuration policy templates.

Add Active Directory scripts

Use this template to create scripts that add or remove devices to or from domains on Mac OS X devices. You can also use this script to ensure that Mac OS X devices check in to Active Directory databases.

When creating the script, you must specify a username and password for a network account with administrative privileges to add or remove devices to or from the specified domain.

1. Go to the *Mac Active Directory* page:
 - a. Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 **Configuration Policies**.
 - c. On the *Configuration Policies* panel, in the *Mac* section, click **Active Directory**.
2. Provide the following information:

Option	Description
Name	A name that identifies the script. This name appears on the <i>Scripts</i> page.
Action	Specify whether you want to add or remove a device from the current domain.
Network Credentials	Enter your administrator username and password.

Option	Description
	 NOTE: The resulting script assumes that you have root access and shows your password unencrypted (clear text), so make sure that anyone using this script is trusted.
Domain To Configure	Specify the LDAP domain name, user authentication information, and other information.

3. Click **Save** to display the *Script Detail* page.
4. Select options for configuration, deployment, and scheduling. See [Add offline KScripts or online KScripts](#).
5. To edit the raw XML used in the script, click **Edit XML** below the *Schedule* section.
6. Click **Save**.

Add Power Management scripts

Use this template to create energy management profiles for Mac OS X devices. Power usage settings are a trade-off between CPU usage and power usage.

To apply unique settings for each power source, create multiple configuration scripts. Some features might not be supported on some devices.

1. Go to the *Mac Power Management* page:
 - a. Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 **Configuration Policies**.
 - c. On the *Configuration Policies* panel, in the *Mac* section, click **Power Management**.
2. Provide the following information:

Option	Description
Name	A name that identifies the script. This name appears on the <i>Scripts</i> page.
Profile Name	Specify the profile option to use: • Better energy savings: Enforce settings that save energy. This might result in lower performance. When you select this setting, the options in the <i>Profile Options</i> section are not editable. • Normal: Use the default settings. When you select this setting, the options in the <i>Profile Options</i> section are not editable. • Better Performance: Enforce settings that optimize performance. This might result in higher energy use. When you select this setting, the options in the <i>Profile Options</i> section are not editable. • Custom: Use custom profile options. When you select this setting, the options in the <i>Profile Options</i> section become editable.

Option	Description
Power Source	Select a power source: • All: The policy always applies, regardless of the device's power source. • Battery: The policy applies only when the device is using internal battery power. • Charger (Wall Power): The policy applies only when the device is connected to a power outlet. • UPS: The policy applies only when the device is connected to a UPS (uninterruptable power supply).
Operating System	If you select Custom in the <i>Profile</i> drop-down list, specify the operating system to which this policy applies. the <i>Profile Options</i> update to show only those options that are available to the selected version.

3. Click **Save** to display the *Script Detail* page.
4. Select options for configuration, deployment, and scheduling. See [Add offline KScripts or online KScripts](#).
5. To edit the raw XML used in the script, click **Edit XML** below the *Schedule* section.
6. Click **Save**.

Add VNC scripts

Use this template to create scripts that configure the built-in VNC (Virtual Network Computing) settings on Mac OS® devices. The VNC settings determine whether viewers can control device screens.

This script also enables or disables screen sharing, which requires a username and password of an account on the Mac to connect from another Mac running Mac OS X. Use this script with caution: Although the credentials are encrypted, the VNC session might not be.

1. Go to the *Mac VNC* page:
 - a. Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 **Configuration Policies**.
 - c. On the *Configuration Policies* panel, in the *Mac* section, click **VNC**.
2. Provide the following information:

Option	Description
Name	A name that identifies the script. This name appears on the <i>Scripts</i> page.
Enabled	Enable the policy.

Option	Description
Password	Provide a password for the VNC.
- Click Save to display the <i>Script Detail</i> page. - Select options for configuration, deployment, and scheduling. See Add offline KScripts or online KScripts. - To edit the raw XML used in the script, click Edit XML below the <i>Schedule</i> section. - Click Save.	

Edit policies and scripts

You can edit policies and scripts as needed.

- Go to the *Script Detail* page:
 - Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
 - On the left navigation bar, click **Scripting**.
 - Display the *Script Detail* page by doing one of the following:
 - Click the name of a script.
 - Select **Choose Action > New**.
- Change options for configuration, deployment, and scheduling.
See [Add offline KScripts or online KScripts](#).
- At the bottom of the page, click **click here** next to one of the following options:
 - To re-edit the policy using the original editor:* View and edit the initial settings available in the template.
 - To edit the policy using this editor:* View and edit all settings.
- Edit the policy, then click **Save**.

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.

- Go to the *Search Scripting Logs* page.
 - Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
 - On the left navigation bar, click **Scripting**, then click **Search Scripting Logs**.
- 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.

Operator	Function
-	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.  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](#).

Managing Mac profiles

You can use the K1000 appliance to distribute Mac profiles to Agent-managed devices running Mac OS X version 10.8, 10.9, or 10.10. Mac profiles contain payloads, or configuration settings, for user-level and system-level policies.

Distributing Mac profiles using the K1000 is an efficient way to configure settings on the Mac devices you manage, and it provides an alternative to configuring and distributing profiles using OS X Server.

You can configure user- and system-level Mac profile payloads, or configuration settings, in the K1000 Administrator Console. In addition, you can create custom payloads using the Apple Profile Manager, download the `MOBILECONFIG` file that contains those payloads, and upload that file to the K1000 for distribution.

For more information about Mac profiles, go to <http://help.apple.com/profilemanager/mac/4.0>.

How the K1000 Agent distributes profiles

When you add or upload a new Mac profile, the K1000 appliance creates the Online KScript required to install or remove the profile from devices. Like other Online KScripts, scripts that contain Mac profiles run when the K1000 Agent is connected to the target device according to the schedule and deployment options specified in the profile.

Tracking changes to Mac profile 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, editing, and uploading Mac profiles

You can add Mac user and system profiles to the K1000 appliance, and you can edit Mac profiles as needed. In addition, you can upload `MOBILECONFIG` files that contain the configuration information to the K1000 appliance.

Add or edit Mac user profiles

You can add Mac user profiles to the K1000 appliance using the Administrator Console. User profiles contain configuration settings that apply to users, such as email settings. User profiles that have been added to the appliance can be deployed to Agent-managed Mac OS X devices running version 10.8, 10.9, or 10.10.

If you are adding or editing profiles, make sure that you have the account information, server information, and port information required to configure Exchange, LDAP, or Mail payloads.



NOTE: You can edit the payloads of profiles you have configured in the Administrator Console. However, you cannot view or edit the payloads of profiles that have been uploaded to the Administrator Console.

1. Go to the *Mac Profile Detail* page:
 - a. Log in to the K1000 Administrator Console, `http://K1000_hostname/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 **Mac Profiles**.

- c. Do one of the following:
 - Click the name of a profile.
 - Click **Choose Action > New User Profile**.

2. In the *General Options* section, provide the following information:

Option	Description
Profile Name	The name to be displayed on the <i>Mac Profiles</i> list. This name does not need to be unique, but it should be descriptive enough for you to identify the profile in a list.  NOTE: You can change the name of a profile any time. However, if you change the name of a profile after it has been installed on a device, the profile name is not updated on the device. The profile continues to be identified by the name it had when it was installed.
Description	Additional information about the profile, such as its configuration settings or its intended use.
User ability to remove profile	Whether users can remove the profile from their devices. Options include: • Never: Users are not allowed to remove the profile. • Always: Users are allowed to remove the profile any time without entering a password. • With Password: Users are allowed to remove the profile provided that they enter the password associated with the profile.
Automatically remove profile	Whether the profile will be removed automatically after a specified amount of time. This action is useful when you are configuring devices that need to have different profiles after a specific date, such as the end of a school semester. Options include: • Never: The profile is not scheduled to be removed automatically. • On Date: The profile is scheduled to be removed automatically on the specified date. Dates must be specified in mm/dd/yyyy format. • After: The profile is scheduled to be removed after the specified amount of time has passed. Time can be specified in days or hours.

3. **Optional:** In the *Payloads* section, add or edit configuration settings for Exchange, LDAP, or Mail.

- Add or edit Exchange configuration information:

 **NOTE:** To prompt users to enter their own information, such as their user name, email address, or password, leave fields blank. Some fields, such as *Account Name*, however, cannot be left blank.

Option	Description
Account Name	The name used to identify the account.
User	The name of the user.
Email Address	The address to use for the email account.
Password	The password of the email account.
Internal Exchange Host and Port	The hostname of the internal Exchange server and the port used for email communication.
External Exchange Host and Port	The hostname of the external Exchange server and the port used for email communication.
Internal Server Path	The path to the server on the internal network.
External Server Path	The path to the server on the external network.
Use SSL for Internal Exchange Host	Whether to use Secure Sockets Layer for email transmitted within the domain.
Use SSL for External Exchange Host	Whether to use Secure Sockets Layer for email transmitted outside the domain.

- Add or edit LDAP configuration information:



NOTE: To prompt users to enter their own information, such as their username or password, leave fields blank. Some fields, such as *Account Hostname*, however, cannot be left blank.

Option	Description
Account Description	The name of the LDAP account, such as <code>Example Corporation LDAP Account</code> .
Account Username	The username of the account to be used to log in to the LDAP server.
Account Password	The password of the account to be used to log in to the LDAP server.
Account Hostname	The hostname or IP address of the LDAP server.
Use SSL	Whether to use Secure Sockets Layer for connections to the LDAP server.

Option	Description
Search Settings	The settings used to search for information on the LDAP server.
Description	Information that differentiates the search information in a list.
Scope	The depth of the search. Whether the search will be conducted on: Base: Includes objects in the base or zero level only. One Level: Includes objects immediately subordinate to the base, but not including the base. Subtree: Includes objects in the base and subtree.
Search Base	Search Base: The location in the directory from which the search begins. The Search Base 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 Base DN 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.
Add or edit Mail configuration information:	 NOTE: To prompt users to enter their own information, such as their display name or email address, leave fields blank. Some fields, such as <i>Incoming Mail Server</i>, however, cannot be left blank.

Option	Description
Account Description	The name of the account, such as <code>Example Corporation Mail Account</code> .
Account Type	The protocol (POP or IMAP) used to access the account.
User Display Name	How the user's name appears in the <i>From</i> field in email messages.
Email Address	The user's email address.
Incoming Mail Server and Port	The hostname or IP address and port number used for incoming mail.

Option	Description
Outgoing Mail Server and Port	The hostname or IP address and port number used for outgoing mail. Use the following standard port assignments: - SMTP: 25 (465 with SSL) - POP3: 110 (995 with SSL) - IMAP: 143 (993 with SSL)
Incoming Mail User Name	The username to use for the incoming mail server.
Outgoing Mail User Name	The username to use for the outgoing mail server.
Incoming Mail Authentication Type	The method of authenticating the user for incoming mail. Authentication types include Password, MD5 Challenge-Response, NTLM, HTTP MD5 Digest.
Outgoing Mail Authentication Type	The method of authenticating the user for outgoing mail. Authentication types include Password, MD5 Challenge-Response, NTLM, HTTP MD5 Digest.
Incoming mail use SSL	Whether to use Secure Socket Layer for mail delivered to the user account.
Outgoing mail use SSL	Whether to use Secure Socket Layer for mail sent from the user account.

4. (Optional) In the *Deploy* section, select the target devices for the profile:



TIP: You can create a profile without selecting target devices. However, profiles cannot be deployed until target devices are selected.

Option	Description
All Devices	Distribute the profile to all K1000 Agent-managed devices running a supported version of Mac OS X (version 10.8, 10.9, or 10.10). If the Organization component is enabled on your appliance, this distribution includes all supported Mac devices in the selected organization.
Labels	Distribute the profile only to the devices in the labels that you select. Limiting the distribution to labels, especially Smart Labels, helps to ensure that profiles are applied appropriately. To use this option, you must already have created labels or Smart Labels. See Adding Smart Labels for devices .
Devices	Distribute the profile to the supported Mac OS X devices that you select (version 10.8, 10.9, or 10.10). To search for devices, begin typing in the field.

Option	Description
Operating Systems	Select the operating systems of the devices to which you want to distribute the profile. Only supported operating systems (Mac OS X version 10.8, 10.9, or 10.10) are displayed. To distribute the profile to all supported Mac operating systems, leave all operating systems unselected.
Remove All	Remove all selected devices from the <i>Devices</i> list in this section.

5. In the *Schedule* section, select the options for distributing the profile to target devices:

Option	Description
None	Do not distribute the profile on a schedule. Profiles that have their schedules set to None have a status of Disabled on the <i>Mac Profiles</i> list. However, profiles whose schedule is set to None can still be deployed if you select Run Now at the bottom of the page.
Every n minutes/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.
Custom	Run according to a custom schedule. Use standard 5-field cron format (extended cron format is not supported): <pre>* * * * * +-----day of week (0-6) (Sun=0) +-----month (1-12) +-----day of month (1-31) +-----hour (0-23) +-----minute (0-59)</pre> 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

Option	Description
	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:

6. In the *Deployment Options* section, select the options for prompting users about the profile installation:

Option	Description
Runtime prompt for logged-in users	When the Agent begins the profile installation, a prompt is displayed to users who are logged in to the target device.
Login prompt for all users	Whenever users log in to the target device, they are prompted to install the profile if they have not done so already.
Both runtime and login prompts	When the Agent begins the profile installation, users who are logged in to the target device are prompted to install the profile if they have not done so already. Users who log in after the script runs are also prompted to install the profile.

7. At the bottom of the page, select one of the following actions:

Option	Description
Save	Save the profile and return to the <i>Mac Profiles</i> list.
Run Now	On target devices that have an active Agent connection to the appliance, install the profile now according to the selected deployment options. See Using the Run and Run Now commands .
Duplicate	Create a copy of the profile with <code>Copy of</code> prepended to the profile name. This option is not available for new profiles that have not yet been saved. See Add Mac profiles using existing profiles as templates .
Remove	Create a profile that can be used to remove the profile from target devices. This option is not available for new profiles that have not yet been saved. See Remove Mac profiles from managed devices .
Delete	Remove the profile from the K1000 appliance. This does not remove the profile from devices on which it is installed, and this option is not available for new

Option	Description
	profiles that have not yet been saved. See Delete Mac profiles from the K1000 appliance .
Cancel	Discard changes and return to the <i>Mac Profiles</i> list.

Add or edit Mac system profiles

You can add Mac system profiles to the K1000 appliance using the Administrator Console. System profiles contain configuration settings that apply to devices, such as passcode requirements. System profiles that have been added to the appliance can be deployed to Agent-managed Mac OS X devices running version 10.8, 10.9, or 10.10.

You have established policies for accessing apps and setting passcodes.



NOTE: You can edit the payloads of system profiles you have configured in the Administrator Console. However, you cannot view or edit the payloads of profiles that have been uploaded to the Administrator Console.

- Go to the *Mac Profile Detail* page:
 - Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
 - On the left navigation bar, click **Scripting**, then click **Mac Profiles**.
 - Do one of the following:
 - Click the name of a profile.
 - Click **Choose Action > New System Profile**.
- In the *General Options* section, provide the following information:

Option	Description
Profile Name	The name to be displayed on the <i>Mac Profiles</i> list. This name does not need to be unique, but it should be descriptive enough for you to identify the profile in a list. NOTE: You can change the name of a profile any time. However, if you change the name of a profile after it has been installed on a device, the profile name is not updated on the device. The profile continues to be identified by the name it had when it was installed
Description	Additional information about the profile, such as its configuration settings or its intended use.

Option	Description
User ability to remove profile	Whether users can remove the profile from their devices. Options include: • Never: Users are not allowed to remove the profile. • Always: Users are allowed to remove the profile any time without entering a password. • With Password: Users are allowed to remove the profile provided that they enter the password associated with the profile.
Automatically remove profile	Whether the profile will be removed automatically after a specified amount of time. This is useful when you are configuring devices that need to have different profiles after a specific date, such as the end of a school semester. Options include: • Never: The profile is not scheduled to be removed automatically. • On Date: The profile is scheduled to be removed automatically on the specified date. Dates must be specified in mm/dd/yyyy format. • After: The profile is scheduled to be removed after the specified amount of time has passed. Time can be specified in days or hours.

3. In the *Payloads* section, add or edit *Gatekeeper* configuration information.

Option	Description
Allow Apps Downloaded From	Whether users are allowed to download apps from: • Mac App Store: Users can download apps only from the Mac App Store. • Mac App Store and Identified Developers: Users can download apps from the Mac App Store and from developers who have digitally signed their apps with a unique Developer ID from Apple. • Anywhere: Users can download apps from anywhere without restriction.
Don't allow user to override Gatekeeper setting	Whether users are allowed to modify the app download settings.

4. Add or edit *Passcode* configuration information.



NOTE: In this section, the term **passcode** is synonymous with the term **password**.

Option	Description
Allow simple value	Allow users to select passcodes with character sequences that are repeating, ascending, and descending.
Require alphanumeric value	Require users to select passcodes that contain at least one letter and one number.
Minimum passcode length	The smallest number of characters allowed in passcodes.
Minimum number of complex characters	The smallest number non-alphanumeric characters, such as *or ! allowed in passcodes.
Maximum number of failed attempts	The number of times users can enter incorrect passcodes to unlock devices before being locked out of their accounts.
Maximum grace period for device lock	When system settings specify that devices should be locked after a period of inactivity, this setting provides a window of time during which users can unlock their devices without entering their passcodes. After the grace period expires, users must enter their passcodes to unlock devices.
Maximum passcode age in days	The number of days after which passcodes must be changed.
Passcode history	The number of passcodes that must be unique before a passcode can be reused.
Delay after failed login attempts in minutes	The number of minutes that must pass before users can attempt to log in after reaching the maximum number of failed login attempts.

5. In the *Deploy* section, select the target devices for the profile:

Option	Description
All Devices	Distribute the profile to all K1000 Agent-managed devices running a supported version of Mac OS X (version 10.8, 10.9, or 10.10). If the Organization component is enabled on your appliance, this includes all supported Mac devices in the selected organization.
Labels	Distribute the profile only to the devices in the labels that you select. Limiting the distribution to labels, especially Smart Labels, helps to ensure that profiles are applied appropriately. To use this option, you must already have created labels or Smart Labels. See Adding Smart Labels for devices.

Option	Description
Devices	Distribute the profile to the supported Mac OS X devices that you select (version 10.8, 10.9, or 10.10). To search for devices, begin typing in the field.
Operating Systems	Select the operating systems of the devices to which you want to distribute the profile. To distribute the profile to all supported Mac operating systems, leave all operating systems unselected.
Remove All	Remove all devices from the <i>Devices</i> list in this section.

6. In the *Schedule* section, select the options for distributing the profile to target devices:

Option	Description
None	Do not distribute the profile on a schedule. Profiles that have their schedules set to None have a status of Disabled on the <i>Mac Profiles</i> list. However, profiles whose schedule is set to None can still be deployed if you select Run Now at the bottom of the page.
Every n minutes/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.
Custom	Run according to a custom schedule. Use standard 5-field cron format (extended cron format is not supported): <pre>* * * * * +-----day of week (0-6) (Sun=0) +-----month (1-12) +-----day of month (1-31) +-----hour (0-23) +-----minute (0-59)</pre> 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

Option	Description
	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:

7. At the bottom of the page, select one of the following actions:

Option	Description
Save	Save the profile and return to the <i>Mac Profiles</i> list.
Run Now	On target devices that have an active Agent connection to the appliance, install the profile now according to the selected deployment options. See Using the Run and Run Now commands .
Duplicate	Create a copy of the profile with <code>Copy of</code> prepended to the profile name. This option is not available for new profiles that have not yet been saved. See Add Mac profiles using existing profiles as templates .
Remove	Create a profile that can be used to remove the profile from target devices. This option is not available for new profiles that have not yet been saved. See Remove Mac profiles from managed devices .
Delete	Remove the profile from the K1000 appliance. This does not remove the profile from devices on which it is installed, and this option is not available for new profiles that have not yet been saved. See Delete Mac profiles from the K1000 appliance .
Cancel	Discard changes and return to the <i>Mac Profiles</i> list.

Add Mac profiles using existing profiles as templates

You can add Mac profiles by duplicating existing profiles. This is useful if you want to install an existing profile on different sets of devices, or schedule profile installations to occur at different times. You can duplicate profiles, and change the target devices or schedules as needed.

You have added a user or system profile to the K1000 appliance.

Profiles that have been imported cannot be duplicated.

1. Go to the *Mac Profiles* page:
 - a. Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 **Mac Profiles**.
2. Click the name of a profile to display the *Mac Profile Detail* page.
3. At the bottom of the page, click **Duplicate**.

The profile is duplicated, and it appears on the *Mac Profile* list with *Copy of* prepended to the profile name. Duplicated profiles have the same properties and identification numbers as the original profiles, but their schedules are automatically set to **None** to prevent duplicated actions from being performed on the same sets of devices

Upload Mac profiles to the K1000 appliance

The K1000 appliance enables you to upload `MOBILECONFIG` files that contain the configuration settings required to create Mac profiles.

You have obtained a file that contains the configuration settings, or payloads, required for the profile, and that file uses the filename extension `MOBILECONFIG`. For example, `mail.mobileconfig`. For information about creating Mac profiles and downloading them from the Mac OS X Server, go to <http://help.apple.com/profilemanager/mac/4.0>.



NOTE: You cannot view or edit the payloads of profiles that have been uploaded to the Administrator Console. However, you can modify the payloads in the `MOBILECONFIG` file outside the Administrator Console, then upload the edited file as a new profile.

1. Go to the *Mac Profiles* list page:
 - a. Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 **Mac Profiles**.
2. Click **Choose Action > Upload a Profile**.
3. Click **Browse** or **Choose File** to locate the `MOBILECONFIG` file.
4. Click **Upload**

The profile appears on the *Mac Profiles* list with *Imported* in the *Source* column.

Select deployment and schedule options for the profile. See:

- [Add or edit Mac user profiles](#)
- [Add or edit Mac system profiles](#)

Installing and managing Mac profiles

You can install Mac profiles, view the devices that have Mac profiles installed, and export the list of profiles that have been added to the K1000 appliance.

Distribute Mac profiles on a schedule

You can configure the K1000 appliance to distribute Mac profiles to Agent-managed Mac OS X devices periodically according to a schedule. This configuration is useful if you have devices that might be offline and unavailable for installation when you select the *Run* option, and for periodically installing profiles on new devices added to inventory.

You have added or uploaded a Mac profile and you have Agent-managed Mac OS X version 10.8, 10.9, or 10.10 devices in your K1000 inventory.

1. Go to the *Mac Profile Detail* page:
 - a. Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 **Mac Profiles**.
 - c. Click the name of a profile.
2. In the *Schedule* section, select the options for distributing the profile to target devices:

Option	Description
None	Do not distribute the profile on a schedule. Profiles that have their schedules set to None have a status of Disabled on the <i>Mac Profiles</i> list. However, profiles whose schedule is set to None can still be deployed if you select Run Now at the bottom of the page.
Every n minutes/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.
Custom	Run according to a custom schedule. Use standard 5-field cron format (extended cron format is not supported): <pre>* * * * * +-----day of week (0-6) (Sun=0) +-----month (1-12) +-----day of month (1-31) +-----hour (0-23) +-----minute (0-59)</pre> 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,

Option	Description
	* / 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:

3. Click **Save**.

The *Mac Profiles* page appears. The *Targeted* column shows the number of devices that are scheduled to have the profile installed. The *Succeeded* column shows the number of devices on which the profile has been installed. Agents on target devices receive instructions to install the profile at the next connection according to the schedule and deployment options specified.

Install Mac profiles on devices using the Run option

After you add or upload Mac profiles to the K1000 appliance, you can use the *Run* option to install those profiles on Agent-managed Mac OS X devices running version 10.8, 10.9, or 10.10.

You have added Mac profiles, and you have Agent-managed Mac OS X version 10.8, 10.9, or 10.10 devices in your K1000 inventory.



TIP: When you use the *Run* option to install Mac profiles on devices, profiles are installed only if devices have an Agent connection to the appliance when the script runs. To ensure that profiles are installed on devices that are offline, consider setting up schedules to deploy profiles. See [Distribute Mac profiles on a schedule](#).

1. Go to the *Mac Profile Detail* page:
 - a. Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 **Mac Profiles**.
 - c. Click the name of a profile.
2. To install the profile on a different set of devices, click **Duplicate** at the bottom of the page to create a copy of the profile, then click the name of the duplicated profile to return to the *Mac Profile Detail* page.
3. On the *Mac Profile Detail* page, select the target devices and deployment options. See:
 - [Add or edit Mac user profiles](#)
 - [Add or edit Mac system profiles](#)
4. At the bottom of the page, click **Run Now**.

The *Mac Profiles* page appears. The *Targeted* column shows the number of devices that are scheduled to have the profile installed. The *Succeeded* column shows the number of devices on which the profile has been installed. On target devices that have an active Agent connection to the appliance, the profile is installed according to the selected deployment options.
5. To run multiple profiles at once, select the check boxes next to profiles on the *Mac Profiles* page, then click **Choose Action > Run**.
6. To view additional details about the profile installation, click **Run Now Status** on the left navigation bar.

Identify devices that have Mac profiles installed

Device detail pages show the Mac profiles that have been installed on devices, and Mac profile detail pages show devices that have Mac profiles installed.

1. Go to the *Mac Profile Detail* page:

- a. Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 **Mac Profiles**.
 - c. Click the name of a profile.
2. Scroll down to the *Results* section at the bottom of the page.

The table lists the devices on which the profile is installed. The *Installed* column indicates the date the profile was installed on the device. The *Last Updated* column indicates the most recent date the K1000 Agent detected that the profile was installed on the device.
3. Go to the *Device Detail* page:
 - a. On the left navigation bar, click **Inventory**.
 - b. Click the name of a device.
4. Scroll down to the *Mac Profiles* section.

The table lists all the profiles that are installed on the device. The *Installed* column indicates the date the profile was installed on the device. The *Last Updated* column indicates the most recent date the K1000 Agent detected that the profile was installed on the device.

View Mac profiles

You can use the *View By* list to sort Mac profiles by source, action, and scope.

You have added or uploaded Mac profiles to the K1000 appliance.

1. Go to the *Mac Profiles* list:
 - a. Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 **Mac Profiles**.
2. In the *View By* drop-down list, which appears above the table on the right, select one of the following:

Option	Description
All Items	Display the complete list of profiles.
Source	Display only those profiles that match the selected source: • Imported: Profiles that have been uploaded to the K1000 appliance. • Configured: Profiles whose payloads were configured using the Administrator Console.
Action	Display only those profiles that match the selected action: • Add: Profiles that are configured to install configuration settings on the target devices. • Remove: Profiles that are configured to remove configuration settings from target devices.

Option	Description
Scope	Display only those profiles that match the selected scope: • System: Profiles that configure system settings, such as passcode settings. • User: Profiles that configure user settings, such as email account settings.
Status	Display only those profiles that match the selected status: • Active: Profiles that are configured to run according to a schedule. • Disabled: Profiles whose schedule is set to None.

Export the Mac profiles list

You can export the list of profiles that appears on the *Mac Profiles* list to CSV (comma-separated values), Excel, or TSV (tab-separated values) formats.

You have created or uploaded Mac profiles.

1. Go to the *Mac Profiles* list:
 - a. Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 **Mac Profiles**.
2. **Optional:** To export selected profiles, select the check boxes next to the profiles you want to export.
3. Do one of the following:
 - To export all profiles in the list, click **Choose Action > Export > Export All to format name**.
 - To export only the select profiles, click **Choose Action > Export Selected to format name**.

Removing and deleting Mac profiles

You can use the K1000 to remove Mac profiles from managed devices, and you can delete Mac profiles from the K1000 appliance.

Remove Mac profiles from managed devices

Mac profiles can be configured to remove user and system profiles from Agent-managed Mac OS X devices. This configuration is useful when you have installed a profile on a large number of devices, and you need to remove that profile from all of those devices or from a subset of those devices.

You have used the K1000 appliance to install a profile on managed devices, and the original Mac profile has not been deleted from the appliance.



IMPORTANT: If you delete a profile from the K1000 appliance, you can no longer use the appliance to remove that profile from managed devices.

1. Go to the *Mac Profile Detail* page:

- a. Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 **Mac Profiles**.
 - c. Click the name of a profile.
2. At the bottom of the page, click **Remove**.
A dialog appears explaining the remove process.
3. Click **Remove from Device**.

The *Mac Profile Detail* page for a new profile, with the *Action* set to *Remove*, appears. The new profile has the same *Profile Name* and *Profile Identifier* as the original profile. The original profile, with the *Action* set to *Add*, remains on the list with its *Schedule* set to *None*. This prevents the same profile from being installed on or removed from the same set of devices, and it enables you to reactivate the original profile later if necessary.

4. On the *Mac Profile Detail* page in the *Deploy* section, select the devices from which you want to remove the profile:

Option	Description
All Devices	Remove the profile from all K1000 Agent-managed devices running a supported version of Mac OS X (version 10.8, 10.9, or 10.10). If the Organization component is enabled on your appliance, this action includes all supported Mac devices in the selected organization.
Labels	Remove the profile from the devices in the labels that you select. Limiting the removal to labels, especially Smart Labels, helps to ensure that profiles are removed appropriately. To use this option, you must already have created labels or Smart Labels. See Adding Smart Labels for devices .
Devices	Remove the profile from the supported Mac OS X devices that you select (version 10.8, 10.9, or 10.10). To search for devices, begin typing in the field.
Operating Systems	Select the operating systems of the devices from which you want to remove the profile. Only supported operating systems (Mac OS X version 10.8, 10.9, or 10.10) are displayed. To remove the profile from all supported Mac operating systems, leave all operating systems unselected.
Remove All	Remove all selected devices from the <i>Devices</i> list in this section.

5. In the *Schedule* section, select the options for removing the profile from target devices:

Option	Description
None	Do not remove the profile on a schedule. Profiles that have their schedules set to None have a status of Disabled on the <i>Mac Profiles</i> list. However, profiles whose schedule is set to <i>None</i> can still be

Option	Description
	removed if you select Run Now at the bottom of the page.
Every n minutes/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.
Custom	Run according to a custom schedule. Use standard 5-field cron format (extended cron format is not supported): <pre>* * * * * +-----day of week (0-6) (Sun=0) +-----month (1-12) +-----day of month (1-31) +-----hour (0-23) +-----minute (0-59)</pre> 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:

6. At the bottom of the page, select one of the following actions:

Option	Description
Save	Save the profile and return to the <i>Mac Profiles</i> list.
Run Now	On target devices that have an active Agent connection to the appliance, remove the profile now

Option	Description
	according to the selected deployment options. See Using the Run and Run Now commands .
Duplicate	Create a copy of the profile with <code>Copy of</code> prepended to the profile name.
Delete	Remove the profile from the K1000 appliance. This action does not remove the profile from devices on which it is installed. See Delete Mac profiles from the K1000 appliance .
Cancel	Discard changes and return to the <i>Mac Profiles</i> list.

The *Mac Profiles* page appears. The *Targeted* column shows the number of devices that are scheduled to have the profile removed. The *Succeeded* column shows the number of devices from which the profile has been removed. On target devices that have an active Agent connection to the appliance, the profile is removed according to the selected options.

Example: Remove a profile that has been deployed to specified devices

If you inadvertently deploy profiles to target devices, you can remove them by creating a *Remove* profile.

- You have created a Mac system profile with these scheduling and deployment options:
 - Scheduled to be installed daily at 8:00.
 - Installed, or scheduled to be installed, on 100 target devices.
- After creating the profile, you realize that you do not want to have the profile installed on 10 of the 100 target devices. You need to remove the profile from the 10 devices and continue to keep the profile available to the other 90 devices.



NOTE: This example uses a Mac system profile, but you can remove both Mac system and Mac user profiles as needed.

- Go to the *Mac Profile Detail* page:
 - Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
 - On the left navigation bar, click **Scripting**, then click **Mac Profiles**.
 - Click the name of the profile. In this example, we refer to this profile as **Profile A**.
- On the *Mac Profile Detail* page for **Profile A**, click **Remove**.
A dialog appears explaining the **remove** process.
- Click **Remove from Device**.

The *Mac Profile Detail* page for a new profile, with the *Action* set to *Remove*, appears. The new profile has the same *Profile Name* and *Profile Identifier* as the original profile. In this example, this is **Profile A Remove**. The original profile, with the *Action* set to *Add*, remains on the list with its *Schedule* set to *None*.

This prevents the same profile from being installed on or removed from the same set of devices, and it enables you to reactivate **Profile A** later if necessary.

4. On the *Mac Profile Detail* page for **Profile A Remove**, in the *Deploy* section, select the devices from which you want to remove the profile.
5. Do one of the following:
 - If you have set the profile to run on a schedule, click **Save** at the bottom of the page.
 - To run the profile on devices that currently have a connection to the K1000 appliance, click **Run Now**.

The *Mac Profiles* page shows the number of target devices in the *Targeted* column and the number of devices from which the profile has been removed in the *Succeeded* column for **Profile A Remove**.

6. When the *Succeeded* column shows that the profile has been removed from all target devices, **Profile A Remove** is no longer needed, and you can delete it from the appliance. See [Delete Mac profiles from the K1000 appliance](#).
7. In **Profile A**, verify that the correct devices are targeted and enable the profile:
 - a. Go to the *Mac Profile Detail* page for **Profile A**.
 - b. Change the list of target devices to include only the correct 90 devices.
 - c. Enable the profile. See:
 - [Add or edit Mac user profiles](#)
 - [Add or edit Mac system profiles](#)

Delete Mac profiles from the K1000 appliance

You can delete Mac profiles from the K1000 appliance as needed.

Deleting a profile does not remove it from any devices on which it has been installed. To remove profiles from devices, use the **Remove** option. See [Remove Mac profiles from managed devices](#).



NOTE: If you delete a profile from the K1000 appliance, you can no longer use the appliance to remove that profile from managed devices.

1. Go to the *Mac Profile Detail* page:
 - a. Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 **Mac Profiles**.
 - c. Click the name of a profile.

2. At the bottom of the page, click **Delete**.

A dialog appears.

3. Verify that you want to delete the profile from the appliance, then click **Delete Profile**.

The profile is removed from the appliance and it no longer appears on the *Mac Profiles* list. However, the Profile Identifier continues to be displayed on the *Device Detail* page of devices on which the profile is installed.

Patching devices and maintaining security

The K1000 enables you to patch managed devices to improve software functionality and protect devices and networks from vulnerabilities.

About patch management

Patch management is the process of obtaining, testing, and installing patches for software on devices. The K1000 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 K1000 appliance.



NOTE: The Patch Management component is supported on Windows and Mac devices only. Patch Management is not available for Linux devices.

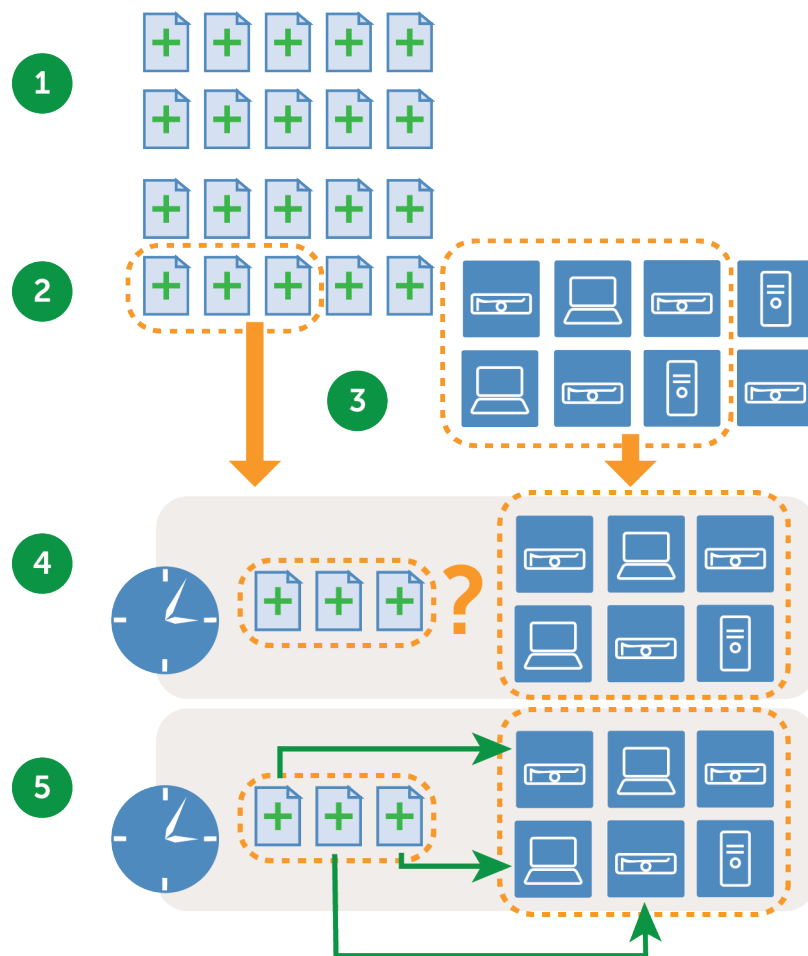
Patching workflow

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 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 9. Patching workflow



Legend number	Action
1	Signature files for patches you subscribe to are downloaded to the appliance from Lumension. Patch packages are downloaded from Lumension and from software vendors.
2	Smart Labels group the downloaded patches.
3	Smart Labels select devices to patch.
4	Devices that need the patch 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 Lumension according to the subscription and download options you select. For more information on downloading patch signature files, see [Select patch download settings](#).

About patch packages

Patch packages are the files required to install patches.

Patch packages are downloaded from Lumension 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 download settings](#).

About patch testing and security

Quest partners with Lumension Security, Inc. to provide safe, timely, and high-quality patch signatures for all major operating systems and many popular applications.

Before patch signatures are made available to the appliance, Lumension 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.

In addition, Quest performs sanity checks on patch feeds after Lumension security checks are complete. For more information, search for Lumension at <https://www.quest.com/kace/>.

About the patch testing environment

Built-in Lumension security uses VMware® ESX®, VMware® vCenter™ Lab Manager™, and custom hardware bench testing.

Testing methods include:

- Verification that patch-naming conventions comply with Lumension policy.
- Verification that patch content supports the replication process. Each patch created by the content team is validated with the Symantec Ghost™ Solution Suite distribution and Update Server products.

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.
- CRC 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 partners with HEAT Software to provide 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, HEAT Software executes test cases covering the following test components.

Testing environment

HEAT Software invests heavily in testing infrastructure. The content development and quality assurance teams have access to a virtual enterprise environment representing more than 1,500 nodes of various configurations. HEAT Software 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

HEAT Software tests with various applications as necessary to ensure the requirements of the patch are satisfied.

Testing strategy

HEAT Software uses the following types of testing:

- **General testing** verifies the following:
 - Patch-naming convention complies with the HEAT Software policy.
 - The content supports the replication process: each patch created by the content team is validated with the Global Subscription Service (GSS) distribution and Patch Server products.
- **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

The HEAT Software GSS is designed and implemented to maximize global availability through a secure content distribution network. All communications with the HEAT Software GSS 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.

The patches (.pls) and its associated packages (.plp) are encrypted with a key. This key is part of our product (kace.plk). Hence these files cannot be opened and modified without the key and also a Lumension-specific library.

SCR is a Java-based tool used to download patches. It employs checksum verification during the download process.

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 K1000 to patch Windows devices**

There are two options for patching Windows devices:

- **Use Windows 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 the K1000 Patch Management component only to detect Windows operating system patches, not to deploy them. Patches will be deployed by Windows Update.
- **Use the K1000:** You can download and deploy patches for Windows operating systems using the K1000 Patch Management component. If you use the K1000, disable Windows Update on managed devices, because patches will be deployed by the K1000.



TIP: The K1000 appliance enables you to create a policy that specifies whether or not managed devices use Windows Update. See [Using Windows configuration policies](#).

- **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 a K1000 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 K1000 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 K1000 Management Appliance problems that administrators encounter. To view patching articles, go to the Knowledge Base and search for *Security*.

- **Use ITNinja.com to connect with other IT professionals**

Sponsored by Quest KACE, ITNinja.com (formerly AppDeploy.com) is a product-agnostic IT-focused community website. It is the Internet's leading destination for IT professionals to share information and ask questions about system-management related topics. See <http://itninja.com>.

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 download settings](#)
- [Using Smart Labels for patching](#)

Applications that the K1000 is able to patch

For a list of applications that the K1000 is able to patch, go to <https://support.quest.com/kb/112030>.

NTP service requirement

When downloading patches using HTTPS, the NTP (Network Time Protocol) service must be running on the K1000 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 K1000 appliance

To complete patch downloads, access product information, and interact with Quest Support, the firewall, DNS server, and proxy server settings must allow the K1000 appliance to access specific domains on both port 80 and port 443.

Table 28. Domains that must be accessible to the K1000 appliance

Domain	Used for
https://api.dell.com	Dell updates
http://ftp.dell.com	Dell updates
http://cache.lumension.com	Lumension patches
http://cache.patchlinksecure.net	Lumension patches
http://cdn.patchlink.com	Quest patches
http://kace.cdn.lumension.com	Quest patches
http://download.windowsupdate.com	Microsoft updates
http://download.microsoft.com	Microsoft updates
http://www.microsoft.com/en-us/default.aspx	Microsoft updates
http://www.itninja.com	ITNinja community features
http://appdeploy.com	Redirects to ITNinja.com

Domain	Used for
https://quest.com/kace	Localized content, third-party software licenses, and product information
https://support.quest.com/download-product-select	Quest updates
http://servicecdn.kace.com	SCAP (Secure Content Automation Protocol)
https://service.kace.com	K1000 appliance and Agent updates from Quest
https://support.quest.com	Quest Support
http://download.skype.com	Skype updates
http://ardownload.adobe.com	Adobe application updates
http://armdl.adobe.com	Adobe application updates
http://download.adobe.com	Adobe application updates
http://swupdl.adobe.com	Adobe application updates
http://www.adobe.com	Adobe application updates
ftp.mozilla.org	Mozilla Firefox updates
http://support1.uvnc.com	Ultra VNC updates
http://downloads.sourceforge.net	7-Zip updates
http://download.videolan.org	VideoLAN VLC updates

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 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 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 K1000 has the Organization component enabled, and you want view information for the appliance, log in to the K1000 System Administration Console: `http://K1000_hostname/system`, or select **System** from the drop-down list in the top-right corner of the page.
 - If your K1000 does not have the Organization component enabled, or if you want to view organization-level information, log in to the K1000 Administrator Console : `http://K1000_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 K1000 Administrator Console, `http://K1000_hostname/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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**.
 - c. On the *Patch Management* panel, click **Subscriptions**.
2. The *Patch Status* section 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 *Subscription* settings. 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 *Operating System Patches* settings. These settings are used to determine the patch status once the patch files are downloaded. The patch status can be active, inactive, or disabled.

Option	Description
Types	Subscribe to security or non-security type operating system patches. Click the edit button to manage the

Option	Description
	selected types: . Select All Types to select both security and non-security patches. To ignore the patch type, select Disabled. Or, select the check boxes next to one or more patch types. Selected items are displayed after you save the settings.

Impacts	Subscribe to patches based on an operating system's patch impact. This can be Critical or Recommended. Click the edit button to manage the selected impacts: . Select All Impacts to select both Critical and Recommended patches. Or, select the check boxes next to one or more patch impacts. Selected items are displayed after you save the settings.

- 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
Types	Subscribe to security, non-security or software installer type application patches. Click the edit button to manage the selected types: . Select All Types to select security, non-security and windows installer patches. To ignore the patch type, select Disabled. Or, select the check boxes next to one or more patch types. Selected items are displayed after you save the settings.

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.

Impacts	Subscribe to patches based on an applications patch impact. The impact can be Critical or Recommended. Click the edit button to manage the selected impacts: . Select All Impacts to select both Critical and Recommended patches. Or, select the check boxes next to one or more patch impacts. Selected items are displayed after you save the settings.

- Specify the subscription's *Advanced Options*.

Option	Description
Labels	Download only those patches that match the selected labels. Click Manage Associated Labels to select the labels.

Option	Description
	This refinement is important when disk space is limited. If the total disk space required for selected patches exceeds the space available on the K1000, patches cannot be downloaded.  NOTE: Appliance disk space information appears in the <i>Patch Status</i> 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 <i>Inactive</i> state after every download. Inactive Superseded Patches are identified with Inactive on the <i>Patch Catalog</i> 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.

7. 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 download settings

The patches 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 Download* settings.
 - 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 K1000 System Administration Console, http://K1000_hostname/system, or select **System** in the drop-down list in the top-right corner of the page, then click **Settings**.
2. Click *Patch Download Settings*.
3. In the *Configure* section, select the following options.

Option	Description
Disabled	Prevent the downloading of patch packages. This prevention includes the installers that are required to install the patches.
All subscribed files	Maintain a full cache of subscribed packages on your K1000 appliance. This option downloads all

Option	Description
	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	Allow 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 Patched on any managed device, the patch package is downloaded. If no managed devices are detected as Not Patched, no packages for this patch are downloaded.
Delete unused files after __ days	Delete patches that have not been deployed in the specified number of days. Patches that are marked as <i>Inactive</i> or <i>Disabled</i> are automatically deleted during the patch download process.
Offline Update	The action to take if the appliance is offline when the update process is scheduled to start. Clear the <i>Offline Update</i> option if the appliance is expected to be connected to the internet and can download patches directly.
Offline Target	The Offline Target to use if the appliance is not connected to the internet, and you want to upload the patch files from a local directory. If you have a K1000 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: <code>\k1000_host\patches</code>. 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 K1000 appliance's Patches file share.

- Select schedule options for patch signatures in the *Schedule* section. Patch signatures include the security bulletins and other files that define patches downloaded from Lumension.

Option	Description
None	Prevent the downloading of patch signatures.
Every __ hours	Download signatures at a specified interval. Use caution when specifying frequent intervals (4, 8 or 12 hours), because this can increase bandwidth requirements.

Option	Description
Every day at the specified time	Select day to download patch 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. i NOTE: When setting up patch 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 patch 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 detection signatures on a monthly basis.

- Set the schedule options for patch files:

Option	Description
After signature download	Download packages after the signatures have been downloaded. This option is not available if package download is disabled in the <i>Patch Download Options</i> section.
Every __ minutes	Specify the frequency with which signatures and packages are downloaded. This option is available only if <i>Patches detected as missing</i> in the <i>Patch Download Options</i> section is selected.
Download Blackout: Start __ End __	Specify a time period during which patch detection signatures 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 patch downloads at the specified time. It does not start patch downloads again until the next specified patch download time. When the download resumes, it starts up where it left off. Downloads that are incomplete might not appear on the <i>Patch Catalog</i> page.

- Click **Save**.
- To immediately download the patches to which you have subscribed, regardless of the schedule, click **Run Now**.
- To immediately remove all patches from the appliance, click **Delete**. This can be useful if you no longer need any patches and you want to quickly reclaim the disk space that they used.

To schedule patch detection and deployment for managed devices, see [Creating and managing patch 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 download settings](#)
1. Go to the *Patch Catalog* list:
 - a. Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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**.
 - c. On the *Patch Management* panel, click **Catalog**.
 2. Search for application patches.
 - a. Click the **Advanced Search** tab above the list on the right to display the *Advanced Search* 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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**.
 - c. On the *Patch Management* panel, click **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 **Advanced Search** 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](#).

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.

You can create and edit the following types of patch schedules:

- [Configure Detect-only patch schedules](#)
- [Configure Detect and Deploy patch schedules](#)
- [Configure Deploy-only patch schedules](#)
- [Configure Detect and Rollback patch schedules](#)
- [Configure Rollback-only patch schedules](#)

Fields on the Patch Schedule Details page

Fields on the *Patch Schedule Detail* page enable you to configure and schedule patch actions.

Configure section

Option	Description
Name	A name that identifies the schedule. This name appears on the <i>Patch Schedules</i> page.
Action	Select Detect. The page updates to the appropriate options. 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.
All Devices	Run the schedule on all devices. If the Organization component is enabled on your appliance, this schedule includes all devices in the selected organization. Use this setting with caution. It is usually better to test patch actions on a limited number of devices, and to limit patch actions to selected devices or device labels. This limitation ensures that patch actions are applied appropriately.  NOTE: This option only appears if the Hide All Devices check box on the <i>General Settings</i> page is not selected.
Device Labels	Restrict the patch actions to the devices in the labels that you select. Limiting the run to labels, especially Smart Labels, helps to ensure that patches are applied appropriately. For example, some application patches have the ability to install applications as well as update applications that are already installed. To prevent the appliance from installing the application on

Option	Description
	devices that do not already have the application installed, you can create a Smart Label to identify devices that have the application. You can then limit the patch action to devices that have that label. The patch is then applied only to devices that already have the application installed. To use this option, you must already have created labels or Smart Labels. See Using Smart Labels for patching.
Devices	Run detect and deploy patch actions on the devices that you select. To search for devices, begin typing in the field.
Operating Systems	Select the operating systems of the devices on which you want to run the actions. The default is all operating systems.

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. <i>All Patches</i>, 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 <i>Patch Labels</i> option.
Patch Labels	Restrict the action to the patches in the labels that you select. This is the most commonly used patch detection option. To select labels, click Edit. To use this option, you must already have labels or Smart Labels for the patches you want to detect. See Using Smart Labels for patching.

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 option is the most commonly used patch detection option. To select labels, click Edit. To use this option, you must already have labels or Smart Labels for the patches you want to detect. See Using Smart Labels for patching.

Option	Description
Maximum Deploy 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.

Rollback section

Option	Description
All Patches	Roll back all patches on the selected devices.
Labels	Restrict the action to the patches in the labels that you select. This option is the most commonly used patch detection option. To select labels, click Edit. To use this option, you must already have labels or Smart Labels for the patches you want to detect. See Using Smart Labels for patching.
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.

Notify section

Option	Description
Options	The options displayed to users when patch actions run. To perform the action without notifying the user, leave the <i>Options</i> field blank. • OK: Run immediately. • Cancel: Cancel until the next scheduled run. • Snooze: Prompt the user again after the <i>Snooze Duration</i>.
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 <i>Timeout</i> 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.
Completion Message	The message displayed to users when the patch action is complete.

Reboot section

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.

Option	Description
	When this option is selected, the following occurs according to the patching schedule: • A Detect job runs. • Patches are deployed. • If no reboot is required, and the patch list is exhausted, a final Detect job runs to verify patch status. • If a reboot is required, patching stops. When the device is rebooted, patching continues until either the patch list is exhausted, or a reboot is needed and patching stops. • When the patch list is exhausted, a final Detect job runs to verify patch status. No Reboot 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	Wait for the user to accept the reboot before restarting the device. When this option is selected, the following occurs according to the patching schedule: • A Detect job runs to identify unwanted patches. • If unwanted patches are found, the appliance attempts to remove them. • If removal is unsuccessful after the maximum number of attempts, the rollback fails and the device is ignored. • If the rollback is successful, the user is prompted to reboot. • If no user is logged in, the device is rebooted immediately. • If the user clicks OK, the device reboots. The rollback process continues until another reboot is required and the user is prompted again. The pattern continues until the patch list is exhausted. If the user snoozes or cancels the reboot, patching stops until a reboot occurs. When a reboot occurs, rollback continues until the next reboot is needed, and the user is prompted again. The pattern continues until the patch list is exhausted.
Force Reboot	Reboot 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. When this option

Option	Description
	is selected, the following occurs according to the patching schedule: • A Detect job runs. • All patches are deployed and the device is rebooted as needed. • After the last reboot, a final Detect job runs. 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 rebooted. 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 <i>Timeout</i> drop-down list. When <i>Force Reboot</i> is selected, the timeout behavior takes into consideration the <code>KUserAlert</code> and global K1000 Agent process timeouts. The global timeout, set in <code>amp.conf</code> through the <i>Agent Settings</i> page, always determines how long any agent-launched processes can run for, including the <code>KUserAlert</code> timeout. For example, if the <code>KUserAlert</code> timeout is set to two hours, and you set the global timeout to one hour, the agent will stop the <code>KUserAlert</code> because it runs too long. Therefore the global timeout must be set to the desired timeout that is longer than the <code>KUserAlert</code> timeout. This value must be set accordingly.
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.
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

Option	Description
	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 nth day every month, (for example, the first or the second) day 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): <pre>* * * * * +-----day of week (0-6) (Sun=0) +-----month (1-12) +-----day of month (1-31) +-----hour (0-23) +-----minute (0-59)</pre> 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,

Option	Description
	* / 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:
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 <i>Suspended</i>. These patching tasks do not resume on the next run and instead start from the beginning with each scheduled patching action.

Configure Detect-only patch schedules

You can create and edit Detect-only patch schedules for managed devices. This is useful when you want to detect 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 **Files detected as missing**. Running a detect-only action before the deploy creates a list of patch files to download before deployment begins.

- Go to the *Patch Schedule Detail* page:
 - Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
 - On the left navigation bar, click **Security**.
 - On the *Patch Management* panel, click **Schedules**.

- d. Display the *Patch Schedule Detail* page by doing one of the following:
 - Click the name of a patch schedule.
 - Select **Choose Action > New**.
2. In the *Configure* section, specify options for the Detect-only schedule.
See [Configure section](#) for descriptions of the options.
3. In the *Detect* section, specify options for the Detect-only schedule.
See [Detect section](#) for descriptions of the options.
4. In the *Schedule* section, specify options for the Detect-only schedule.
See [Schedule section](#) for descriptions of the options.
5. Click **Save**.

The Detect-only schedule is created. If you add devices that match the Smart Label criteria, they are automatically included in the patching schedule.

Configure Detect and Deploy patch schedules

You can create and edit patch schedules that both detect and deploy patches for managed devices. Doing so is usually appropriate for 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](#).

1. Go to the *Patch Schedule Detail* page:
 - a. Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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**.
 - c. On the *Patch Management* panel, click **Schedules**.
 - d. Display the *Patch Schedule Detail* page by doing one of the following:
 - Click the name of a patch schedule.
 - Select **Choose Action > New**.
2. In the *Configure* section, specify options for the Detect and Deploy schedule.
See [Configure section](#) for descriptions of the options.
3. In the *Detect* section, specify options for the Detect and Deploy schedule.
See [Detect section](#) for descriptions of the options.
4. In the *Deploy* section, specify options for the Detect and Deploy schedule.
See [Deploy section](#) for descriptions of the options.
5. In the *Notify* section, specify options for the Detect and Deploy schedule.
See [Notify section](#) for descriptions of the options.
6. In the *Reboot* section, specify options for the Detect and Deploy schedule.
See [Reboot section](#) for descriptions of the options.
7. In the *Schedule* section, specify options for the Detect and Deploy schedule.
See [Schedule section](#) for descriptions of the options.
8. Click **Save**.

The Detect and Deploy schedule is created. If you add devices that match the Smart Label criteria, they are automatically included in the patching schedule.

Configure Deploy-only patch schedules

You can create and edit patch schedules that perform Deploy-only actions. Doing so 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.

1. Go to the *Patch Schedule Detail* page:
 - a. Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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**.
 - c. On the *Patch Management* panel, click **Schedules**.
 - d. Display the *Patch Schedule Detail* page by doing one of the following:
 - Click the name of a patch schedule.
 - Select **Choose Action > New**.
2. In the *Configure* section, specify options for the Deploy-only schedule.
See [Configure section](#) for descriptions of the options.
3. In the *Deploy* section, specify options for the Deploy-only schedule.
See [Deploy section](#) for descriptions of the options.
4. In the *Notify* section, specify settings for the Deploy-only schedule.
See [Notify section](#) for descriptions of the options.
5. In the *Reboot* section, specify options for the Deploy-only schedule.
See [Reboot section](#) for descriptions of the options.
6. In the *Schedule* section, specify options for the Deploy-only schedule.
See [Schedule section](#) for descriptions of the options.
7. Click **Save**.

The Deploy-only schedule is created. If you add devices that match the Smart Label criteria, they are automatically included in the patching schedule.

Configure Detect and Rollback patch schedules

You can create and edit patch schedules that find and remove unwanted patches. Rollback might not be available for some patches.

See [Determine whether a patch can be rolled back](#).

1. Go to the *Patch Schedule Detail* page:
 - a. Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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**.
 - c. On the *Patch Management* panel, click **Schedules**.

- d. Display the *Patch Schedule Detail* page by doing one of the following:
 - Click the name of a patch schedule.
 - Select **Choose Action > New**.
2. In the *Configure* section, specify options for the Detect and Rollback schedule.
See [Configure section](#) for descriptions of the options.
3. In the *Detect* section, specify options for the Detect and Rollback schedule.
See [Detect section](#) for descriptions of the options.
4. In the *Rollback* section, specify settings for the Detect and Rollback schedule.
See [Rollback section](#) for descriptions of the options.
5. In the *Notify* section, specify options for the Detect and Rollback schedule.
See [Notify section](#) for descriptions of the options.
6. In the *Reboot* section, specify options for the Detect and Rollback schedule.
See [Reboot section](#) for descriptions of the options.
7. In the *Schedule* section, specify options for the Detect and Rollback schedule.
See [Schedule section](#) for descriptions of the options.
8. Click **Save**.

The Detect and Rollback schedule is created. If you add devices that match the Smart Label criteria, they are automatically included in the patching schedule.

Configure Rollback-only patch schedules

You can create and edit patch schedules that roll back selected patches. Rollback might not be available for some patches.

See [Determine whether a patch can be rolled back](#).

1. Go to the *Patch Schedule Detail* page:
 - a. Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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**.
 - c. On the *Patch Management* panel, click **Schedules**.
 - d. Display the *Patch Schedule Detail* page by doing one of the following:
 - Click the name of a patch schedule.
 - Select **Choose Action > New**.
2. In the *Configure* section, specify options for the Rollback-only schedule.
See [Configure section](#) for descriptions of the options.
3. In the *Rollback* section, specify options for the Rollback-only schedule.
See [Rollback section](#) for descriptions of the options.
4. In the *Notify* section, specify options for the Rollback-only schedule.
See [Notify section](#) for descriptions of the options.
5. In the *Reboot* section, specify options for the Rollback-only schedule.

See [Reboot section](#) for descriptions of the options.

6. In the *Schedule* section, specify options for the Rollback-only schedule.

See [Schedule section](#) for descriptions of the options.

7. Click **Save**.

The Rollback-only schedule is created. If you add devices that match the Smart Label criteria, they are automatically included in the patching schedule.

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 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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**.
2. On the *Patch Management* panel, click **Schedules**.

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.
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

Option	Description
	one of the following in the <i>Security</i> section of the <i>Device Detail</i> page: • <i>waiting to connect</i> • <i>scheduled</i> • <i>waiting to schedule</i>
Downloading	The number of managed devices that are downloading the patch. Patches with this status show the following in the <i>Security</i> section of the <i>Device Detail</i> page: <i>downloading</i>
Executing	The number of managed devices on which the patch is running. Patches with this status show one of the following in the <i>Security</i> section of the <i>Device Detail</i> page: • <i>handshake</i> • <i>detecting</i> • <i>rolling back</i> • <i>deploying</i> • <i>cleanup</i> • <i>verifying</i> • <i>alerting</i> • <i>upload</i>
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 <i>Security</i> section of the <i>Device Detail</i> page: • <i>rebooting</i> • <i>reboot pending</i> • <i>connecting</i>
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 <i>Security</i> section of the <i>Device Detail</i> page: • <i>reboot snoozed</i> • <i>snoozed</i>
Succeeded	The number of managed devices on which the patching process finished successfully. Patches with this status show the following in the <i>Security</i> section of the <i>Device Detail</i> page: <i>completed</i>.
Failed	The number of managed devices for which errors were reported during the patching process. Patches

Option	Description
	with this status show one of the following in the <i>Security</i> section of the <i>Device Detail</i> page: <i>suspended</i> <i>cancelled</i>
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 <i>Security</i> section of the <i>Device Detail</i> page: <i>not scheduled</i> .
Complete	The number of managed devices on which the patching process completed with a status of <i>Succeeded</i> , <i>Failed</i> , or <i>Offline</i> .

- (Optional) To change column visibility, select **Column Visibility** from the *Table Options* drop-down list above the table on the right.

View patch status

You can view the status of patches, including a list of the devices on which patches have been deployed.

- Go to the *Patch Detail* page:
 - Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
 - On the left navigation bar, click **Security**.
 - On the *Patch Management* panel, click **Catalog**.
 - Do one of the following:
 - If the **Show** drop-down list is set to *Applicable Packages* or *All Packages*, click the name of the package and then 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.
- 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.

- Go to the organization *Device Detail* page:
 - Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
 - On the left navigation bar, click **Inventory**.
 - Click the name of a device.
- 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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**.
 - c. On the *Patch Management* panel, click **Catalog**.
 - d. Do one of the following:
 - If the **Show** drop-down list is set to Applicable Packages or All Packages, click the name of the package and then 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.
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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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**.
 - c. On the *Patch Management* panel, click **Reporting**.

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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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**.
 - c. On the *Patch Management* panel, click **Catalog**.
 - d. Click the name of a patch.
2. Click the **Advanced Search** tab above the list on the right to display the *Advanced Search* 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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**.
 - c. On the *Patch Management* panel, click **Schedules**.
 - d. Click the name of a patch schedule.

2. In the *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.

See:

- [Configure Detect and Rollback patch schedules](#)
- [Configure Rollback-only 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 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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**.
 - c. On the *Patch Management* panel, click **Catalog**.
2. There are two drop-down lists that appear above and to the right of the patch list that display the patches on the list in different ways.
 - **Show:** There are three ways to show the patch list, Applicable Packages, All Packages, and Individual Patches.

Column	Description
Applicable Packages	View the patch list at the package level. This view shows the list of bulletins that apply to at least one managed device. This is the default filter.
All Packages	View the patch list at the package level. This view shows the list of bulletins.
Individual Packages	View each downloaded patch separately. This list is not grouped by package.

- **View By:** Control the patches shown in the list based on the drop-down list selection.

Column	Description
All Patches	View all patches.
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 .
Impact	Filter the patch list by the importance specified by Lumension. Impact levels include Critical , Recommended , and so on.
Severity	Filter the patch list by the importance specified by vendors, such as Microsoft. Severity levels include Critical , Important , Low , and so on.
Type	View Security , Non-Security , and Software Installer type patches. This classification is specified by Lumension.

Column	Description
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 you subscribe to, but that have been marked as inactive to prevent them from being detected or deployed automatically. When showing by Applicable Packages or All Packages, (x of x) might show after the status if the patches within the bulletin are both active and inactive. For example, Active (2 of 18) means 2 active out of 18.
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.
Type	The category of the patch. • Security: Critical updates released by vendors. • Non-Security: Non-critical updates. • Software Installer: Updates to software installation programs.
Impact	The importance of the patch as reported by Lumension.
Severity	The importance of the patch as determined by the publisher, such as Microsoft.

Column	Description
Reboot	Whether devices must be rebooted to complete the patching process.
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.
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. When showing by Applicable Packages or All Packages, (x of x) may show in the superseded column if some patches within the bulletin are superseded. For example, Yes (2 of 18) means 2 superseded out of 18.

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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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**.
 - c. On the *Patch Management* panel, click **Catalog**.

- d. Do one of the following:
 - If the **Show** drop-down list is set to Applicable Packages or All Packages, click the name of the package and then 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.

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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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**.
 - c. On the *Patch Management* panel, click **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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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**.
 - c. On the *Patch Management* panel, click **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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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**.
 - c. Click the name of a device.
 2. Scroll down to the *Security* section.
 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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**.
 - c. On the *Patch Management* panel, click **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.

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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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**.

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 K1000 Administrator Console, `http://K1000_hostname/admin`, then click **Settings**.
 - If the Organization component is enabled on the appliance, log in to the K1000 System Administration Console, `http://K1000_hostname/system`, or select **System** in the drop-down list in the top-right corner of the page, then click **Settings**.
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 K1000 Administrator Console, `http://K1000_hostname/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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**.
 - c. On the *Patch Management* panel, click **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 K1000 Administrator Console, `http://K1000_hostname/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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**.
 - c. On the *Patch Management* panel, click **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 **Advanced Search** 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 Dell devices and updates

You can use the K1000 appliance to manage device updates from Dell.

Managing Dell devices with Dell Updates

Using the K1000 appliance, you can keep your Dell devices up-to-date with the latest Dell updates.

These updates include:

- Software and firmware for servers
- Software and firmware for client devices
- Some Dell-supplied applications

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:

- The Dell Update subscription process differs from the K1000 patch subscription process. For instructions on subscribing to Dell Updates, see [Configure Dell Update catalog updates](#).
- 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	Configuring Dell Updates

- You manage and run patching and Dell Updates from different places in the Administrator Console:

Action	Administrator ConsolePage
Run Dell Updates	Security > Dell Updates
Manage Dell Updates	If the Organization component is not enabled on your appliance: Settings > Dell Update Subscription If the Organization component is enabled on your appliance: System > Settings > Dell Update Subscription
Run Patching Schedules	Security > Schedules
Manage Patching	Security > Subscriptions

Configuring Dell Updates

There are two steps to configuring Dell Updates.

- [Configure Dell Update catalog updates](#)
- [Create Dell Update schedules](#)

Configure Dell Update catalog updates

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 *Update Subscription* 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 K1000 System Administration Console, http://K1000_hostname/system, or select **System** in the drop-down list in the top-right corner of the page, then click **Settings**.

2. Click **Dell Update Subscription**.

The current status of the Dell catalog is displayed.

3. In the *Configure* section, select the following options:

Option	Description
All Files	Download all available updates. If you change operating systems or acquire new Dell equipment frequently, it is best to keep all Dell Updates available.
Files detected as missing	Download only the updates that you need for your managed devices.
Catalog	Click Refresh Now to update the catalogs immediately.
Update Files	Click Delete to remove all update files.
Unused files	Click Delete Unused Files to remove only those files that are not needed. This helps to limit the amount of disk space used by update files.

4. In the *Schedule* section, select the following options:

Option	Description
None	Stop Dell Updates.
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
Check for changes 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.

- In the *Download Blackout* section, select options to limit the amount of time the Dell Updates can run.
You might want to enforce a hard stop at a specific time, for example, when your users start working or if bandwidth or network traffic is an issue.
- Click **Save**.

Create Dell Update schedules

The K1000 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 patch schedule to update them. For more information about creating labels for updates and devices, see [Using Smart Labels for patching](#).

- Go to the *Dell Updates* page:
 - Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
 - On the left navigation bar, click **Security**, then click **Dell Updates**.

- 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:

- On the *Dell Updates* panel, click **Catalog**.
 - Select the check box next to an update.
 - Select **Choose Action > Change Status to > Inactive**.
- 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 a patch schedule.

To schedule inventory and updates:

- On the left navigation bar, click **Security**, then click **Dell Updates**.
- On the *Dell Updates* panel, click **Schedules**.
- Select **Choose Action > New**.
- Choose inventory and update options.

These options are similar to the options available for patch schedules. Normally, you create different schedules for the laptops, workstations, and servers, because these three types of devices have very different usage characteristics.

i **NOTE:** The Agent Timezone is only available if there is a Dell device in inventory to pull the Timezone information from.

- 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.

- f. 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.

Related topics

[Managing patch inventory](#)

[Configure Dell Update catalog updates](#)

Maintaining device and appliance security

The K1000 enables you to test the security of Agent-managed devices using standard vulnerability tests and scans. To maintain appliance security, review daily security reports, and apply appliance software updates as they become available.

Testing device security

To test device security, you can schedule OVAL vulnerability tests and SCAP scans to run on Agent-managed devices.

About OVAL security checks

OVAL (Open Vulnerability and Assessment Language) is an internationally recognized standard for detecting security vulnerabilities and configuration issues on devices.

OVAL security checks determine assets that are out of compliance and let you customize security policies to enforce rules, schedule tests to run automatically, and run reports based on the results.

OVAL is compatible with the Common Vulnerabilities and Exposures (CVE) list. CVE content is determined by the CVE Editorial Board, which is composed of experts from the international information security community. New information about security vulnerabilities discussed on the Community Forum is sent to the CVE Initiative for possible addition to the list. For more information about CVE, MITRE Corporation, or the OVAL Board, go to <http://cve.mitre.org>.

The ability to describe vulnerabilities and exposures in a common language makes it easier to share security data with other CVE-compatible databases and tools.

Understanding OVAL tests and definitions

OVAL definitions contain the information required to perform OVAL tests. This information can include checks for registry entries, file versions, and WMI (Windows Management Instrumentation) data.

OVAL test definitions pass through a series of phases before being released. Depending on where a definition is in this process, it is assigned one of the following status values:

Status	Description
Draft	Indicates that the definition is assigned an OVAL ID number and is under discussion on the Community Forum and by the OVAL Board.

Status	Description
Interim	Indicates that the definition is under review by the OVAL Board and available for discussion on the Community Forum. Definitions are generally assigned this status for two weeks, unless additional changes or discussions are required.
Accepted	Indicates that the definition has passed the Interim stage and is posted on the OVAL Definition pages. All history of discussions pertaining to Accepted definitions are linked from the OVAL definition.

Other possible status values include:

- Initial Submission
- Deprecated

For more information about the stages of OVAL definitions, go to <http://cve.mitre.org>.

When OVAL tests are enabled, all available OVAL tests run on the target devices.

OVAL test details do not indicate the severity of the vulnerability. Use your own judgment to determine whether to test your network for the presence of a particular vulnerability.

View OVAL tests and definitions

You can view OVAL tests and definitions in the Administrator Console.

- Go to the *OVAL Catalog* list:
 - Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
 - On the left navigation bar, click **Security**, then click **OVAL Scan**.
 - On the *OVAL Scan* panel, click **Catalog**.
- Optional:** Limit which tests are displayed by using the *View By* drop-down list or *Search* field to find OVAL tests by OVAL-ID, CVE Number, operating system, or text.
- Click a **Name** link in the *OVAL Catalog* list.

The *OVAL Definition Detail* page displays the following information:

Field	Description
OVAL-ID	The status of the vulnerability following the OVAL-ID. Possible values are Draft, Interim, or Accepted.
Class	The nature of the vulnerability. Possible values are: Compliance, Deprecated, Patch, and Vulnerability.
Ref-ID	A link to additional details about the vulnerability.
Description	The common definition of the vulnerability as found on the CVE list.
Definition	The steps used to test whether the vulnerability exists.

The table at the bottom of the *OVAL Tests: Definition* page displays the list of devices in your network that contain the vulnerability. For convenience, a printer-friendly version of this data is available.

Running OVAL tests

The K1000 appliance runs OVAL tests automatically based on the schedule specified in OVAL Settings.

It takes approximately one hour to run OVAL tests. In addition, OVAL Tests consume a large amount of memory and CPU resources, which might affect the performance of target devices. To minimize the disruption to users, run OVAL tests weekly or monthly and during hours when users are least likely to be inconvenienced.

In addition, you can run OVAL tests manually by logging in to the device as Administrator and running `debug.bat`. This file is usually located in the program data directory. For example:

- Windows 7 and 8: `C:\ProgramData\Dell\KACE\kbots_cache\packages\kbots\9`
- Windows XP: `C:\Documents and Settings\All Users\Dell\KACE\kbots_cache\packages\kbots\9`

Using labels to restrict OVAL tests

If you are running OVAL tests periodically or if you want to obtain the OVAL test results for only a few devices, you can assign a label to those devices. You can then use the *Run Now* function to run OVAL tests on those devices only.

For more information about using labels, see [About labels](#).

Understanding OVAL updates

The K1000 appliance checks for new OVAL definitions every night, but you should expect new definitions every month. If OVAL tests are enabled, the appliance downloads new OVAL definitions to all managed devices during the next scripting update whenever a new package becomes available, regardless of the OVAL schedule settings.

The OVAL update ZIP file can be more than 30 MB in size — large enough to impact the performance of devices with slow connections. The ZIP file includes both 32- and 64-bit versions of the OVAL Interpreter and uses the correct version for the device. The OVAL Interpreter requires Microsoft .NET Framework and supports both the full ("Extended") and Client Profile versions.

Configure OVAL Settings

To run OVAL tests, you must enable OVAL, select target devices and operating systems, and establish a run schedule.

OVAL tests require extensive resources and can affect the performance of target devices. Therefore, exercise caution when configuring OVAL settings.

1. Go to the *OVAL Schedule Detail* page:
 - a. Log in to the K1000 Administrator Console, `http://K1000_hostname/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 **OVAL Scan**.
 - c. On the *OVAL Scan* panel, click **Schedule**.
2. In the *Configure* section, specify the following settings:

Setting	Description
Enabled	Run on the target devices. Only enabled configurations can run. If OVAL tests are disabled, updates are stored on the appliance but they are not pushed out to

Setting	Description
	target devices until OVAL tests are enabled and scheduled.
Allow Run While Logged Off	Run even if no user is logged in. Clear this check box to run the item only when a user is logged in to the device.

3. In the *Deploy* section, specify the following settings:

Setting	Description
All Devices	Deploy to all devices. Clear the check box to limit the deployment to specific labels or devices.
Labels	Limit deployment to devices that belong to specified labels. To select labels, click Edit, drag labels to the <i>Limit Deployment to</i> 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 <i>Devices</i> field. The number next to the field indicates the number of devices available.
Operating Systems	Select the operating systems you want to deploy to. To select multiple items, use Ctrl-click or Command-click.  NOTE: Leave all operating systems unselected to deploy to all supported operating systems.

4. In the *Schedule* section, specify the time and frequency for running OVAL:

Setting	Description
None	Run in combination with an event rather than on a specific date or at a specific time.
Every n minutes/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.
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:

Run on next connection if offline

When the OVAL scan runs, it calculates the number of machines it is supposed to run on based on their labels, or their operating systems, or by identifying manually selected machines. Given that set of machines, the OVAL scan 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 OVAL scan skips the step that identifies online machines and it runs on the offline 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 OVAL scan (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.

Setting	Description
	By default, this option is disabled.

5. Click **Save**.
6. Click **Run Now** to run the script immediately.

Tests run on the devices selected in the *Deploy* section.

View the OVAL vulnerability report

The *OVAL Report* page shows the OVAL tests that have been run since the last time the OVAL definitions were updated.

OVAL results are deleted from this page when OVAL definitions are updated. To save the results, schedule an OVAL device report to run periodically. See [Add report schedules](#).

1. Go to the *OVAL Scan* page:
 - a. Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 **OVAL Scan**.
 - c. In the *Reporting* section, click **Show summary results**.

Apply labels to affected devices

From the *Test detail* view, you can view all the devices that failed the OVAL test, and you can assign a label to those devices so that you can patch them later.

1. Go to the *OVAL Scan Summary* page:
 - a. On the left navigation bar, click **Security**, then click **OVAL Scan**.
 - b. Under *Reporting*, click **Show device compliance**.
2. Select the check box next to one or more tests.
3. Select **Choose Action**, then select the appropriate label under *Apply Label to Affected Devices*.

You can also search tests by making the appropriate selection in the *View By* drop-down list, which appears above the table on the right.

View the OVAL Report

The *OVAL Device Compliance* page shows a list of devices with OVAL test results. Here, you can view a summary of tests that were run on specific devices.

The label under the *Device* column in the *OVAL Computer Report* page is the inventory ID assigned by the K1000 Inventory component.

For more information about any of the devices in the report, click the linked device name to navigate to the device detail page.

1. Go to the *OVAL Device Compliance* page:
 - a. Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 **OVAL Scan**.
 - c. Under *Reporting*, click **Show summary results**.

The *OVAL Device Compliance* page appears containing a list of OVAL reports.

About SCAP

SCAP (Secure Content Automation Protocol), is a set of open standards that enumerate software flaws, monitor security-related configurations and product names, and examine systems to determine the presence of vulnerabilities and rank (score) the impact of the discovered security issues on Windows devices.

SCAP is maintained by the National Institute of Standards and Technology (NIST), and its use is mandated by government agencies such as the US OMB (United States Office of Management and Budget).

SCAP uses the US government's National Vulnerability Database (NVD), which is a standards-based vulnerability management data repository. NVD includes databases of security checklists, security-related software flaws, misconfigurations, product names, and impact metrics. For more information on SCAP and NVD, go to the NIST websites at <http://scap.nist.gov/index.html> and <http://nvd.nist.gov/>.

SCAP supported versions and platforms

The K1000 appliance supports SCAP 1.0, 1.1, and 1.2, and SCAP is certified to run on Windows 7 (32-bit and 64-bit systems), Windows Vista, and Windows XP platforms.

The K1000 appliance conducts SCAP scans using the K1000 Agent software that is installed on managed devices. SCAP is not available for devices that do not have the K1000 Agent software installed, such as Agentless devices.

How the K1000 conducts SCAP scans

The K1000 appliance conducts SCAP scans by running scripts on selected Agent-managed devices using security configuration checklists from the National Checklist Repository.

For SCAP versions 1.0 and 1.1, the script checks the SCAP data stream written in XML formats using the following SCAP standards: CCE, CPE, CVE, CVSS, OVAL, and XCCDF. See [Definitions of SCAP standards](#).

SCAP 1.2 adds the concept of the "Data Stream," where all of the individual results files are combined into a single XML file. In addition, SCAP 1.2 adds a new output format called ARF (Asset Report Format 1.1). For more information, go to <http://scap.nist.gov/specifications/arf/>.

The K1000 appliance uses the Agent software to perform SCAP scan compliance checks. The results files are uploaded to the appliance or organization database and collated into a single file for reporting to a government agency (if required). Results are also displayed for each device on the appliance's *SCAP Scan Results* page.

If the Organization component is enabled on your appliance, you view SCAP scan results for each organization separately.

SCAP uses the OVAL Interpreter version 5.10.1 and provides:

- Security configuration monitoring of devices that have different operating systems and software applications.
- System security status at any given time.
- Compliance for various sets of security requirements.
- A standardized, automated way to perform security tasks.
- Interoperability across security tools.

These features improve software security, threat assessment, and vulnerability correction.



NOTE: The K1000 does not currently support Tailoring.

Definitions of SCAP standards

SCAP scans monitor device security using specified protocols and standards.

Standard	Definition
CCE	Common Configuration Enumeration provides unique identifiers to system configuration issues for facilitating fast and accurate correlation of configuration data across multiple information sources and tools. The compliance checking results produced by the K1000 Management Appliance SCAP scan include the relevant CCE ID references for XCCDF and OVAL definitions for every rule checked as designated by the checklist definition. CCE information is available both in the XCCDF result file and the appliance's <i>SCAP Scan Results</i> page.
CPE	Common Platform Enumeration is a structured naming scheme for information technology systems, platforms, and packages. Based on the generic syntax for Uniform Resource Identifiers (URI), CPE includes a formal name format, a language for describing complex platforms, a method for checking names against a system, and a description format for binding text and tests to a name. In essence, CPE ensures that the security checklist is applied to the correct platform. This information is available both in the XCCDF result file and the appliance's <i>SCAP Scan Results</i> page.
CVE	Common Vulnerability and Exposures is a list or dictionary that provides standard identifiers (common names) for publicly known security vulnerabilities and software flaws. The compliance checking results produced by the K1000 Management Appliance SCAP scan include the relevant CVE ID references and OVAL definition for every rule checked in the checklist definition. For every patch or vulnerability, CVE ID references are provided in the appliance's <i>SCAP Scan Result</i> page. The CVE information is stored in a patch result XML file generated by the scan. The file is available for inspection and verification in the Agent's working directory and on the server's <i>SCAP Scan Results</i> page.
CVSS	Common Vulnerability Scoring System provides an open framework for communicating the characteristics and impacts of IT vulnerabilities. Its quantitative model helps ensure repeatable accurate measurement while enabling users to see the underlying vulnerability characteristics that were used to generate the scores. CVSS is well suited for industries, organizations, and governments that need accurate and consistent vulnerability impact scores. Among others, CVSS

Standard	Definition
	assists prioritizing vulnerability remediation activities and calculating the severity of vulnerabilities. The National Vulnerability Database (NVD) provides CVSS scores for almost all known vulnerabilities.
OVAL	Open Vulnerability and Assessment Language is an international, information security, community standard for promoting open and publicly available security content. It standardizes the transfer of this information across the entire spectrum of security tools and services. The results of each OVAL test are written to several files on the target device and then compiled into a single result file on the appliance and displayed on the <i>SCAP Scan Results</i> page.
SCAP	Secure Content Automation Protocol is a set of open standards that enumerate software flaws, monitor security-related configurations and product names, and examine devices to determine the presence of vulnerabilities and rank (score) the impact of the discovered security issues. See About SCAP .
XCCDF	The eXtensible Configuration Checklist Description Format is a specification language for writing security checklists, benchmarks, and related documents. An XCCDF file contains a structured collection of security configuration rules for a set of target devices. The specification is designed to support information interchange, document generation, organizational and situational tailoring, automated compliance testing, and compliance scoring. See How a SCAP scan works .

About benchmarks

A SCAP benchmark is a security configuration checklist that contains a series of rules for evaluating the vulnerabilities of a device in a particular operational environment.

The NIST (National Institute of Standards and Technology) maintains the National Checklist Repository that contains various security configuration checklists for specific IT products and categories of IT products.

There are two benchmark standards:

- FDCC (Federal Desktop Core Configuration): Addresses Microsoft Windows Vista and XP operating systems.
- USGCB (United States Government Configuration Baseline): Evolved from the FDCC and currently addresses Windows XP, Windows Vista, Windows 7, and Internet Explorer versions 7 and 8.

A checklist consists of a ZIP file that contains several XML files called a SCAP Stream. The primary file in the Stream is the XCCDF file. The XCCDF file is a structured collection of security configuration rules for a set of target devices. Essentially, it is a list of OVAL tests that should be run. The other XML files contain the OVAL tests specified in the XCCDF file. For detailed information on the XCCDF Specification, go to <http://scap.nist.gov/specifications/xccdf/>.

A benchmark can contain one or more profiles. A profile specifies the rules that run on specific kinds of devices. For example, a benchmark might contain one set of rules for desktops and another set for servers.

How a SCAP scan works

Before SCAP scans are conducted, the K1000 appliance imports and verifies a benchmark. After it is imported and verified, the benchmark is loaded into the appliance and the XCCDF file undergoes a process called resolution.

During resolution, the `oval-command.zip` file is generated. This ZIP file contains the input files necessary to run a particular profile. You can view the files on the *Script Detail* page. See [Configure SCAP schedules](#).

The SCAP scan is controlled by a KScript. When the scan runs, the following files are downloaded to the target device as script dependencies:

- `benchmark.zip`: contains the benchmark files, that is, the SCAP Stream that was uploaded to the appliance. (The XCCDF file is not actually used by the device.)
- `oval-command.zip`: contains the input files generated by the XCCDF.
- `ovalref.zip`: contains the OVAL scanning engine (`ovaldi.exe`).

The KScript initiates the OVAL scans on the target device and generates several results files. The OVAL scanning engine runs two or three times:

- The first run checks that the target device is the correct platform for that benchmark profile using the CPE files contained in the benchmark.
- The second run checks the vulnerability of the device using the rules defined in the benchmark. It implements the CCE standard.
- The third run checks that the security patches are up-to-date. It implements the CVE standard.

Each run generates a results file. These files are named according to the run. For example, the file from the first run is named `scap-profile-10-result-1.xml` and the second is named `scap-profile-10-result-2.xml`. These files are located in the following directories:

Windows XP: `C:\Documents and Settings\All Users\Dell\KACE\kbots_cache\packages\kbots\<working directory>`

Windows Vista and Windows 7: `C:\ProgramData\Dell\KACE\kbots_cache\packages\kbots\<working directory>`

To find the K1000 Agent's working directory, go to **Inventory > Devices > Device Detail > Logs**.

These results files are then uploaded to the K1000 appliance and collated into a single results file (`xccdf-results.xml`). You can use this file for reporting the results to a government agency such as the US OMB (United States Office of Management and Budget). The K1000 appliance and managed device retain only the latest results files.

In the final step of a run, a subset of the results files is extracted and stored in the Organization database for reporting and displayed on the *SCAP Scan Results* page for each device.

The database tables that contain this information are `SCAP_RESULT`, `SCAP_RESULT_RULE`, and `SCAP_RESULT_SCORE`. See [View SCAP scan results](#).

Access SCAP Scan information

You can access SCAP Scan information in the *Security* section.

1. Go to *SCAP Scan* page:
 - a. Log in to the K1000 Administrator Console, `http://K1000_hostname/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 **SCAP Scan**.

- c. This page has three links:
 - **Catalog:** Shows the status of SCAP benchmarks. Additionally from this page, you can import checklists, delete checklists, and export a checklist to CSV format.
 - **Schedules:** Displays the name of the benchmarks and when they are scheduled to run. Additionally from this page, you can add and delete benchmarks, enable or disable benchmarks, and export a benchmark to CSV format.
 - **Reporting:** Shows the general results of SCAP scans.

The page also displays a dashboard that shows the results by benchmark. For a device to pass a benchmark, it must score 100%.

View and manage benchmarks

You can view and manage SCAP benchmarks, which include profiles and checklists that have been imported to the appliance.

Additionally, you can import benchmarks, delete benchmarks, and export benchmarks to CSV format by selecting **Choose Action** on the *SCAP Catalog* page.

1. Go to *SCAP Catalog* list:
 - a. Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 **SCAP Scan**.
 - c. On the *SCAP Scan* panel, click **Catalog**.
2. **Optional:** Specify which benchmarks are displayed using either the *View By* drop-down list or *Search* field.
You can search by partial string in the title or identifier.
3. **Optional:** To sort the benchmarks, click a column heading.
4. Click the name of a benchmark to view details.

The *SCAP Catalog* contains general information about the selected benchmark and the time and date that the SCAP data was uploaded to the appliance. See [Download benchmarks from the archive](#).

Import and modify benchmarks

You can import and modify benchmarks from the National Checklist Repository as needed.

Download benchmarks or checklists from the National Checklist Repository at <https://web.nvd.nist.gov/view/ncpl/repository>.

1. Go to *SCAP Catalog* list:
 - a. Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 **SCAP Scan**.
 - c. On the *SCAP Scan* panel, click **Catalog**.
2. Select **Choose Action > Import New Checklists**.
The *SCAP Configuration Scan Settings* page appears and displays Step 1 of the import wizard.
3. Click **Browse** or **Choose File** to import a benchmark ZIP file.
4. Click **Next**.

A dialog box appears indicating that the file is being uploaded. After the file is uploaded, a message appears on the *SCAP Configuration Scan Settings* page that the import was successful.



NOTE: The appliance verifies that the ZIP file contains valid benchmarks. If no valid benchmarks are present, an error message appears and the file is not uploaded.

5. Select a benchmark in the *Select a profile to scan* drop-down list, then click **Next**.

Step 2 appears.

6. Select the OVAL Engine that you want to use in the *Scan using existing engine* drop-down list.



NOTE: The default engine is MITRE's OVAL Interpreter (`ovaldi.exe`). The K1000 automatically downloads updates to this engine when Quest certifies and releases new versions of the engine and OVAL definitions.

7. **Optional:** Click **Browse** or **Choose File** to find and upload a custom engine and its configuration files.

A dialog box appears indicating that the file is being uploaded and a message appears on the *SCAP Configuration Scan Settings* page that the engine was successfully imported.



TIP: Use a custom engine if you need local control of the OVAL engine or if you do not want automatic updates to change the engine. The custom engine must be a ZIP file of a folder containing the custom `ovaldi.exe` and any necessary configuration files required to run the engine. This ZIP file replaces the `ovalref.zip` dependency file in the SCAP scan script. See [View the resolved XCCDF files](#).

8. Click **Next**.

A dialog box appears indicating that the benchmark file is being loaded, followed by the *Script Detail* page. See [Editing SCAP scan schedules](#).

Configure SCAP schedules

You can import benchmarks or definitions, and change settings for SCAP scans, by configuring SCAP schedules.

1. Go to *SCAP Scan Schedules* list:
 - a. Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 **SCAP Scan**.
 - c. On the *SCAP Scan* panel, click **Schedules**.
2. Select **Choose Action** and select an action to add or delete benchmarks, enable or disable benchmarks, and export a benchmark to CSV format.
3. Click a benchmark to edit its schedule on the *Script Detail* page.
4. Scroll down the page to the *Scheduling* section and make the necessary changes.

Editing SCAP scan schedules

You can view or edit a benchmark schedule on the *Script Detail* page. This page allows you to manage and customize scripts for configuring, scheduling, and specifying which devices the SCAP scan runs on. The scripts for SCAP are standard KScripts.



NOTE: This section does not provide information about every feature available on the *Script Detail* page; it only contains information pertinent to using and understanding a SCAP scan.

NOTE: For more detailed information on editing a KScript, see [Adding and editing scripts](#).

You can access the *Script Detail* page from the Benchmark wizard, as described in [Access SCAP Scan information](#) and from the *SCAP Scan Schedules* page, as described in [View SCAP scan results](#).

View the resolved XCCDF files

You can view the input files generated by the SCAP scan resolution process.

A benchmark is loaded into the server and the XCCDF file undergoes a process called resolution, which generates the input files necessary to run a particular profile.

1. Go to the *Script Detail* page:
 - a. Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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**.
 - c. Click the name of a script.
2. (Optional) To add any supporting executable files necessary to run the script, scroll down to the *Dependencies* section, then click **Add a new dependency**, then click **Browse** or **Choose File**.
3. **Optional:** To view the details of these files, click and download the selected ZIP file.
4. To see how these dependency files are executed, view the *Task* sections.

View the OVAL timestamp

You can view the OVAL timestamp (the time the OVAL document was compiled).

1. Go to the *Script Detail* page:
 - a. Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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**.
 - c. Click the name of a script.
2. Scroll down to the *Dependencies* section, then click **benchmark.zip** and extract the OVAL XML file.
For example, `fdcc-winxp-oval.xml`.
3. In the OVAL file, look for `<oval:timestamp>`.

View script tasks

You can view tasks associated with a particular script.

1. Go to the *Script Detail* page:
 - a. Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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**.
 - c. Click the name of a script.
2. Scroll down to the *Task* sections.

The Task sections are displayed on the *Script Detail* page.

View SCAP scan results

The *Scan Results* page shows the results of SCAP scans per device. From this page you can access detailed information about each scan.

1. Go to *SCAP Scan* page:
 - a. Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 **SCAP Scan**.
 - c. On the *SCAP Scan* panel, click **Reporting**.
2. **Optional:** To display the results for a specific benchmark, select the desired benchmark in the *View By* drop-down list, which appears above the table on the right.

The results page contains the following information:

Section	Description
Device Name	The device on which the scan was run.
Benchmark - Profile	The particular profile in a benchmark that was used.
Scanned	The date and time that the scan was run.
Passed	The number of rules that the device passed.
Failed	The number of rules that the device failed.
Other	The number of rules having other values such as error, unknown, not checked, not applicable, and informational. The XCCDF specification also defines “not selected”, which is excluded from the results.
Total	The total number of rules that were executed.
Compliance	The percentage of rules that were passed.
Score	The default score defined by the benchmark.
Result	The Pass or Fail results of the scan.

3. To view the details on a particular device, click its name in the *Device* column.

A page containing the details of the scan result for the selected device appears. The following table describes each section in more detail:

Section	Description
Summary	General information about the benchmark.
Test Results	Test results in a tree structure that represents the grouping of the rules. Symbols display the pass-fail status of a rule. You can click a rule to open a dialog box containing the rule’s details.
Scores	Compliance scores for each scoring model as defined for the benchmark.
Results by CCE	Pass-fail results by CCE. The FDCC requires that compliance is reported by CCE.
Result XML files	Links to the XML files: • XCCDF Benchmark: The file processed by the XCCDF file and formatted into a single

Section	Description
	results file (<code>xccdf-results.xml</code>) from each run of the OVAL scanning engine. • CPE Inventory: The file output by the first run of the OVAL scanning engine to test whether the benchmark applies to the device being scanned. • Oval Compliance: The file output by the second run of the OVAL scanning engine to test the device against the rules defined in the benchmark. • OVAL Patches: The file output by the third run of the OVAL scanning engine to ensure that the security patches are up-to-date. See How a SCAP scan works.

4. To view a rule's details, click the rule's icon.

The *Viewing Details* for that rule appears. This page shows a description of the rule from the XCCDF definition, whether the device passed or failed the rule, and the XML for the rule.

Download benchmarks from the archive

On a daily basis, the K1000 gathers the SCAP scan results from devices and creates an archive for each benchmark. The benchmark archive consists of a ZIP file that can be sent to the appropriate agency, such as the US OMB (United States Office of Management and Budget).

1. Go to *SCAP Catalog* list:
 - a. Log in to the K1000 Administrator Console, `http://K1000_hostname/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 **SCAP Scan**.
 - c. On the *SCAP Scan* panel, click **Catalog**.
2. Click the name of the benchmark you want to download.
3. In the *Download Results Archive* field, click the ZIP file to download the archive.

This file contains the results for all devices that have been scanned with the selected benchmark.

About security policy templates

Security policy templates enable you to create security policies or scripts. These scripts can be deployed to the devices on your network to manage their security settings.

Windows templates include:

- [Add Internet Explorer scripts](#)
- [Add XP SP3 Firewall scripts](#)
- [Add McAfee AntiVirus scripts](#)
- [Add McAfeeSuperDAT scripts](#)
- [Add Symantec AntiVirus scripts](#)

Mac templates include:

- [Add Application Layer Firewall scripts](#)
- [Add Parental Controls scripts](#)
- [Add Security scripts](#)

Using Windows security policy templates

You can use security policy templates to create scripts that configure security settings on Windows devices.



NOTE: If you edit a template-based policy, keep *Run As* set to *local system*. Using *local system* ensures that the script has full access to the Windows system, including the registry. Running the script as a different user might not provide adequate access to the Windows system.

Add Internet Explorer scripts

Use this template to create a script that controls Internet Explorer preferences. You can control specific preferences while keeping others as user-defined.

Policy settings overwrite the corresponding user's Internet Explorer preferences. Because this script modifies user settings, schedule it to run when users are logged in.

1. Go to the *Security Policies* list:
 - a. Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 **Security Policies**.
2. Click **Internet Explorer** to display the *Windows Internet Explorer* page.
3. Provide the following information:

Option	Description
Name	A name that identifies the script. This name appears on the <i>Scripts</i> page.
User Home Page	Enforce User home page policy: Force the user's home page to the specified page. Select the check box, then specify the URL to use as the home page.
Security	• Enforce Internet Zone settings policy: Specify the security level for each zone. Select the check box, then choose the security level from the <i>Security level</i> drop-down list. • Enforce Local Internet Zone settings policy: Specify the security level for intranet zones. Select the check box, then choose the security level from the <i>Security level</i> drop-down list and choose the sites to include. • Enforce Trusted Zone settings policy: Specify the security level of trusted zones. Select the check box, then choose the

Option	Description
	security level from the <i>Security level</i> drop-down list. • Enforce Zone Map: Select the check box, then specify the IP addresses or ranges.  NOTE: Domains that are not listed default to the Internet Zone.

Privacy	Control the cookies and pop-ups that are accepted by Internet Explorer from the Internet Zone. Select from these options: • Enforce Privacy settings policy: Select the check box, then set the <i>Cookie policy</i>. • Enforce Pop-up settings policy: Select the check box, then set the Pop-up filter level.

4. Click **Save** to display the *Script Detail* page.
5. Select options for configuration, deployment, and scheduling. See [Add offline KScripts or online KScripts](#).
6. To edit the raw XML used in the script, click **Edit XML** below the *Schedule* section.
7. Click **Save**.

Add XP SP3 Firewall scripts

Use this template to create scripts that enforce firewall settings on Windows XP Service Pack 3 devices.

If target devices authenticate with a domain controller, they use the Domain Policy. Otherwise, they use the Standard Policy, and tighter restrictions might be advised.

Script settings override existing settings on devices. Further, if a script disables the firewall on a device, the device user cannot enable the firewall. If the firewall is set to no policy, the user's configuration for the firewall is used.

1. Go to the *Security Policies* list:
 - a. Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 **Security Policies**.
2. Click **XP SP3 Firewall** to display the *Windows XP SP3 Firewall* page.
3. Provide the following information:

Option	Description
Name	A name that identifies the script. This name appears on the <i>Scripts</i> page.
Domain Policy	The policy used when the device has authenticated with a domain controller. If you do not have a domain controller, use the Standard Policy configuration.
Standard Policy	The policy used when the device has not authenticated with a domain controller, for example, when a device user is at home or using a Wi-Fi®

Option	Description
	hotspot. This configuration is more restrictive than the Domain Policy.
	NOTE: If the firewall is enabled, the policy settings override any settings the user might have set. If the firewall is disabled, the user cannot enable the firewall. If the firewall is set to No Policy , the user's configurations for the firewall are used.

- If you select the **Enabled** option for the firewall, specify the following options:

Option	Description
Enable logging	Enable the firewall to log information about the unsolicited incoming messages that it receives. The firewall also records information about messages that it blocks and successful inbound and outbound messages. Specify a location and name for the log file. The default is: C:\Program Files\KACE\firewall.log
Allow WMI traffic	Enable inbound TCP traffic on ports 135 and 445 to traverse the firewall. These ports are necessary for using remote administration tools such as the Microsoft Management Console (MMC) and Windows Management Instrumentation (WMI).
Allow Remote Desktop	Enable inbound TCP traffic on port 3389 to traverse the firewall. This port is required for the device to receive Remote Desktop requests.
Allow File and printer sharing	Enable inbound TCP traffic on ports 139 and 445, and inbound UDP traffic on ports 137 and 138. These ports are required for the device to act as a file or printer sharing server.
Allow Universal Plug-and-Play (UPnP)	Enable inbound TCP traffic on port 2869 and inbound UDP traffic on port 1900. These ports are required for the device to receive messages from plug-and-play network devices, such as routers with built-in firewalls.

- To specify *Inbound Port Exceptions*, click **Add Port Exception**.
Inbound port exceptions enable additional ports to be opened in the firewall. These ports might be required for the device to run other network services. An Inbound Port Exception is automatically added for port 52230 for the KACE Agent Listener, which is required to use the **Run Now** command.
- Specify a **Name**, **Port**, **Protocol**, and **Source** for the exception and click **Save Changes**.
- Click **Save** at the bottom of the page to display the *Script Detail* page.
- Select options for configuration, deployment, and scheduling. See [Add offline KScripts or online KScripts](#).
- To edit the raw XML used in the script, click **Edit XML** below the *Schedule* section.
- Click **Save**.

Add McAfee AntiVirus scripts

Use this template to create scripts that install the selected McAfee VirusScan® features on devices.

Upload the McAfee Antivirus installation files to the appliance as a ZIP archive. When you upload the ZIP archive, the McAfee application is added to the appliance software inventory if it does not already exist.

This script verifies that the software is installed with the configuration you specify. The script also confirms that the On Access Scanner (McShield) is running.

1. Go to the *Security Policies* list:
 - a. Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 **Security Policies**.
2. Click **McAfee AntiVirus** to display the *McAfee Antivirus for Windows* page.
3. Provide the following information:

Option	Description
Name	A name that identifies the script. This name appears on the <i>Scripts</i> page.
McAfee 8.0 Setup Zip	The ZIP archive that contains the installation files to use for the script. click Browse or Choose File to select the ZIP archive. Click Software Inventory to go to the <i>Software Detail</i> page to select the ZIP archive.
User Interaction	How the installation appears to users. For a description of the available options, see the McAfee documentation.
McAfee Features	The features to be installed. Use Ctrl -click or Command -click to select multiple features. To install the Alert Manager, use the McAfee tools to include the Alert Manager installation files in the deployment package. See the McAfee documentation for information about available features.
Enable On-Access Scanner	Select this check box to start McAfee's automatic file scanner after the installation is complete. The On-Access scanner scans files whenever they are accessed, for example, when opening a file or running a program.
Preserve earlier version settings	Select this check box to preserve the present configuration settings for the On-Access Scanner before the update occurs.
Lockdown VirusScan Shortcuts	Select this check box to not display any VirusScan shortcuts in the Windows Start menu.
Remove other antivirus software	Select this check box to remove competing anti-virus software that could conflict with McAfee.
Installation Directory	The directory on the target device where the application is to be installed.

Option	Description
Source Paths	Provide the path to the source McAfee ZIP file uploaded to the appliance.
Logging	The information to record in the installation log. Use Ctrl-click or Command-click to select multiple items.
Log File Name	The name of the log file.
Additional Arguments	Any additional arguments.
Reboot	Whether to restart the target device after installation.
After Installation	The action to be performed after installation. Options include Run AutoUpdate or Run AutoUpdate silently . You can also select to Scan all local drives or Scan all local drives silently .

4. Click **Save** to display the *Script Detail* page.
5. Select options for configuration, deployment, and scheduling. See [Add offline KScripts or online KScripts](#).
6. To edit the raw XML used in the script, click **Edit XML** below the *Schedule* section.
7. Click **Save**.

Add McAfeeSuperDAT scripts

Use this template to create scripts that apply McAfee SuperDAT or XDAT updates to managed devices.

Obtain the McAfee SDAT or XDAT file to use with this script.

1. Go to the *Security Policies* list:
 - a. Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 **Security Policies**.
2. Click **McAfee SuperDAT** to display the *McAfee SuperDAT for Windows* page.
3. Provide the following information:

Option	Description
Name	A name that identifies the script. This name appears on the <i>Scripts</i> page.
SDAT or XDAT file	The installation files to use for the script. click Browse or Choose File to select the ZIP archive. Click Software Inventory to go to the <i>Software Detail</i> page to select the ZIP archive.
Install Silently	The file is installed without displaying installation feedback or progress on the device.
Prompt For Reboot	If the installation requires the device to be rebooted, prompt the user before rebooting.

Option	Description
Reboot If Needed	The device is rebooted as needed. Without this option, a silent installation does not reboot the device.
Force Update	All file versions are updated, even if the device already appears to have the latest versions.

- Click **Save** to display the *Script Detail* page.
- Select options for configuration, deployment, and scheduling. See [Add offline KScripts or online KScripts](#).
- To edit the raw XML used in the script, click **Edit XML** below the *Schedule* section.
- Click **Save**.

Add Symantec AntiVirus scripts

Use this template to create scripts that install and configure the Symantec AntiVirus application. The script is intended to run periodically to ensure that Symantec AntiVirus is configured and running properly.

Upload the Symantec AntiVirus.msi file to be distributed. When you upload the file, the application is added to the appliance inventory if it does not already exist.

- Create an application inventory item and upload the Symantec AntiVirus.msi file to be distributed.
- Go to the *Security Policies* list:
 - Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
 - On the left navigation bar, click **Scripting**, then click **Security Policies**.
- Click **Symantec AntiVirus** to display the *Symantec AntiVirus for Windows* page.
- Provide the following information:

Option	Description
Name	A name that identifies the script. This name appears on the <i>Scripts</i> page.
Action	The task to be performed. Tasks include Install , Uninstall , Repair missing files , and Reinstall all files .
Software	The application to use for the script. To search for an application, begin typing in the field.
MSI Filename	The MSI filename (required if the file is a ZIP archive).
User Interaction	How the installation appears to users. Options include: Default , Silent , Basic UI , Reduced UI , and Full UI .
Install Directory	The directory on the target device where the application is to be installed.

Option	Description
Additional Switches	Any additional installer switches. Additional switches are inserted between the <code>msiexec.exe</code> and the <code>/i foo.msi</code> arguments.
Additional Properties	Any additional properties. These are inserted at the end of the command line. For example: <pre>msiexec.exe /s1 /switch2 /i patch123.msi TARGETDIR=C:\patcher PROP=A PROP2=B</pre>
After Install	What to do with the installation files when installation is complete.
Restart Options	Whether to restart the target device after installation.
Logging	The information to record in the installation log. Use Ctrl-click or Command-click to select multiple items.
Log File Name	The name of the log file.
Network Management	The network type.
Server Name	If you select Managed from the <i>Network Management</i> drop-down list, specify the server name.
Enable AutoProtect	The AutoProtect option.
Disable SymProtect	The Disable SymProtect option.
Run Live Update	The Live Update behavior.
Features to Install	The features you want to install from the <i>Features to Install</i> list. Use Ctrl-click or Command-click to select multiple features. See the Symantec documentation for specific information about the options available here. You must include the SAVMain feature for this script to work properly (although this template does not enforce this requirement).

5. Click **Save** to display the *Script Detail* page.
6. Select options for configuration, deployment, and scheduling. See [Add offline KScripts or online KScripts](#).
7. To edit the raw XML used in the script, click **Edit XML** below the *Schedule* section.
8. Click **Save**.

Using Mac security policy templates

You can use security policy templates to create scripts that configure security settings on Mac devices.

The following sections explain how to use the policies available to Mac OS X devices.



NOTE: If you edit a template-based policy, keep the *Run As* setting as local system.

Add Application Layer Firewall scripts

Use this template to create scripts that configure the Application Layer Firewall (ALF) on Mac devices.

In Mac OS X, ALF is located in Mac System Preferences.

1. Go to the *Security Policies* list:
 - a. Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 **Security Policies**.
2. In the *Mac* section, click **Application Layer Firewall** to display the *Mac Application Layer Firewall* page.
3. Provide the following information:

Option	Description
Name	A name that identifies the script. This name appears on the <i>Scripts</i> page.
Application Layer Firewall Mode	The level of security to use for the firewall.
Enable Firewall Logging	Enable the firewall to log information about the unsolicited requests, blocked requests, and successful requests.
Enable Stealth Mode	Enable the firewall to drop packages that are denied without sending error messages to requesters.
Trusted Applications	The full path to the application binaries, for example: <code>/Applications/Safari.app/Contents/MacOS/</code>

4. Click **Save** to display the *Script Detail* page.
5. Select options for configuration, deployment, and scheduling. See [Add offline KScripts or online KScripts](#).
6. To edit the raw XML used in the script, click **Edit XML** below the *Schedule* section.
7. Click **Save**.

Add Parental Controls scripts

Use this template to create scripts that configure the parental control options available on Mac OS X.

Some of the options are set using Managed Client for Mac OS X (MCX) on a local device. This method of setting options takes the place of network-based policy settings on an Open Directory server. Mixing network-based policy settings with local node settings might lead to unpredictable results.

Most of these settings require a reboot or logout and login to take effect.

1. Go to the *Security Policies* list:
 - a. Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 **Security Policies**.
2. In the *Mac* section, click **Parental Controls** to display the *Mac Parental Controls* page.
3. Provide the following information:

Option	Description
Name	A name that identifies the script. This name appears on the <i>Scripts</i> page.
Hide Profanity in Dictionary	Prevent words identified as profanity from being displayed in the dictionary on target devices.
Prohibit actions	Prevent actions from being performed on target devices.
Website Restrictions	Select the access restrictions for websites.
URLs of approved websites	If you select Allow access only to these websites , provide the URLs of the websites you want to approve. Users on target devices can only access approved websites.

- Click **Save** to display the *Script Detail* page.
- Select options for configuration, deployment, and scheduling. See [Add offline KScripts or online KScripts](#).
- To edit the raw XML used in the script, click **Edit XML** below the *Schedule* section.
- Click **Save**.

Add Security scripts

Use this template to create scripts that configure security options on Mac OS X devices.

Security options are available in Mac System Preferences.

Some of the options are set using Managed Client for Mac OS X (MCX) on a local device. This method of setting options takes the place of network-based policy settings on an Open Directory server. Mixing network-based policy settings with local node settings might lead to unpredictable results.

Most of these settings require a reboot or log out and log in to take effect.

- Go to the *Security Policies* list:
 - Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
 - On the left navigation bar, click **Scripting**, then click **Security Policies**.
- In the *Mac* section, click **Security Policies** to display the *Mac Security Policy* page.
- Provide the following information:

Option	Description
Name	A name that identifies the script. This name appears on the <i>Scripts</i> page.
Actions to enforce	The actions to perform on target devices.
Timeout	The period, in minutes, after which actions are performed.

- Click **Save** to display the *Script Detail* page.
- Select options for configuration, deployment, and scheduling. See [Add offline KScripts or online KScripts](#).
- To edit the raw XML used in the script, click **Edit XML** below the *Schedule* section.
- Click **Save**.

Resolve Windows security issues that prevent Agent provisioning

If Windows security settings prevent the K1000 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
```

Maintaining appliance security

To maintain appliance security, review daily security reports, and apply appliance software updates as they become available.

When appliance software updates are available, they are advertised on the appliance Dashboard.

Security run output

The appliance security status is provided in the security run output email.

The K1000 security run output is automatically emailed to the system administrator every day at 02:00.

The following example shows the content of the security run output.

```
Checking setuid files and devices:
Checking for uids of 0:
root 0
toor 0
Checking for passwordless accounts:
MyK1 kernel log messages:
+++ /tmp/security.GljFJvQh 2013-04-21 02:01:01.000000000 -0700
+em0: link state changed to DOWN
+em0: link state changed to UP
+em0: link state changed to DOWN
+em0: link state changed to UP
+em0: link state changed to DOWN
+em0: link state changed to UP
+em0: link state changed to DOWN
+em0: link state changed to UP
+em0: link state changed to DOWN
+em0: link state changed to UP
+em0: link state changed to DOWN
+em0: link state changed to UP
+em0: link state changed to DOWN
+em0: link state changed to UP
+em0: link state changed to DOWN
```

```
+em0: link state changed to UP  
MyKl login failures:  
MyKl refused connections:  
-- End of security output --
```


Using reports and scheduling notifications

You can configure the K1000 appliance to run reports and send notifications to administrators when specified criteria are met.

About reports and notifications

The K1000 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 K1000 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 K1000 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@K1000_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 K1000 has the Organization component enabled, and you want to access a System-level report:
Log in to the K1000 System Administration Console, http://K1000_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 K1000 components.
 - If your K1000 does not have the Organization component enabled, or if you want to access an organization-level report, log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the 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 K1000 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 *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

Option	Description
	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 <i>Reports</i> page.
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 a 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

Option	Description
	contain any software or File Synchronization rows, respectively.
4.	Click Next to display the <i>Fields to Display</i> page.
5.	Select the fields that you want to include in the report.
6.	Click Next to display the <i>Column Order</i> 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 <i>Sort and Breaks</i> 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 <i>Order By</i>.
10.	Click Next to display the <i>Filters</i> page.
11.	Optional: If you do not want to return the entire data set in your report, add filter criteria: - Click Specify rules to filter the records. A rule set, with <i>Match all of the following</i> 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. - Specify filter criteria, then click Save. - To add a rule to the current rule set, click the Add button +. - Select filter criteria, then click Save at the right of the row. - 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. - Click Save next to the rule set. - Add additional rules and rule subsets as needed.
12.	Click Save .
	The <i>Reports</i> page appears with the new report listed. The <i>View By</i> list, which appears above the table on the right, is automatically set to the category of the new report.
13.	To run the report, click a format in the <i>Generate Report</i> column.
	The output is generated. In HTML reports, the first data column is automatically linked to the detail page for the item in the Administrator Console.
	TIP: Charts and graphs cannot be created from within the K1000 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.

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 K1000 has the Organization component enabled, and you want to access a System-level report:

Log in to the K1000 System Administration Console, http://K1000_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 K1000 components.

- If your K1000 does not have the Organization component enabled, or if you want to access an organization-level report, log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the 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 K1000 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 <i>Reports</i> 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 <i>User</i> 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.

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.



TIP: Charts and graphs cannot be created from within the K1000 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.

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**.
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.
Category	The category of the report. If the category does not already exist, it is added to the drop-down list on the <i>Reports</i> 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

Option	Description
	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 <i>User</i> 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.

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 K1000 has the Organization component enabled, and you want to access a System-level report:
Log in to the K1000 System Administration Console, http://K1000_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 K1000 components.
 - If your K1000 does not have the Organization component enabled, or if you want to access an organization-level report, log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the 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 K1000 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 K1000 has the Organization component enabled, and you want to access a System-level report:

Log in to the K1000 System Administration Console, http://K1000_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 K1000 components.

- If your K1000 does not have the Organization component enabled, or if you want to access an organization-level report, log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the 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 K1000 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.

Create reports from history lists

You can create reports from any history list.

1. Go to the history list for settings, assets, or objects:
 - [View asset history](#)
 - [View object history](#)
 - [View settings history](#)
2. Select **Choose Action > Create Report**.

The *Report Detail* page appears. See [Create reports from list pages](#).

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 K1000 System Administration Console, http://K1000_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 K1000 System Administration Console, http://K1000_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](#)

Create or modify linked reports

If your environment uses Federated K1000 appliances, you can create or modify linked reports that contain consolidated information from multiple appliances.

Ensure the following settings are configured:

- **Enable linked reporting** must be selected on the *General Settings* page. For more information, see [Configure appliance General Settings with the Organization component enabled](#).
 - Each linked appliance must have access to Federation API settings and be granted the Administrator role. For more information, see [Enable access to Federation API settings](#).
1. Log in to the K1000 System Administration Console, http://K1000_hostname/system, or select **System** from the drop-down list in the top-right corner of the page.
 2. On the left navigation bar, click **Reporting**, then click **Linked Reports**.
 3. On the **Linked Reports** list that appears, do one of the following:
 - To edit an existing linked report, in the row containing the report that you want to edit, click the **Name** column.
 - To create a new linked report, select **Choose Action > New**.

The *Edit Linked Report* wizard appears, with the *Title and Category* page displayed.

4. On the *Title and Category* page, provide the following information:

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 <i>Linked Reports</i> page.
Description	A description of the report.

5. Click **Next**.
6. On the *Appliances to Run On* page that appears, select the organizations on each appliance on which you want to run the linked report.



NOTE: Do not select **System** together with one or more named organizations unless you are using a specific report definition for which that combination is valid.

7. Click **Next**.
8. On the *Report Definition* page that appears, use the drop-down controls to select the report definition to use to create the linked report.

The report definition specifies the table, fields, and processing data to use in the report. Some report definitions are included with the product, others can be created using the *Reports* page. For more information, see [Creating and modifying reports](#).

Option	Description
Select Appliance	The drop-down list is populated with all appliances that are linked with the current appliance. Select the appliance that contains the required report definition. To choose the current appliance, select Local .
Select Organization	The drop-down list is populated with all organizations on the selected appliance. Select the organization that contains the required report definition. To choose the System-level organization, select System .

Option	Description
Select Category	The drop-down list is populated with the categories for all report definitions in the selected organization. If there are definitions without a category, they are listed under NONE . Select the required category.
Select Report Definitions	The report definition that is used to generate a linked report.

9. Click **Finish**.

The *Edit Linked Report* wizard closes, and the newly created report appears in the *Linked Reports* list.

10. To view the contents of the report, the *Linked Reports* list, in the *Generate Report* column, click the format in which you want to display the report.

For example, to generate the report in HTML format click **HTML**.

The report appears in the browser window.

Scheduling reports and notifications

You can schedule reports and notifications to monitor the activity on your K1000 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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**.
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 K1000 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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**.
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 K1000 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 K1000 System Administration Console, http://K1000_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.

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 <i>Reports</i> page.
Formats	The format of the report.
Description	A description of the schedule. This description appears on the <i>Schedule Reports</i> page.

4. In the *Notify* section, 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 Zippered Attachment to attach the file as a ZIP archive.

5. In the *Schedule* section, 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 minutes/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.
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.

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 K1000 System Administration Console, http://K1000_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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 > Device Notification**
 - **New > Discovery Notification**
 - **New > Asset Notification**
 - **New > Monitoring Alerts Notification**

The *Notification* panel appears.

Choose Action ▾

Advanced Search Smart Label Notification

Notification

Name ▾ contains ▾ Windows ▾ AND ▾ Add Line Add Group

Disk % Capacity ▾ > ▾ 95 ▾ AND ▾ Add Line Add Group

Frequency: 15 Minutes ▾ Title: ▾ Recipient: ▾

Test Save

3. Select notification criteria. For example, to send a notification when Windows 7 devices have not connected to the K1000 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 **Add Line**.
- c. Specify the criteria required to find devices that have not connected to the K1000 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 <i>Subject</i> line of the email. This also appears as the name of the notification on the <i>Notification Schedules</i> 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the 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.

The screenshot shows the 'Notification' panel in the K1000 Administrator Console. The panel has a header with 'Choose Action', 'Advanced Search', 'Smart Label', and 'Notification'. The main form area is titled 'Notification' and contains the following fields and controls:

- Name:** A text input field with a dropdown arrow.
- Operator:** A dropdown menu showing 'contains'.
- Value:** A text input field containing 'Windows'.
- AND:** A dropdown menu showing 'AND'.
- Add Line:** A button.
- Add Group:** A button.
- Disk % Capacity:** A text input field with a dropdown arrow.
- Operator:** A dropdown menu showing '>'.
- Value:** A text input field containing '95'.
- AND:** A dropdown menu showing 'AND'.
- Add Line:** A button.
- Add Group:** A button.
- Frequency:** A dropdown menu showing '15 Minutes'.
- Title:** A text input field.
- Recipient:** A text input field.
- Test:** A button.
- Save:** A button.

3. Select the criteria to use for the notification schedule.

See [Example: Search for managed devices using Advanced Search criteria](#).

4. Provide the following information below the notification criteria:

Field	Description
Title	The information that you want to appear in the <i>Subject</i> line of the email. This title also appears as the name of the notification on the <i>Notification Schedules</i> 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 <i>Subject</i> line of the email. When you create notifications on the <i>Notification</i> panel, you enter this information in the <i>Title</i> field.
Recipients	The email address or addresses of intended recipients. Email addresses must be fully qualified

Field	Description
	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 **click here** next to *To re-edit the Notification using the original editor* above the **Save** button.
4. **Optional:** To change the SQL criteria that triggers the alert, click 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 servers

The K1000 offers you a module with which you can perform basic performance monitoring for your servers in inventory.

About server monitoring

The K1000 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.

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 29. Monitoring interface components under the Monitoring tab in the K1000 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

Section	Description
	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 K1000 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 K1000 comes with monitoring available for 5 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 **About K1000** in the Page-level Help panel accessible from the Help icon (🔍) in the top-right corner of the page. The line for *Management Capacity Usage* displays *Monitored Servers*, 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 K1000 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 K1000 has a number of functions that make working with alerts more efficient:

- **Alert consolidation (repeat counts):** To prevent notification spam, the K1000 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 K1000 limits the collection for any one device to 50 alerts in a single collection. The K1000 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 K1000 automatically limits a device to storing 2000 alerts before the K1000 begins deleting alerts from the database.

Getting started with server monitoring

The K1000 comes with monitoring available for a set number of servers. If a server is in inventory, you can enable monitoring for that device and have it start reporting alerts after the next inventory.



NOTE: Your K1000 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 server device in your inventory, up to a total of 200 servers, as prescribed by your K1000 license.

Eligible devices have server-class operating systems. Non-computer devices and computers without server-class operating systems cannot be monitored.

The K1000 provides two methods for enabling monitoring.

- [Enable monitoring for one or more servers 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:

- : Server monitoring is enabled and active on this Agent-managed device.
- : Server monitoring is paused on this Agent-managed device.
- : Server monitoring is enabled and active on this Agentless-managed device.
- : Server 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 servers 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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**.
2. Select the check box for each device on which you want to enable monitoring.
3. Select **Choose Action > Enable Monitoring**.

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 an individual server from its Device Detail page.

1. Go to the *Device Detail* page:
 - a. Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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**.
 - c. Click the name of a device.
2. Scroll down and click **Monitoring** under *Activities* to expand the section.

If a device is not eligible for monitoring because it does not have a server-class 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](#)

Obtain a new license key to increase server monitoring capacity

To take advantage of expanded monitoring capabilities for up to 200 servers, you must obtain a new license key. You contact the Quest Sales team to obtain the key.

1. Go to the *How to Buy* page of the Quest website: <https://quest.com/buy>.
2. Contact Sales by one of the three methods presented on the *How to Buy* page:
 - Call the toll-free number for your location.
 - Send an email to the address for your location.
 - Fill out the *Contact Form* and send it.

In the *Comments* field, include the information that you are a current K1000 user and want to gain access to the server monitoring functionality.

Update the license key information in your K1000.

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 K1000 Administrator Console, `http://K1000_hostname/admin`, then click **Settings**.
 - If the Organization component is enabled on the appliance, log in to the K1000 System Administration Console, `http://K1000_hostname/system`, or select **System** in the drop-down list in the top-right corner of the page, then click **Settings**.
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 K1000 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
<code>critical</code>	Critical
<code>error</code>	Error
<code>fatal</code>	Error
<code>fail</code>	Error
<code>K1000 monitor alert</code>	Error
<code>warn</code>	Warning
<code>unavailable</code>	Warning

You can add other alerts customized to your operational needs.

The default profiles cover the following supported operating systems:

- CentOS
- Debian
- FreeBSD
- HP-UX
- IBM-AIX
- Mac OS X
- Oracle Enterprise Linux
- Red Hat Enterprise Linux
- Solaris
- SUSE Linux
- Ubuntu
- Windows Server

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 K1000 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.

In addition, for convenience, there is a default profile that can be used if you download optional Windows Reliability and Performance Monitor (PerfMon) templates to managed Windows Server 2003 devices. See [Set up a Windows Server 2003 device with an ITNinja monitoring Log Enablement Package \(LEP\)](#).

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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 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 Criteria.
 1. On the *Criteria* category header, click the **Add** button: .
 2. Set the level, include text, exclude text (optional), and case sensitivity, and click **Save** at the right of the row.
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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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.
%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).

Element	Description
%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.

- 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 alert level, click .

- 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".

- 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.

- Go to the *Profiles* list page:
 - Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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
HP-UX	/var/adm/syslog/syslog.log
IBM-AIX	/var/adm/ras/syslog.caa
Mac OS X	/var/log/system.log
openSUSE	/var/log/messages
Oracle Enterprise Linux	/var/log/messages
Red Hat Enterprise Linux	/var/log/messages
Solaris	/var/adm/messages
SUSE Enterprise Linux	/var/log/messages
Ubuntu	/var/log/syslog
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

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](#).

i **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.

i **NOTE:** Only one log path can be defined in a profile. You must create multiple profiles for multiple logs.

For up-to-date tables of the log paths for MySQL and Apache logs, go to <http://www.itninja.com/blog/view/mysql-and-apache-profile-log-path-locations>.

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 K1000.

You have access to an XML profile file created by another user.

1. Go to the *Profiles* list page:
 - a. Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 server monitoring on a device, the K1000 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 or obtain from other sources, like ITNinja.

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 K1000 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 server 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 K1000 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 K1000, a default Windows OS and Application LEP Profile has been predefined in the K1000 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.



NOTE: PerfMon templates for Microsoft Server 2003 are available from ITNinja.

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 K1000 has predefined the criteria in the syslog defaults for all non-Windows profiles for ease of configuration.

Packages available through ITNinja

ITNinja is a product-agnostic IT collaborative community that serves as a destination for IT professionals to share with one another, and acts as a go-to resource for information on setup and deployment topics. You can browse and contribute to specific software title topics, and other topics, such as deployment, management, configuration, and troubleshooting. The K1000 server monitoring community is located at <http://itninja.com/community/k1000-monitoring>.

In ITNinja, you can find PerfMon templates beyond the standard ones available on the *Log Enablement Packages* list page. For instance, there are templates to configure monitoring for many Windows Server 2003 logs. The Log Enablement Package Install feature in the K1000 does not support Windows Server 2003. For those servers, you install their LEP by using PowerShell, with a method documented in ITNinja.

K1000 monitoring users who are members of the ITNinja community can contribute their own templates and scripts, to expand the library of available LEPs. Similar to Windows Server 2003 packages, because these LEPs

are not covered by the install process available to the standard packages, they must be installed by using one of the methods documented in ITNinja.

Install one or more LEPs on monitored devices

You can install Log Enablement Packages on Windows devices and non-Windows devices directly from the K1000.

1. Go to the *Log Enablement Packages* list page:
 - a. Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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.

Set up a Windows Server 2003 device with an ITNinja monitoring Log Enablement Package (LEP)

Windows Server 2003 Log Enablement Packages do not appear in the K1000 Log Enablement Packages list page, and the K1000 LEP installation function does not support Windows Server 2003. However, you can obtain packages from ITNinja with which to monitor Windows 2003 devices, and that entails a different setup process.

Add the Windows Server 2003 device to inventory in the K1000, managed either through an Agent or through Agentless management. See [About managing devices](#).

The process entails action on the server device that is to be monitored, and action in the K1000. On the server device, you download a Log Enablement Package from ITNinja, and start PerfMon. In the K1000, you enable monitoring for the device, define the profile from the monitoring package, and bind the profile to the device.



NOTE: Following this procedure installs one package on one device. If you want to install multiple packages with one procedure, you can find instructions on ITNinja for using PowerShell scripts to do so. See <http://itninja.com/community/k1000-monitoring>.

1. Acquire the appropriate monitoring LEP from ITNinja.
 - a. Go to the ITNinja K1000 Monitoring community page: <http://itninja.com/community/k1000-monitoring>.
 - b. From the **Downloads** tab, find the package for the Performance Category with the Performance Counters you want to probe.

You can use Search to narrow your search.
 - c. Click **Download** to download the HTM file for the package.
 - d. Copy the HTM file <Performance_Category>_Alerts.htm to the device you want to monitor.

2. On the Windows Server 2003 device you want to monitor, start the Performance Monitor and expand the **Performance Logs and Alerts** folder.
3. Under **Performance Logs and Alerts**, right-click **Alerts** and select **New Alerts Settings From . . .**
4. In the *Open* dialog, browse to the location of the package, select it, and click **Open**.
5. In the *New Alert Settings* dialog, confirm the package name and click **OK** to display the property page for the package.
6. Accept or edit the LEP properties:

- Leave the default settings, and click **OK** to leave the page.
- **Optional:** On the **General** tab of the property page, add or remove counters, and revise threshold values, if you want, then click **OK**. See [Edit the monitoring Log Enablement Package \(LEP\) for a Windows Server 2003 device](#).

7. In the Performance window, right-click on the package name and select **Start** to start the monitoring.

With the device taken care of, you move to the K1000 to enable the monitoring feature, create a profile, and bind the profile to the device.

8. On the K1000, enable monitoring for this device.
 - a. Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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**.
 - c. Click the name of the device to display its *Device Detail* page.
 - d. Scroll down and click **Monitoring** under *Activities* to expand the section.
 - e. 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 too.

9. Create the monitoring package profile on the *Profile Detail* page.
 - a. On the left navigation bar, click **Monitoring**, then click **Profiles**.
 - b. On the *Profiles* list page, select the check box next to **Windows ITNinja Plug-In Template** and select **Choose Action > Duplicate and Edit** to display the *Profile Detail* page.
 - c. Edit the name and type a description for the monitoring profile.
 - d. Use the Windows Server 2003 *Log Path*, Application.
 - e. Leave the *Log Date Format* empty.
 - f. **Optional:** Click **Edit** () , and in the drop-down menu under *Level*, select a level if you want to use something other than **Error**.
 - g. Click **Save** at the end of the criteria line, then click **Save** at the bottom of the page.
10. Add this new profile to the device.
 - a. On the left navigation bar, click **Monitoring**, then click **Devices**.

- b. Click the name of the device to display its *Monitoring Detail* page.
- c. Click in the *Profiles* field to display a drop-down list of all available profiles, and click the profile you created.
- d. Click **Save**.

The profile is bound to the device.

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: a. Select the counter in <i>Performance counters</i>. b. Edit the alert trigger using the <i>Alert when</i> drop-down list and the <i>Limit</i> field. c. Edit the collection interval using the <i>Sample interval</i> and <i>Units</i> drop-down menus. d. Click OK to save the changes. To add a performance counter to this LEP: a. Click Add to display the add counters dialog. Performance counters for applications installed locally appear in <i>Available counters</i>. You can also select objects and counters from a remote system if you use the list in <i>Select counters from computer</i> or use Browse. b. In <i>Available counters</i>, select the counter or counters you want to add, and click Add >>. c. Click OK to return to the <i>Properties</i> dialog. To remove a performance counter from this LEP: a. Select the counter in <i>Performance counters</i>. b. Click Remove. c. 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 K1000 can pick up an alert, so the

Option	Description
	check box for <i>Log an entry in the application event log</i> 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.

Edit the monitoring Log Enablement Package (LEP) for a Windows Server 2003 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, and expand the **Performance Logs and Alerts** folder.
2. Click **Alerts**, and in the details pane, right-click the LEP you want to edit.
3. **Optional:** If the package is running, select **Stop** after you right-click the LEP name.
4. Right-click the LEP name again, if necessary, and select **Properties** to display the *Properties* dialog.
5. Use the **General** tab on the *Properties* dialog to edit the package:
 - a. Select a performance counter in *Counters* to display its current configuration.
 - b. Edit the alert trigger using the *Alert when the value is* drop-down list and the *Limit* field.
 - c. Edit the collection interval using the *Interval* and *Units* drop-down menus for *Sample data every*.
 - d. Set account permissions in *Run as*.
 - By default, the package runs using the System account permission. To continue to use System account permission, leave <Default> as the entry in *Run as*.
 - Built-in groups have access to the following Performance Monitor features:

Group	Capabilities
Members of the local Administrators group	All Performance Monitor features are available
Members of the Users group	• Can change the Performance Monitor display properties • Can view log files in Performance Monitor • Cannot create an Alert Setting
Members of the Performance Monitor Users group	• Can use all features available to the Users group • Can view real-time logs in Performance Monitor and alter Performance Monitor display properties in real time • Cannot create or modify Alert Settings
Members of the Performance Log user group	• Can use all features available to the Performance Monitor Users group • Can create and modify Alert Settings after the group is assigned the log on as a batch user

6. **Optional:** Add a performance counter to the LEP:

- On the *Properties* dialog, click **Add** to display the *Add Counters* dialog.

When *Use local computer counter* is selected, performance counters for applications installed locally appear in *Select counters from list*. You can also select objects and counters from a remote system if you use the list in *Select counters from computer*.

- In *Select counters from computer*, select the counter or counters you want to add, and click **Add**.
- Click **OK** to return to the *Properties* dialog.

7. **Optional:** Remove a performance counter from the LEP:

- On the *Properties* dialog, select the counter in *Counters*.
- Click **Remove**.
- Click **OK** to save the changes.

8. Click **OK** at the bottom of the *Properties* dialog to return to Performance Monitor.

9. In the details pane, right-click the LEP 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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:

-  Server monitoring is paused on this Agent-managed device.
-  Server 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 K1000 polls the logs for alerts. In addition, you can configure the K1000 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 K1000 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 K1000 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 K1000 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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.

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.

1. Go to the *Monitoring Detail* page:
 - a. Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 <i>Maintenance Windows</i> list.
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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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**.
 2. Click the name of a device.
 3. Scroll down and click **Monitoring** under *Activities* to expand the 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. Click **Disable Monitoring**.
 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**.
 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 K1000 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**.
 2. Click the name of a device.
 3. Scroll down and click **Monitoring** under *Activities* to expand the 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**.
 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:

-  **Critical**
-  **Error**
-  **Warning**
-  **Information**
-  **Recovered**

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 <i>Subject</i> 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.
Summary	A more detailed description of the issue. You can replace or expand upon the monitoring-provided summary.
Knowledge Base Article	Look up a Knowledge Base article and append its contents to the ticket summary.
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.

Option	Description
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.
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.
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

Option	Description
	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 <i>Service Desk</i> 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 .
Process Status	The status of the workflow associated with this process template. For example, <i>Pending Approval</i> .
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.
Attachments	Files that you want to add to the ticket. You can paste up to five files. See Add or delete screenshots and attachments to Service Desk tickets .

Option	Description
Screenshots	Screenshots that you want to add to the ticket. You can paste up to five screenshots to a ticket. See Add or delete screenshots and attachments to Service Desk tickets .

Related topics

[Managing Service Desk tickets, processes, and reports](#)

Search for alerts using Advanced Search 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 Advanced Search to find critical alerts related to a connection issue.

- 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**.

- Click **Advanced Search** on the right, above the *Monitoring Alerts* list.

The *Advanced Search* panel appears.

- Specify the criteria required to find alert level:


```
Monitoring Alert Information: Level | is | Critical
```
- With **AND** selected in the operator drop-down list, click **Add Line** to add a new line, then specify the criteria required to find alerts that contain Unable to connect in the message:


```
Monitoring Alert Information: Message | contains | unable to connect
```
- 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. 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.

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.

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.



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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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, 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.
 - 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.
 - 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, and click **Save** at the right of the row.
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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance 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:

String Format (what to match)	Example Data	Include Text	Comments
			"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" 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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**.
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 K1000 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 K1000 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 a K1000 appliance, an email server, and user account information.

- **K1000 requirements:** To use Service Desk, you must have a KACE Systems Management Appliance (K1000) 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 K1000 Management 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 K1000 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://K1000_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 K1000 Management 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](#)

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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 **Queues**.
 - d. To display the *Queue Detail* page, do one of the following:
 - Click the name of a queue.
 - Select **Choose Action > New**.
2. Scroll down to the *Service Level Agreement* section. 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
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.

Option	Description
Use Business Hours/Holidays	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 .
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. i 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 K1000 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 **Queues**.
 - 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:

Field	Description
Name	The name of the <i>Service Desk</i> queue. This name appears in the <i>From</i> 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 K1000 Management Appliance email, specify an email address in the <i>Alternate Email Address</i> field.

Field	Description
Alternate Email Address	Support@mydomain.com The primary email address your users send email to. The K1000 Management Appliance also uses this address to send email from the Service Desk. Confirm that the domain name is correct for your email service. For information on creating POP3 email accounts, see Create and configure POP3 email accounts. i NOTE: As a valid email address, this address is subject to the same spam and security vulnerabilities as any other email address.

3. **Optional:** Specify POP3 settings.

To use a POP3 email server, you need to enable SMTP Server and POP3 in the appliance network settings. See [Changing appliance network settings](#).

Option	Description
POP3 Server	The hostname or IP address of the POP3 server. If you specify an IP address, enclose the address in brackets. For example [10.10.10.10].
POP3 Username	The username of an account that has access to the POP3 server.
POP3 Password	The password of the specified server account.

4. Select the **SMTP Settings** check box, then provide the following information for an external SMTP server.

To use a SMTP server, you need to enable SMTP Server in the appliance network settings. See [Changing appliance network settings](#).

i **NOTE:** If you do not use a POP3 email server, you can use the K1000 appliance's built-in SMTP server to accept incoming email messages from your internal email server.

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. If you specify an IP address, enclose the address in brackets. For example [10.10.10.10].
SMTP Port	The port number to use for the external SMTP server. For standard SMTP, use port 25. For secure SMTP, use port 587.
SMTP Username	The username of an account that has access to the external SMTP server, such as your_account_name@gmail.com.

Option	Description
SMTP Password	The password of the specified server account.
5. Click Save to create the queue and configure additional settings.	
6. Specify <i>User Preferences</i> :	
Field	Description
Allow all users as submitters	Allow anyone who is a user on the K1000 Management 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	Confirm that All Ticket Owners is the label selected. This label designates 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.
Accept email from unknown users	Allow unrecognized users to create tickets. If Accept email from unknown users is enabled in the queue configuration, any email sent to the Service Desk queue is allowed to set the <i>Submitter</i> field of a ticket, provided that the username passed in the @submitter token is that of an existing user, or 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.
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 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.

Field	Description
Default ticket owner comments to Owners Only visibility	Automatically select the <i>Owners Only</i> 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 <i>Ticket Detail</i> 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. i NOTE: By default, this warning is enabled on new queues and disabled on queues that were created in K1000 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. i 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.

7. In the *Archive Preferences* section, select settings for ticket archival. Click the **Settings** link to enable ticket archival.

i **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 opened. 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 opened. To prevent tickets in the queue from being

Option	Description
	deleted from the archive, select Never . Deleted tickets cannot be restored to the queue.
- In the *Ticket Defaults* section, select the default values for new tickets. For example:
 - Category:** Software
 - Status:** New
 - Impact:** 1 person cannot work
 - Priority:** Medium
- i** **NOTE:** If any of these fields are marked as Required in the *Customize Fields and Layout* page, the default value is ignored and users are required to select a value from the drop-down list.
- 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](#).
 - 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](#).
 - 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.
 - Click **Save**.

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.

- Go to the Service Desk *Settings* page:
 - Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
 - On the left navigation bar, click **Service Desk**, then click **Configuration**.
 - On the *Configuration* panel, click **Settings**.
- Specify the following settings:

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 <i>Service Desk Configuration</i> page and on the <i>Queue</i> list in the Administrator Console. This text also appears as an option in the <i>Choose Action</i> menu and as a heading on the <i>Ticket</i> page in the User Console.
Ticket	The text that you want to display instead of Ticket and Tickets on the <i>Ticket</i> tab and <i>Ticket</i> page in the

Setting	Description
Tickets	Administrator Console. This text also appears on the <i>Ticket</i> page in the User Console.
Process Processes	The text that you want to display instead of Process and Processes on the <i>Service Desk Configuration</i> page and on the <i>Process</i> 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 **Queues**.
 - 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* section, enable or disable the conflict warning:



NOTE: By default, this warning is enabled on new queues and disabled on queues that were created in K1000 version 6.3 or earlier.

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 <i>Ticket Detail</i> 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**.

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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 **Queues**.
 - d. To display the *Queue Detail* page, do one of the following:
 - Click the name of a queue.
 - Select **Choose Action > New**.
2. 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 *Ticket Defaults* section, click **Customize These Values** to display the *Queue Customization* page.
4. In the *Category Values* section, 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
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. 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. 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 K1000 System Administration Console, http://K1000_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**.
 - c. On the *Control Panel*, click **General Settings**.
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. In the *Logo Overrides* section, select the graphics to use:

Option	Description
User Console	The logo or other graphic displayed at the top of the User Console. Follow these guidelines for graphics: • 224 pixels wide by 50 pixels high is the default size. • 104 pixels wide by 50 pixels high stays inside the blue highlight around the Log Out link. • 300 pixels wide by 75 pixels high is the maximum size that does not impact the layout.
Report	The logo or other graphic displayed at the top of each report.

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

The default Home page and a customized version appear in the following figures.

Figure 10. Default logoUser Console Home page

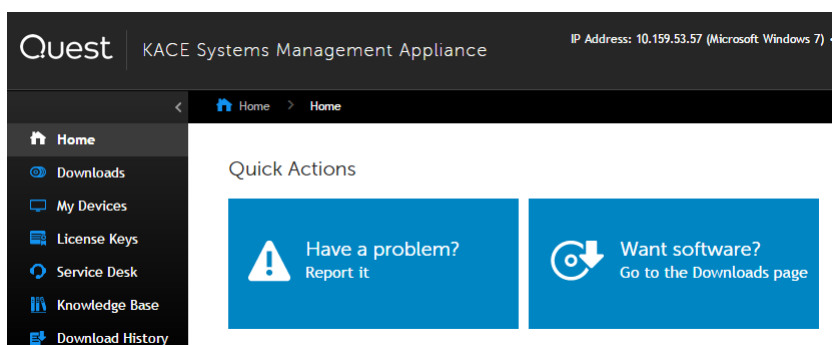


Figure 11. Custom logo onUser Console Home page

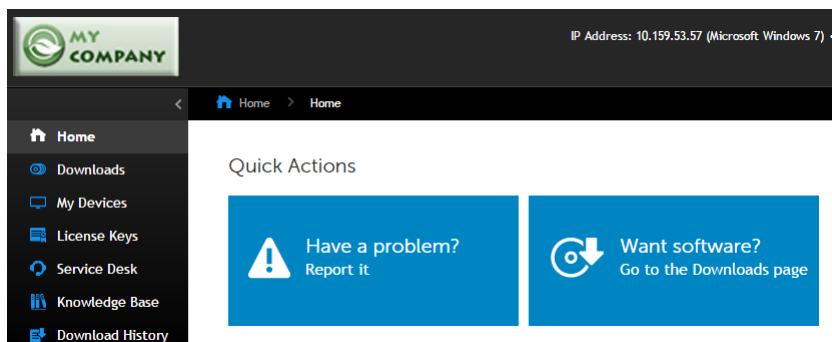


Figure 12. Default report logo

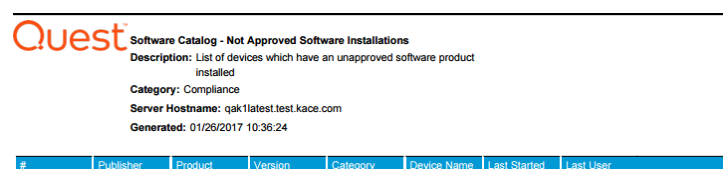


Figure 13. Custom report logo

 Software Catalog - Not Approved Software Installations Description: List of devices which have an unapproved software product installed Category: Compliance Server Hostname: qak1latest.test.kace.com Generated: 01/26/2017 10:36:24							
#	Publisher	Product	Version	Category	Device Name	Last Started	Last User

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](#).

- Go to the Admin-level *General Settings* page:
 - Log in to the K1000 Administrator Console, http://K1000_hostname/admin.
 - On the left navigation bar, click **Settings**.
 - On the *Control Panel*, click **General Settings**.
- 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.

- In the *Logo Overrides* section, select the graphics to use:

Option	Description
User Console	The logo or other graphic displayed at the top of the User Console. Follow these guidelines for graphics: 224 pixels wide by 50 pixels high is the default size. 104 pixels wide by 50 pixels high stays inside the blue highlight around the Log Out link. 300 pixels wide by 75 pixels high is the maximum size that does not impact the layout.
Report	The logo or other graphic displayed at the top of each report.

- Click **Save and Restart Services**.

The default home page and a customized version appear in the following figures.

Figure 14. Default logoUser Console home page

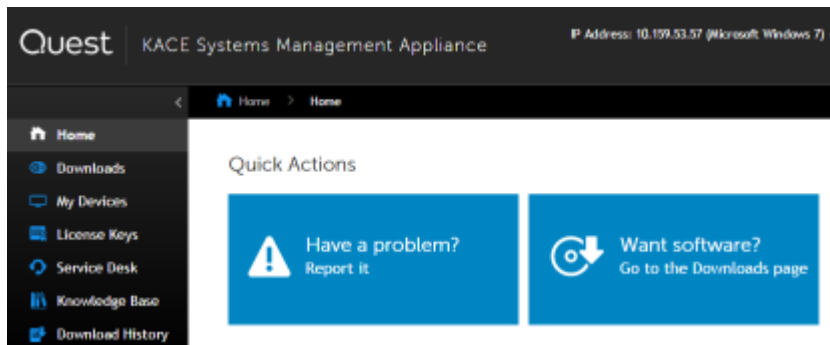


Figure 15. Custom logo on User Console home page

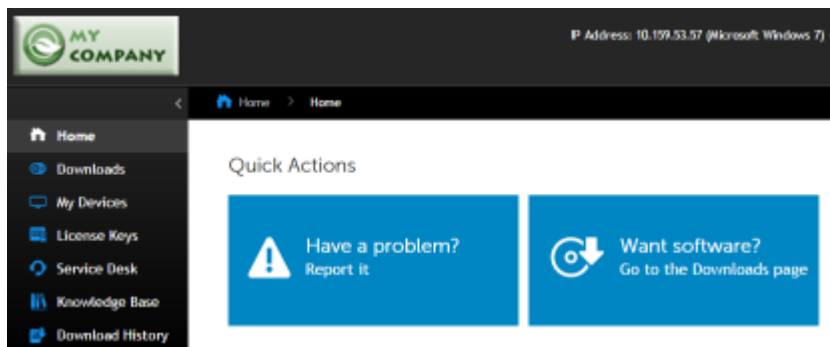


Figure 16. Default report logo



Figure 17. 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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
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 i 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 <i>Incident Quick Action</i>. 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.
Right Panel Widgets - Announcements Widget - Helpful Links Widget	Show or hide the widgets for: Announcements: Messages you want to display to the user. Helpful links: HTML links to your corporate intranet, wiki, cloud applications, or any other web resource.

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.

i **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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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.

i **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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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. i NOTE: Links cannot be used in the <i>Message Title</i> field.
Message Body	(Optional) Any additional information you want to display, including links. This information appears below the title. 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.
Assigned 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 K1000 Administrator Console, `http://K1000_hostname/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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.
URL	The URL of the link. Acceptable link formats include: • <code>http://example.com</code> • <code>https://example.com</code> • <code>http://www.example.com</code>  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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 K1000 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 **Queues**.

- d. Click the name of a queue.
2. At the top of the page, click Customize Fields and Layout to display the *Queue Customization* page.
3. In the *Layout Ticket Fields* section, click the **Edit** button in the *SAT_SURVEY* row: .
4. In the *Label* section, type the new label for the survey box.
5. Click the **Save** button to the right of the item.
6. Click the **Save** 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 **Queues**.
 - d. Click the name of a queue.
2. At the top of the page, click Customize Fields and Layout to display the *Queue Customization* page.
3. In the *Layout Ticket Fields* section, click the **Edit** button in the *SAT_SURVEY* row: .
4. In the *Permissions* section, select **Hidden** in the drop-down list.
5. Click the **Save** button to the right of the item.
6. 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 K1000 Administrator Console, `http://K1000_hostname/admin`, then click **Settings**.
 - If the Organization component is enabled on the appliance, log in to the K1000 System Administration Console, `http://K1000_hostname/system`, or select **System** in the drop-down list in the top-right corner of the page, then click **Settings**.
2. Click **Security Settings** to display the *Security Settings* page.
3. 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 K1000 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.

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://K1000_hostname/user` where K1000_hostname is the hostname of your appliance.
 - b. On the left navigation bar, click **Service Desk**.
 - 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**.
 - 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 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. Provide the following information:

Option	Description
Title	(Required) A brief description of the issue.
Summary	A more detailed description of the issue.
Submitter	The login name of the user submitting the ticket. To change the submitter, select a different login name in the drop-down list.
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 screenshots and attachments to Service Desk tickets .

Option	Description
Screenshots	Screenshots that you want to add to the ticket. You can paste up to five screenshots to a ticket. See Add or delete screenshots and attachments to Service Desk tickets .

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 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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**.
 - 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**.
 - 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 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. Provide the following information:

Option	Description
Title	(Required) A brief description of the issue.
Summary	A more detailed description of the issue.
Knowledge Base Article	Look up a Knowledge Base article and append its contents to the ticket summary.

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. To view the submitter contact information, click i. If you are creating or editing a child ticket from a process template, you also have an option to set this field to the <i>Parent Owner</i> or the <i>Parent Submitter</i> 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 i.
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 i.
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 <i>Ticket Detail</i> 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.
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

Option	Description
	field to the <i>Parent Owner</i> or the <i>Parent Submitter</i> of the associated parent 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.
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.
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 <i>Service Desk</i> 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 .

Option	Description
Process Status	The status of the workflow associated with this process template. For example, <i>Pending Approval</i> .
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. 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.
Attachments	Files that you want to add to the ticket. You can paste up to five files. See Add or delete screenshots and attachments to 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 screenshots and attachments to Service Desk tickets .

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](#).

5. 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 <i>Their Changes</i> column. These changes might conflict with the changes submitted by other users. i 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 <i>Category</i> and you have not modified that field, the change appears in the <i>Modified!</i> section. The <i>Your Changes</i> 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 <i>Category</i> to Software , and a different user changed the <i>Category</i> to Network , the changes would be summarized in the <i>Conflict!</i> section.
Modified!	A summary of the changes that do not conflict. For example, if you added information to the ticket <i>Summary</i> and a different user changed the Impact , each of the changes would be summarized in the <i>Modified!</i> section.

6. 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](#).

7. 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 <i>Their Changes</i> column. These changes might conflict with the changes submitted by other users. i 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 <i>Category</i> and you have not modified that field, the change appears in the <i>Modified!</i> section. The <i>Your Changes</i> 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 <i>Category</i> to Software , and a different user changed the <i>Category</i> to Network , the changes would be summarized in the <i>Conflict!</i> section.
Modified!	A summary of the changes that do not conflict. For example, if you added information to the ticket <i>Summary</i> and a different user changed the Impact , each of the changes would be summarized in the <i>Modified!</i> section.

8. 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.

i **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.

- Go to the *Device Detail* page:

- a. Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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**.
 - c. Click the name of a device.
2. In the *Activities* section, click **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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
 - b. On the left navigation bar, 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. You can replace or expand upon the monitoring-provided summary.
Knowledge Base Article	Look up a Knowledge Base article and append its contents to the ticket summary.
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.

Option	Description
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.

Option	Description
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.
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 <i>Service Desk</i> 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 .
Process Status	The status of the workflow associated with this process template. For example, <i>Pending Approval</i> .
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

Option	Description
	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.
Attachments	Files that you want to add to the ticket. You can paste up to five files. See Add or delete screenshots and attachments to 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 screenshots and attachments to Service Desk tickets .

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 K1000 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.

Enable email ticket creation

You can enable users to create and manage Service Desk tickets using email.

- Go to the Service Desk *Ticket Detail* page:
 - Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
 - On the left navigation bar, click **Service Desk**, then click **Configuration**.
 - On the **Configuration** panel, click **Queues**.
 - Click the name of a queue.
- Set up a valid email account, such as Support@mydomain.com, where users can send email to create tickets.
- Add the email address to the *Alternate Email Address* field.
- Select the **Allow all users as submitters** check box.
- 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.

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 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.

Field	Description
@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 <i>Name</i> portion of the email address. For example, name@domain.com.
@title	A title for the ticket.

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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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**.
 - 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* section.
 - Click a ticket referenced as *See Also*.
 - Click a ticket referenced as a *Referrer*.
 - 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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**.

- 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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**.

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

Group	View
	My Overdue Tickets My Recent Tickets
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
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
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 custom 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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**.
2. Select the **Custom View** tab above the list on the right.

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 **Test** to confirm the results.
5. Click **Create** 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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**.
2. **Optional:** Click the **Custom View** tab above the list on the right and choose the settings for the custom view. See [Create custom 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* list.

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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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**.

- c. Click the title of a ticket.
2. Click the **Comments** tab at the bottom of the ticket detail page, if it is not already selected.
3. Enter the comment in the **Comment** text box.
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 there is an attachment to add to the ticket, click **Choose File** and select the file to attach.
6. 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.
7. Click **Submit** 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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**.
 - c. Click the title of a ticket.

2. Click the **Comments** 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**.



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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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**.
 - c. Click the title of a ticket.
2. At the bottom of the *Ticket Detail* page, select the **Comments** 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 screenshots and attachments to Service Desk tickets

You can paste up to five screenshots into each Service Desk ticket. In addition, you can add up to five files as attachments to each ticket.

To paste screenshots into tickets:

- The content that you want to capture must be visible on your screen and you must be able to save a screenshot to your computer's clipboard.
- You must access the Administrator Console using one of the following or higher browsers: Internet Explorer 11, Firefox 34, or Chrome 35. Pasting screenshots is not available to earlier versions of those browsers, and it is not available to any version of Safari.



NOTE: The paste screenshot feature is hidden if you are using an earlier or unsupported browser. However, you can still attach screenshots 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.

1. With the content you want to capture visible, do one of the following to save a screenshot 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 screenshot is copied to your computer's clipboard.

2. Go to the Service Desk *Ticket Detail* page:
 - a. Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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**.
 - 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**.
 - Click the name of a ticket.

3. On the *Ticket Detail* page, scroll down to the *Attachments* section.
4. Click **Paste Screenshot**.

The screenshot dialog window appears.

5. Use one of the following key combinations to paste the screenshot into the dialog window:
 - On Windows, hold down **Ctrl**, then press **V**.
 - On Mac, hold down **command**, then press **V**.

A thumbnail of the screenshot appears in the dialog window.

6. Click **Add Screenshot**.

The filename assigned to the screenshot appears in the *Attachments* section.

7. At the bottom of the page, click **Apply Changes**.

The screenshot is added to the ticket.

8. To attach a screenshot file to the ticket:
 - a. Scroll down to the *Attachments* section of the *Ticket Detail* page.
 - b. Click **Browse** or **Choose File**.
 - c. Select a file, then click **Open**.

The name of the file appears in the *Attachments* field.

9. At the bottom of the page, click **Apply Changes**.

The file is attached to the ticket.

10. To delete an attachment from a ticket:
 - a. In the *Attachments* section, click the file you want to delete.
 - b. Click **Delete**: .
 - c. At the bottom of the page, click **Apply Changes**.

The file is deleted from 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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**.
 - 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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**.
 - 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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**.
 - 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.

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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 **Queues**.

- 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 escalation 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 **Queues**.
 - d. Click the name of a queue.
2. In the *Ticket Defaults* section, click **Customize These Values** to display the *Queue Customization* page.
3. In the *Priority Values* section, click the **Edit** button in a row to change the escalation time limit: .
4. Click **Save** in the row, then 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 **Queues**.
 - d. Click the name of a queue.
2. In the *Email on Events* section, click **Customize Emails** to display the *Service Desk Email Notifications* page.
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

Service Desk processes are ticket templates that enable you to automatically use parent and child tickets to track tasks that require 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 **Process Templates**.
 - d. To display the *Create Process Template* wizard, do one of the following:
 - Select **Choose Action > New**.
 - On the *Process Templates* page, click a process template name.

The *Create Process Template* wizard appears, with the *Define Process Template* page open.

2. On the *Define Process Template* page, 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.
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 <i>Description</i> box. For example: <pre><h1> Before you proceed:</h1> <h1> Ensure the new employee acquisition process is finalized by HR. Ensure the Badge ID exists for the new employee

 If you do not have a Badge ID, contact HR. </h1></pre> 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 <i>Service Desk</i> process type is included. You can create new process types, as required. For example, you can create a process type for accessing a

Option	Description
	specific application, or a group of applications. For more information, see Define process types .
	Click Save and Continue .
3.	On the <i>Parent Ticket</i> page that appears in the <i>Create Process Template</i> wizard, select a queue containing the parent ticket that you want to associate with this process template, and click Add Parent Ticket .
4.	On the <i>Parent Ticket</i> page that appears, 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. ◦ Most fields are similar to those on the <i>Ticket Detail</i> 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 <i>Due Date Offset</i> 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 <i>Due Date Offset</i> 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 <i>Ticket</i> list and they appear as Overdue on reports. For additional information about creating tickets, see Create tickets from the Administrator Console Ticket page. Click Save to return to the <i>Create Process Template</i> 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 <i>Parent Ticket</i> page that appears in the <i>Create Process Template</i> wizard, under <i>Child Tickets</i>, 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. b. On the <i>Child Ticket</i> page that appears, 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. For additional information about creating tickets, see Create tickets from the Administrator Console Ticket page. c. Click Save to return to the <i>Create Process Template</i> wizard.
6.	If you want the tickets created from this process template to require approvals, on the <i>Approvals</i> page that appears, select One or more approvals required for this process to start , and specify the information listed in the table below.

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.

Option	Description
Approval Step	
Approval Step 1	One or more ticket approvers, as required.
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.
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.

Option	Description
Specify Label	Any users belonging to group with this label can override approvals.

Click **Save and Continue**.

7. On the *Email Notifications* page that appears, select the recipients of email notifications for each stage of the ticket lifecycle.

When Service Desk tickets associated with this process template are created or changed, the appliance can be configured to send email notifications each time the ticket enters any of the following stages: *Process Submitted*, *Approval Required*, *Approval Timed Out*, *Approval Received*, *Approval Rejected*, *Process Cancelled*, and *Process Complete*.

For each ticket stage, you can configure the process template to send an email notification to a Submitter, Owner, Approver, and the contacts on the CC List, as required.

Some options appear pre-selected by default, but you can change that, if required. For example, by default, when an approval is required, an email notification is sent to the ticket owner and the approver using the predefined email template.

8. **Optional.** Customize the email template for one or more process stages.
 - a. On the *Email Notifications* page, in the row containing the stage whose email template you want to edit, click .
 - b. In the *Edit Email Template* dialog box, specify the following information:

Option	Description
Subject	An email subject.
Body	An email body.
Use 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 <i>Description</i> box. For more information about the Markdown syntax, visit http://daringfireball.net/projects/markdown/syntax .



TIP: If you want to reference some ticket- or process-specific information in the email subject or message body, such as the ticket title or process status, you can use email tokens. For more information about the available email tokens, see [Configure email templates](#).

- c. Click **Save**.
9. On the *Email Notifications* page, click **Save and Continue**.
10. On the *Publish Options* page 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.

Option	Description
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.
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 <i>Status</i> field does not appear on the <i>Ticket Detail</i> page, even if that field is configured to appear for the related queue. The ticket <i>Status</i> 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 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.

Create a parent ticket.

1. Go to the Service Desk *Process Detail* page:
 - a. Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 **Save**.
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 **Save**.

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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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**.
 - c. Select **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.

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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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**.
- 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* section. The level of information appearing in this section depends on the settings configured on the *Publish* page 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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**.
 - 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 **Process Templates**.
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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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**.
 - 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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**.
 - 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.

- Go to the Service Desk *Queue Detail* page:
 - Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
 - On the left navigation bar, click **Service Desk**, then click **Configuration**.
 - On the **Configuration** panel, click **Queues**.
 - Click the name of a queue.
- In the *Ticket Rules* section at the bottom of the page, click **Customize** to display the *Ticket Rules* page.
- Select **Choose Action > New (Wizard)** to display the *Define Ticket Rule* panel.
- Enter the criteria required to choose the tickets for the custom Ticket Rules. For example:


```
Priority | = | Medium
```
- Click **Test** to display tickets that match the criteria.
- Click **Next**.
- Select the values you want to change to. For example:


```
Priority | change value to | High
```
- Click **Done** to display the *Ticket Rule Detail* page.
- 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 <i>Ticket Rule</i> 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 <i>Email</i> 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 <i>Comment</i> 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 <i>Email</i> 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 <i>TITLE</i> and <i>DUE_DATE</i> 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 <i>Subject</i> field. Enter the email column name in the <i>Email</i> field, for example, OWNER_. Email is sent to each email address returned by the Select Query in this <i>Email</i> column. Enter an email message in the <i>Email Body</i> field.
Run update query	Run a second database query using the results from <i>Update Query</i> 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 <i>Ticket Rule</i> page. This query operates on the tickets selected by the Select Query. The <i>Update Query</i> 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.

Option	Description
	 NOTE: Ticket Rules that run <i>on Ticket Save</i> 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.

10. Click **Run Now** to immediately run the Ticket Rule.
11. 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 **Queues**.
 - d. Click the name of a queue.
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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 **Queues**.
 - d. Click the name of a queue.
2. In the *Ticket Rules* section at the bottom of the page, click **[Customize]** to display the *Ticket Rules* page.
3. 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**.
4. 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 **Queues**.
2. Click the queue that includes the Ticket Rule you want to move.
The *Queue Detail* page appears.
3. In the *Ticket Rules* section at the bottom of the page, click **Customize** to display the *Ticket Rules* page.

 **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.
4. Select the check box next to the Ticket Rule.
5. 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 K1000 appliance includes a set of pre-configured reports for Service Desk data.

1. Go to the *Reports* list:
 - a. Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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**.
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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 **Settings**.
2. In the *Ticket Archival* 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
None	Run in combination with an event rather than on a specific date or at a specific time.
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.
Custom	Run according to a custom schedule. Use standard 5-field cron format (extended cron format is not supported): <pre>* * * * * +-----day of week (0-6) (Sun=0) +-----month (1-12) +-----day of month (1-31) +-----hour (0-23) +-----minute (0-59)</pre> 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

Option	Description
	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:
Run Now	Run immediately for all queues for which archiving has been configured. See Archive selected tickets .

4. 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](#).

- Go to the Service Desk *Queue Detail* page:
 - Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
 - On the left navigation bar, click **Service Desk**, then click **Configuration**.
 - On the **Configuration** panel, click **Queues**.
 - Click the name of a queue.
- In the *Archive 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 opened. 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.

Option	Description
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 opened. 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 <i>Archive Preferences</i> .	

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](#).

- Go to the Service Desk *Tickets* list:
 - Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
 - On the left navigation bar, click **Service Desk**.
- Select the check box next to one or more tickets.
- Select **Choose Action > Archive**.
- On the confirmation dialog, click **Yes**.
- 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.

- Go to the Service Desk *Archived Tickets* list:
 - Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
 - On the left navigation bar, click **Service Desk**, then click **Archive**.
- Select the check box next to one or more archived tickets.
- 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.

- Go to the Service Desk *Archived Tickets* list:
 - Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 **Queues**.
 - d. Click the name of a queue.
2. In the *User Preferences* section, 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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**.
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.

About Service Desk ticket queues

Service Desk tickets are stored in one or more queues on the K1000 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 **Queues**.
 - 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 K1000 Management Appliance directly (forwarding email to the K1000 Management Appliance), the local portion of the K1000 Management 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 K1000 Management Appliance confirms this before allowing you to save the new queue.

3. 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 K1000 Management 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 **Queues**.
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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 **Queues**.
 - 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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**.
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.

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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 **Settings**.
2. In the *Queue Preferences* section, 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.
All Queues	Display the <i>All Queues</i> view by default. When this is selected, the <i>All Queues</i> 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

Option	Description
	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](#).

- 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.

- Go to the *User Detail* page:
 - Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
 - On the left navigation bar, click **Settings**, then click **Users**.
 - Click the name of a user.
- 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 <i>All Queues</i> view by default. When this is selected, the <i>All Queues</i> 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.

- 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 **Settings**.
 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. Click **Save**.
 4. Click **Customize List Layout for All Queues View** to display the *Layout* page.
 5. 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.
6. For each field you edit, click **Save** at the end of the row.
The default queue settings are saved.
 7. 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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**.
 - c. Click the title of a ticket.
2. Select **Choose Action > Move to queue > queue name**.
3. Click **Yes** to confirm the ticket move.
4. Click **Save** to save the ticket in the new queue.

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 K1000 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 K1000 *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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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. i TIP: When you add a cataloged software item to user downloads, the <i>User Downloads</i> (Administrator Console) and <i>Downloads</i> (User Console) pages display some additional information about that application in the <i>Category</i>, <i>License Type</i>, <i>Platform</i>, <i>End of Life</i>, <i>General Availability</i>, and <i>MSRP</i> (\$) 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. 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

Option	Description
	Scripting > Scripts. Devices must have the Agent software installed to run scripts.

- 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.
- Specify the information to include:

Field	Description
Product Key	Send the product key to users when they download the application. To view <i>Asset Detail</i> license information, click Assets .
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 <i>Asset Detail</i> 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.

- In the *Access Control* section, specify distribution restrictions:

Field	Description
Labels	(Optional) Click Edit to select a label and limit application deployment to users who are included in the label.
Also Restrict By Device Label	(Optional) Restrict access to specific device labels.

- 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.

- Go to the *User Downloads* list:

- a. Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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."
Use Markdown	Allow both markdown and full HTML text. Markdown is a plain text formatting syntax and a software tool, written in Perl, that converts plain-text formatting to HTML. It translates an easy-to-read/easy-to-write structured text into HTML. Markdown's text format is similar to that of plain text and supports headers, <i>*emphasis*</i>, code blocks, block quotes, and links. The following are formatting examples you can use if the <i>Use Markdown</i> check box is selected: <i>*normal emphasis with asterisks*</i> = normal emphasis with asterisks **strong emphasis with asterisks** = strong emphasis with asterisks For more information about markdown, go to http://daringfireball.net/projects/markdown/.
Assign 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.

Field	Description
	i NOTE: To include external links to web pages, use the <code>href</code> format. For example, <code>Visit Quest KACE!</code>. To include images, use the <code>src</code> format. For example, <code></code>. 3. Optional: In the <i>Attachments</i> section, click Add, then click Browse or Choose File to add an attachment. 4. Click Save. i TIP: To create a Knowledge Base article from the comments in a ticket, click Create KB article on the <i>Ticket Detail</i> page. The K1000 Management Appliance assigns the Knowledge Base article an Article ID and displays it on the <i>Knowledge Base</i> page. To see how the Knowledge Base article appears to users in the User Console, click the Knowledge Base article's title on the <i>Knowledge Base</i> page, then click the User URL on the <i>Article Detail</i> page. 5. Optional: Click Duplicate.

Delete Knowledge Base articles

You can delete Knowledge Base articles to permanently remove them from the appliance.

- Go to the *Knowledge Base Articles* list:
 - Log in to the K1000 Administrator Console, `http://K1000_hostname/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
 - On the left navigation bar, click **Service Desk**, then click **Knowledge Base**.
- Select the check box next to one or more articles.
- 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.

- Go to the Knowledge Base *Article Detail* page:
 - Log in to the K1000 Administrator Console, `http://K1000_hostname/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
 - On the left navigation bar, click **Service Desk**, then click **Knowledge Base**.
 - 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.

- 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.

i **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:

Category:

Hardware	▼
Monitor	▼

When users select the *Monitor* subcategory, you might want to display additional subcategories, such as model information:

Category:

Hardware	▼
Monitor	▼
AceElectronics	▲
ClearView2000	
AceElectronics	

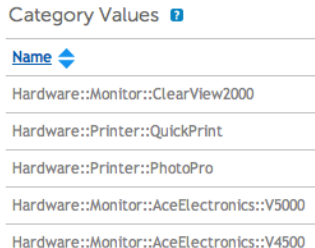
Most customers use a two-tiered approach to categories and subcategories. They create general categories and subcategories for users, such as:

- 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 **Queues**.
 - 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 *Ticket Defaults* section, click **Customize These Values** to display the *Queue Customization* page.
3. In the *Category Values* section, click the **Add** button: **+**.
A new row appears.
4. Provide the following information in the row:

Field	Description
Name	The name of the category or subcategory. To create a subcategory, use this syntax: Category 1::Subcategory A To create multiple subcategories, use this syntax: Category 2::Subcategory A::Subcategory B On the <i>Queue Customization</i> page, categories and subcategories appear as follows: 

On the *Ticket Detail* page, categories and subcategories appear as follows:

Field	Description
	Category: Hardware Monitor AceElectronics V5000 V5000 V4500
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	Allow 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.

- Click **Save** in the row.

The icons to the right of each row allow 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: .

- 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 **Queues**.
 - 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 *Ticket Defaults* section, click **Customize These Values** to display the *Queue Customization* page.
3. In the *Status Values* section, 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 **Queues**.
 - 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 *Ticket Defaults* section, click **Customize These Values** to display the *Queue Customization* page.
3. In the *Priority Values* section, 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.
Escalation Time	(Optional) Enter a time limit, after which an open ticket of this priority is escalated. Enter a time integer and a unit from the drop-down list. See Using the ticket escalation process .
Use Business Hours/Holidays	(Optional) Whether to use the settings for business hours and holidays when calculating the priority of tickets in the queue. If business hours and holidays are configured for the Service Desk, select this check box to take these hours and holidays into account when determining whether to escalate tickets based on their priority. Clear the check box to ignore settings for business hours and holidays in this queue.

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 Detail* 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 **Queues**.
 - 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 *Ticket Defaults* section, click **Customize These Values** to display the *Queue Customization* page.
3. In the *Impact Values* section, 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 **Queues**.
 - d. To display the *Queue Detail* page, do one of the following:
 - Click the name of a queue.
 - Select **Choose Action > New**.
2. At the top of the page, click **Customize Fields and Layout** to display the *Queue Customization* page with the *Layout*, and *Related Ticket Fields*:

Section	Description
Layout Ticket Fields	This section includes the <i>Survey</i>, <i>Title</i>, and <i>Summary</i> fields, the <i>Submitter</i>, <i>Asset</i>, and <i>Device</i> sections, and any other fields that are not displayed in the <i>Related Ticket Fields</i> 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 <i>Ticket</i> page in the specified order. All fields in this section are displayed in a two-fields-per-row format except the <i>Resolution</i> field, which occupies a full row.  NOTE: If the <i>Summary</i> field is hidden, the <i>Comment</i> field is displayed on the <i>New Ticket</i> page. Text entered in the <i>Summary</i> 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 Fields	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 <i>Ticket Detail</i> 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 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 Field Options 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 **Queues**.
 - d. To display the *Queue Detail* page, do one of the following:
 - Click the name of a queue.
 - Select **Choose Action > New**.
2. At the top of the page, click **Customize Fields and Layout** to display the *Queue Customization* page.
3. In the *Comment Field Options* section, 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 **Queues**.

- d. To display the *Queue Detail* page, do one of the following:
 - Click the name of a queue.
 - Select **Choose Action > New**.
2. At the top of the page, click **Customize Fields and Layout** to display the *Queue Customization* page.
3. In the *Custom Fields* section, 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 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.

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 queue, 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.

1. Go to the Service Desk *Queue Detail* page:
 - a. Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, 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 **Queues**.

- c. To display the *Queue Detail* page, do one of the following:
 - Click the name of a queue.
 - Select **Choose Action > New**.
2. At the top of the page, click **Customize Fields and Layout** to display the *Queue Customization* page.
3. Make your customizations, as required.
4. On the **Queue Customization** page, in the top-left corner, click **Preview Form As**.
5. Choose one of the following options, as required:

Option	Select it to view...
Input Form - User	<i>New Ticket</i> page, as a User
Input Form - Owner	<i>New Ticket</i> page, as a Ticket Owner
Edit Form - User	<i>Ticket Detail</i> page, as a User
Input Form - Owner	<i>Ticket Detail</i> page, as a Ticket Owner

6. Click **Preview**.
The *Confirm* dialog box appears, asking you to save your changes before displaying a preview.
7. In the *Confirm* dialog box, click **Save**.
The dialog box closes and your preview appears. A note at the top of the page indicates that your changes are saved and that you are previewing the selected page.
8. To return to the **Queue Customization** page, in the top-right corner, click **Back to Queue Configuration page**.

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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 **Queues**.
 - d. To display the *Queue Detail* page, do one of the following:
 - Click the name of a queue.
 - Select **Choose Action > New**.
2. At the top of the page, click **Customize Fields and Layout** to display the *Queue Customization* page.
3. Scroll down to the **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.

4. Click **Save** at the bottom of the page.

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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 **Queues**.

- d. To display the *Queue Detail* page, do one of the following:
 - Click the name of a queue.
 - Select **Choose Action > New**.
2. At the top of the page, click **Customize Fields and Layout**.
3. Scroll down to the *Related Ticket Fields* section 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 **Queues**.
 - 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* section, select the *Allow parent tickets to close child tickets* check box.
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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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**.
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**.

i **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**.

i **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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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**.
 - 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**.
2. In the *Related Ticket Information* section, 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance 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. 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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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** to display the *Service Desk Queues* page.
6. Click the name of a queue to display the *Queue Detail* page.
7. In the *User Preferences* section, clear the *Allow all users as approvers* check box, then click **Save**.
8. In the *Ticket Defaults* section, click **Customize These Values** to display the *Queue Customization* page.
9. In the *Ticket Layout* 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 K1000 appliance

You can connect your email server to the K1000 appliance so that the K1000 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 K1000_HelpDesk.
4. Select **Administrative Groups > Connectors > K1000_HelpDesk** to display the *K1000_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 K1000 SMTP server. Use the following settings:
 - **Type:** SMTP
 - **Address:** Enter the fully qualified K1000 server name. The syntax is k1000.mydomain.com.
 - **Cost:** Set this to one level above the other connectors. That way, K1000 email is filtered first, and no K1000 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 *K1000_HelpDesk Properties* page.

Your email server is now connected to the K1000 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 K1000 Management Appliance includes an internal SMTP server. If most of the email traffic coming to the K1000 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 K1000 Management 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 K1000 Administrator Console, `http://K1000_hostname/admin`, then click **Settings**.
 - If the Organization component is enabled on the appliance, log in to the K1000 System Administration Console, `http://K1000_hostname/system`, or select **System** in the drop-down list in the top-right corner of the page, then click **Settings**.
2. Click **Network Settings** to display the *Network Settings* page.
3. In the *Email Configuration* section, clear the **Enabled** 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 K1000 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 K1000 Management 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 K1000 Administrator Console, `http://K1000_hostname/admin`, then click **Settings**.
 - If the Organization component is enabled on the appliance, log in to the K1000 System Administration Console, `http://K1000_hostname/system`, or select **System** in the drop-down list in the top-right corner of the page, then click **Settings**.
3. Click **Network Settings** to display the *Network Settings* page.
4. In the *Email Configuration* section, select the **Enable SMTP Server** check box.
The SMTP server options appear.
5. Specify the 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.
Port	Enter the port number to use for the 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 <code>your_account_name@gmail.com</code> .
Password	Enter the password of the specified account.
Enable Service Desk POP3 Server	Select this check box to use POP3 for Service Desk ticket email.

6. **Optional:** To enable POP3 email for a queue, go to the Service Desk *Queue Detail* page:
 - a. Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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 **Queues**.
 - d. To display the *Queue Detail* page, do one of the following:
 - Click the name of a queue.
 - Select **Choose Action > New**.
7. In the top section of the page, select **Configure SMTP Settings**.
8. In the top section of the page, specify the following SMTP server settings:



NOTE: POP3 options are available only if *Service Desk POP3 Server* is enabled in the appliance Network Settings. See [Changing appliance network settings](#).

Option	Description
POP3 Server	Enter the name of the POP3 server you want to use for the queue. For example, <code>pop.gmail.com</code> .
POP3 User / Password	Enter the username and password of an account that has access to the POP3 server.
SMTP Server	Specify the hostname or IP address of an SMTP server, such as smtp.gmail.com . The SMTP server 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

Option	Description
	must be configured to allow the relaying of email from the appliance without authentication.
SMTP Port	Enter the port number to use for the SMTP server. For standard SMTP, use port 25. For secure SMTP, use port 587. If you leave this field blank, the appliance uses the settings specified on the <i>Network Settings</i> page.
SMTP User / Password	Enter the username and password of an account that has access to the SMTP server.

9. Select **Use SSL**.

10. 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 K1000. To change this setting, see the setting, *Accept email from unknown users* in the section [Configuring Service Desk ticket queues](#).

Maintenance and troubleshooting

The K1000 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 K1000 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 K1000 version number and date, and only paired backup files can be used to restore the appliance.



NOTE: Beginning with the 6.4 release of the K1000 appliance, backups are created while the K1000 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.
- **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 K1000 Administrator Console, `http://K1000_hostname/admin`, then click **Settings**.
 - If the Organization component is enabled on the appliance, log in to the K1000 System Administration Console, `http://K1000_hostname/system`, or select **System** in the drop-down list in the top-right corner of the page, then click **Settings**.
2. Click **Backup Settings** to display the *Backup Settings* page.
3. In the *Retention* section, specify the following settings:

Option	Description
Daily	The number of daily backups to retain on the appliance. You can retain up to seven daily backups.
Monthly	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 *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 K1000 Administrator Console, `http://K1000_hostname/admin`, then click **Settings**.
 - If the Organization component is enabled on the appliance, log in to the K1000 System Administration Console, `http://K1000_hostname/system`, or select **System** in the drop-down list in the top-right corner of the page, then click **Settings**.
2. Click **Backup Settings** to display 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.

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 K1000 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 K1000 Administrator Console, `http://K1000_hostname/admin`, then click **Settings**.
 - If the Organization component is enabled on the appliance, log in to the K1000 System Administration Console, `http://K1000_hostname/system`, or select **System** in the drop-down list in the top-right corner of the page, then click **Settings**.
2. Click **Backup Settings** to display the *Backup Settings* page.
3. In the *Backups* section download a matched pair of Differential and Base backup files:
 - a. Click the name of a backup file with `incr` in the filename. For example: `<date>_k1_incr_<version>.tgz`.
 - b. If prompted, select a download location for the file.
 - c. Click the name of a backup file with `base` in the filename. For example `<date>_k1_base_<version>.tgz`.
 - d. If prompted, select a download location for the file.

Access backup files through FTP

You can use FTP to access K1000 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 kl_base.tg
> get kl_base.tgz
> get kl_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 you have a VK1000, and you use virtual machine snapshots to back up appliance data instead of using the K1000 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 VK1000. Disabling backups is not recommended for physical versions of the K1000 appliance.

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 VK1000. Disabling backups is not recommended for physical versions of the K1000 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 K1000 Administrator Console, `http://K1000_hostname/admin`, then click **Settings**.
 - If the Organization component is enabled on the appliance, log in to the K1000 System Administration Console, `http://K1000_hostname/system`, or select **System** in the drop-down list in the top-right corner of the page, then click **Settings**.
3. Click **Backup Settings** to display the *Backup Settings* page.
4. In the *Retention* section, 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.

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 K1000 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 K1000 Administrator Console, `http://K1000_hostname/admin`, then click **Settings**.
 - If the Organization component is enabled on the appliance, log in to the K1000 System Administration Console, `http://K1000_hostname/system`, or select **System** in the drop-down list in the top-right corner of the page, then click **Settings**.
2. Click **Backup Settings** to display the *Backup Settings* page.
3. In the *Backups* section, 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.

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 K1000 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 K1000 Administrator Console, `http://K1000_hostname/admin`, then click **Settings**.
 - If the Organization component is enabled on the appliance, log in to the K1000 System Administration Console, `http://K1000_hostname/system`, or select **System** in the drop-down list in the top-right corner of the page, then click **Settings**.
 2. Click **Backup Settings** to display the *Backup Settings* page.
 3. In the *Uploads* section, under the *Differential* heading, click **Browse** or **Choose File**, to locate the Differential file you want to upload.
 4. In the *Uploads* section, under the *Base* heading, click **Browse** or **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 K1000 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 K1000 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](#).

1. Go to the appliance *Control Panel*:

- If the Organization component is not enabled on the appliance, log in to the K1000 Administrator Console, `http://K1000_hostname/admin`, then click **Settings**.
- If the Organization component is enabled on the appliance, log in to the K1000 System Administration Console, `http://K1000_hostname/system`, or select **System** in the drop-down list in the top-right corner of the page, then click **Settings**.

2. Click **Backup Settings** to display the *Backup Settings* page.

3. In the *Restore* section, select the pair of files you want to restore.

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.

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 K1000 Administrator Console, `http://K1000_hostname/admin`, then click **Settings**.
 - If the Organization component is enabled on the appliance, log in to the K1000 System Administration Console, `http://K1000_hostname/system`, or select **System** in the drop-down list in the top-right corner of the page, then click **Settings**.
2. Click **Backup Settings** to display the *Backup Settings* page.
3. At the bottom of the page, click **Factory Reset**, 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 K1000 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 K1000 Administrator Console, `http://K1000_hostname/admin`, then click **Settings**.
 - If the Organization component is enabled on the appliance, log in to the K1000 System Administration Console, `http://K1000_hostname/system`, or select **System** in the drop-down list in the top-right corner of the page, then click **Settings**.
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 K1000 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 K1000 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 K1000 Administrator Console, `http://K1000_hostname/admin`, then click **Settings**.
 - If the Organization component is enabled on the appliance, log in to the K1000 System Administration Console, `http://K1000_hostname/system`, or select **System** in the drop-down list in the top-right corner of the page, then click **Settings**.
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 K1000 Administrator Console, `http://K1000_hostname/admin`, then click **Settings**.
 - If the Organization component is enabled on the appliance, log in to the K1000 System Administration Console, `http://K1000_hostname/system`, or select **System** in the drop-down list in the top-right corner of the page, then click **Settings**.
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 the Help button (🔗) in the top-right corner of the page, then click **About K1000** at the bottom of the *Help* panel to verify the current version. See [View the K1000 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 K1000 Administrator Console, `http://K1000_hostname/admin`, then click **Settings**.
 - If the Organization component is enabled on the appliance, log in to the K1000 System Administration Console, `http://K1000_hostname/system`, or select **System** in the drop-down list in the top-right corner of the page, then click **Settings**.
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 K1000 Administrator Console, `http://K1000_hostname/admin`, then click **Settings**.
 - If the Organization component is enabled on the appliance, log in to the K1000 System Administration Console, `http://K1000_hostname/system`, or select **System** in the drop-down list in the top-right corner of the page, then click **Settings**.
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**. The appliance restarts and then verifies the database.
 - Click **Shutdown**. The appliance shuts down, and it is safe to power-down the appliance hardware.

Update OVAL definitions from KACE

Although the definitions for OVAL (Open Vulnerability Assessment Language) tests are updated automatically on a scheduled basis, you can retrieve the latest files manually from the *Appliance Updates* page.

For more information about OVAL definitions, see [Maintaining device and appliance security](#).

1. Go to the appliance *Control Panel*:
 - If the Organization component is not enabled on the appliance, log in to the K1000 Administrator Console, `http://K1000_hostname/admin`, then click **Settings**.
 - If the Organization component is enabled on the appliance, log in to the K1000 System Administration Console, `http://K1000_hostname/system`, or select **System** in the drop-down list in the top-right corner of the page, then click **Settings**.
2. On the left navigation bar, click **Appliance Updates** to display the *Appliance Updates* page.
3. In the *OVAL Catalog* section, click **Check for Update**, then click **Yes**.

Understanding the daily run output

The K1000 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.
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.

Column heading	Description
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    0
lo0       16384 <Link#3>      392328      0 392328    0    0
lo0       16384 fe80:3::1      fe80:3::1    0    0    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 K1000 Administrator Console, `http://K1000_hostname/admin`, then click **Settings**.
 - If the Organization component is enabled on the appliance, log in to the K1000 System Administration Console, `http://K1000_hostname/system`, or select **System** in the drop-down list in the top-right corner of the page, then click **Settings**.
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 K1000 appliances, the status of RAID drives is displayed in the server logs. This status is available for physical K1000 appliances 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 K1000

The K1000 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 K1000 Administrator Console, `http://K1000_hostname/admin`, then click **Settings**.
 - If the Organization component is enabled on the appliance, log in to the K1000 System Administration Console, `http://K1000_hostname/system`, or select **System** in the drop-down list in the top-right corner of the page, then click **Settings**.
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**.

Enable a tether to Quest Support

Tethering the K1000 appliance to Quest Support enables Quest representatives to access your appliance for troubleshooting.

The tether uses a key pair that consists of a public key and a private key. The public key is provided by Quest Support and used to encrypt the tether key. The private key resides on your K1000 and is used to decrypt the tether key.

In addition, you can create an admin-level user account that Quest Support can use to log in to the Administrator Console for troubleshooting. Using this dedicated account is helpful for tracking the actions performed by Quest Support. This account can be used with or without the tether.

Contact Quest Support and do the following:

- Tell the representative that you want to enable a tether to your K1000 for troubleshooting.
- Provide the representative with the serial number of your K1000 appliance. To view the serial number, click **About** in the lower left of the Administrator Console.
- Obtain the public tether key for your appliance.

1. Go to the appliance *Control Panel*:
 - If the Organization component is not enabled on the appliance, log in to the K1000 Administrator Console, `http://K1000_hostname/admin`, then click **Settings**.
 - If the Organization component is enabled on the appliance, log in to the K1000 System Administration Console, `http://K1000_hostname/system`, or select **System** in the drop-down list in the top-right corner of the page, then click **Settings**.
2. **Optional:** If you believe that the private key previously generated for tethering has been compromised, you can regenerate it:



NOTE: Whenever you generate the private key, you must obtain a new public key from Quest Support.

- a. Click **Security Settings** on the appliance *Control Panel* to display the *Security Settings* page.
 - b. In the *Appliance Encryption Key* section, click **Generate Key**.
3. Enable the tether and enter the public key you obtained from Quest Support:

- a. On the left navigation bar, click **Support** to display the *Support* page.
 - b. In the *Troubleshooting Tools* section, click **Enter a Tether Key** to display the *Diagnostic Utilities* page.
 - c. In the *Quest Support Tether* section, select **Enable Tether**.
 - d. In the *Key* field, enter the public tether key. To obtain the public tether key, contact Quest Support at <https://support.quest.com/contact-support>.
4. **Optional:** Enable the Quest Support User account:
 - a. In the *Quest Support Tether* section of the *Diagnostic Utilities* page, select **Enable Quest Support User**.
 - b. Specify the password you want Quest Support to use to log in to the K1000, then provide this password to Quest Support. The password is not delivered to Quest automatically.
 - c. **Optional:** Select **Allow Quest to set password** to enable Quest Support to create a password for the user account. This makes it possible for a Quest representative to create a password they can use to log in to the appliance. This option is not available if you are using the encryption method available prior to K1000 version 6.2.
5. Click **Save**.

Troubleshooting appliance issues

The K1000 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 K1000 appliance logs in the Administrator Console. Appliance logs provide information related to K1000 processes and errors the system encounters.

If the appliance is configured to share detailed usage data with Quest KACE, K1000 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 K1000 Administrator Console, `http://K1000_hostname/admin`, then click **Settings**.
 - If the Organization component is enabled on the appliance, log in to the K1000 System Administration Console, `http://K1000_hostname/system`, or select **System** in the drop-down list in the top-right corner of the page, then click **Settings**.
 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).

Log Type	Log Name	Description
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.
	System Performance	System performance information, including webserver, disk, and Agent connection statistics. To ensure that Apache graphs in this log are updated, enable webserver diagnostics. See Configure security settings for the appliance .
	Konductor Log	Konductor-related logs. Konductor is an internal K1000 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 <i>Tasks in Progress</i> widget. In addition, task throughput information appears on the appliance <i>General Settings</i> page (on appliances with the Organization component enabled) or on the <i>Communication Settings</i> page (on appliances without the Organization component enabled). See: • Configure appliance General Settings with the

Log Type	Log Name	Description
		Organization component enabled • Configure Agent communication and log settings
	Patch Download Log	Information about patches that have been downloaded to the appliance.
	Opcode Cache	Opcode cache log information (not available for virtual appliances).
	Backup Log	Details of daily and monthly K1000 appliance backups.
	Agentless Log	Information related to Agentless device connections to the K1000.
	Monitoring Log	Information related to monitored servers and their connections to the K1000.
	Software Inventory	Information related to K1000 Software Catalog inventory processing.
	Software Inventory Errors	Processing errors related to K1000 Software Catalog inventory processing.
	Account Management Service	Information related to the Account Management Service, which is a service that manages user account information and authentication for the K1000.
	Account Management Service Errors	Errors related to the Account Management Service, which is a service that manages user account information and authentication for the K1000.
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.

Log Type	Log Name	Description
	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.
Device	Client Errors	K1000 Agent exception logs.
	AMP Server	Server-related AMP (Agent Messaging Protocol) errors.
	AMP Queue	Queue-related AMP 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.

- Go to the appliance *Control Panel*:
 - If the Organization component is not enabled on the appliance, log in to the K1000 Administrator Console, `http://K1000_hostname/admin`, then click **Settings**.
 - If the Organization component is enabled on the appliance, log in to the K1000 System Administration Console, `http://K1000_hostname/system`, or select **System** in the drop-down list in the top-right corner of the page, then click **Settings**.
- On the left navigation bar, click **Support** to display the *Support* page.
- 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 K1000 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 [Security run output](#).

Troubleshooting and debugging the K1000 Agent

Use the Agent's debugging features to troubleshoot Agent-related issues.

If devices do not show up in Inventory:

- For Windows devices, see [Enabling debugging on Windows devices](#).
- For Linux (Red Hat) devices, see [Enable debugging on Linux devices](#).
- For Mac OS X devices, see [Enable debugging on Mac OS X devices](#).

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 K1000 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
```

Enabling debugging on Windows devices

You can enable debugging on Windows devices by adding `debug=true` to AMPTools.

Enable Windows debugging by editing the amp.conf file

You can enable Windows debugging on Windows devices by editing the amp.conf file.

On Windows Vista and Windows 7 devices, you must have Run as administrator privileges.

1. Open a command prompt.
2. Stop the Agent: In the command prompt, type:

```
net stop ampagent
```
3. Open the `amp.conf` file, which is located in the following directories:
On Windows Vista and Windows 7: `C:\ProgramData\Dell\KACE`
4. Add the following line:

```
debug=true
```
5. Start the Agent: In the command prompt, type:

```
net start ampagent
```

The output is recorded in various K1000 Agent logs. See [View appliance logs](#).

Enable Windows debugging from the command line

You can enable debugging on Windows devices from the command line.

On Windows Vista and Windows 7 devices, you must have Run as administrator privileges.

1. Open a command prompt.
2. In the command prompt, type one of the following:
 - On 32-bit devices: `"%ProgramFiles%\Dell\KACE\AMPTools.exe" debug=true`
 - On 64-bit devices: `"%ProgramFiles(x86)%\Dell\KACE\AMPTools.exe" debug=true`

The output is recorded in various K1000 Agent logs. See [View appliance logs](#).

Enable debugging on Linux devices

You can enable debugging on Linux devices by adding `debug=true` to AMPTools.

1. Open a terminal window from **Applications > System Tools**.
2. In the terminal window, type:

```
/opt/dell/kace/bin/AMPTools debug=true
```

The output is recorded in various K1000 Agent Logs. See [View appliance logs](#).

Enable debugging on Mac OS X devices

You can enable debugging on Mac OS X devices by adding `debug=true` to AMPTools.

1. Open a terminal window from **Applications > Utilities**.
2. Go to the following folder:

```
cd Library/Application Support/Dell/KACE/bin
```
3. In the terminal window, type:

```
sudo ./AMPTools debug=true
```

The output is recorded in various K1000 Agent logs. See [View appliance logs](#).

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 K1000 Management 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 K1000 Administrator Console, http://K1000_hostname/admin, then click **Settings**.
 - If the Organization component is enabled on the appliance, log in to the K1000 System Administration Console, http://K1000_hostname/system, or select **System** in the drop-down list in the top-right corner of the page, then click **Settings**.
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 K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in 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**.
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 K1000 Management 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 K1000 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 K1000 Administrator Console, http://K1000_hostname/admin, then click **Settings**.
 - If the Organization component is enabled on the appliance, log in to the K1000 System Administration Console, http://K1000_hostname/system, or select **System** in the drop-down list in the top-right corner of the page, then click **Settings**.
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:

- `khelptdeskmailhandler_output`
- `khelptdeskmailnotifier_error`
- `khelptdeskmailnotifier_output`

8. Examine the Microsoft Exchange SMTP service logs in `C:\windows\system32\oologFiles\*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 Two-Factor Authentication

Two-Factor Authentication (also known as 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 K1000 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 *Support 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 K1000 System Console. On the left navigation bar, under *Settings*, click **Support**, and on the *Support* page, under *Troubleshooting Tools*, click **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 K1000 machine. You may be required to provide this information to Support, when needed.

After upgrading from an earlier version, a message appears indicating that Two-Factor Authentication is disabled. Follow the instructions in the message to enable Two-Factor Authentication.

- To replace the secret key and regenerate the offline tokens, click **Replace Secret Key**.
- To regenerate offline tokens, click **Regenerate Offline Tokens**.

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 K1000 appliance:

- [Organization-level \(ORG1\) database tables](#)
- [System-level \(KBSYS\) database tables](#)
- [Changes to the ORG1 database](#)
- [Changes to the KBSYS database](#)

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 30. 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	Assets
ASSET_ASSOCIATION	Assets
ASSET_CATALOG_ASSOCIATION	Assets
ASSET_CLASS	Assets: Asset Subtypes
ASSET_DATA_1	Assets: Import Assets
ASSET_DATA_2	Assets: Import Assets
ASSET_DATA_3	Assets: Import Assets
ASSET_DATA_4	Assets: Import Assets
ASSET_DATA_5	Assets: Import Assets

Table	Component
ASSET_DATA_6	Assets: Import Assets
ASSET_DATA_7	Assets: Import Assets
ASSET_FIELD_DEFINITION	Settings: Asset History
ASSET_FILTER	Assets: Labeling
ASSET_HIERARCHY	Assets
ASSET_HISTORY	Settings: Asset History
ASSET_TYPE	Assets: Asset Types
AUTHENTICATION	Appliance Administration
CLIENTDIST_LABEL_JT	Appliance Administration: K1000 Agent
CLIENT_DISTRIBUTION	Appliance Administration: K1000 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

Table	Component
DELL_PKG_UPDATE_HISTORY	Security: Dell Updates
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
DEVP_PROFILE_APPLIED	Scripting: Mac Profiles
DEVP_PROFILE_APPLIED_MACHINE	Scripting: Mac Profiles
DEVP_PROFILE_APPLIED_PAYLOAD	Scripting: Mac Profiles
DEVP_PROFILE_APPLIED_PAYLOAD_ATTRIBUTE	Scripting: Mac Profiles
DIB_APPROVAL	Settings: Quest Identity Broker
DIB_USER	Settings: Quest Identity Broker
FILTER	Labels
FS	File Synchronization
FS_LABEL_JT	File Synchronization
FS_MACHINE_JT	File Synchronization
GLOBAL_OPTIONS	Appliance Administration
GRID_COLUMNS_OVERRIDES	Appliance Administration

Table	Component
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
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

Table	Component
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
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

Table	Component
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
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

Table	Component
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
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

Table	Component
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
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

Table	Component
OVAL_STATUS	Security: OVAL
PATCHLINK_BULLETIN_COUNT	Security: Patch Management
PATCHLINK_BULLETIN_MACHINE_STATUS	Security: Patch Management
PATCHLINK_MACHINE_APPLICABLE_PACKAGE	Security: Patch Management
PATCHLINK_MACHINE_STATUS	Security: Patch Management
PATCHLINK_PATCH_COUNT	Security: Patch Management
PATCHLINK_PATCH_LABEL_JT	Security: Patch Management
PATCHLINK_PATCH_STATUS	Security: Patch Management
PATCHLINK_SCHEDULE	Security: Patch Scheduling
PATCHLINK_SCHEDULE_DEPLOY_LABEL_JT	Security: Patch Scheduling
PATCHLINK_SCHEDULE_DETECT_LABEL_JT	Security: Patch Scheduling
PATCHLINK_SCHEDULE_LABEL_JT	Security: Patch Scheduling
PATCHLINK_SCHEDULE_MACHINE_STATUS	Security: Patch Scheduling
PATCHLINK_SCHEDULE_OS_JT	Security: Patch Scheduling
PATCHLINK_SCHEDULE_ROLLBACK_LABEL_JT	Security: Patch Scheduling
PATCHLINK_SCHEDULE_RUN	Security: Patch Scheduling
PATCHLINK_SCHEDULE_RUN_COUNTS	Security: Patch Scheduling
PATCHLINK_SCHEDULE_RUN_LOG	Security: Patch Scheduling
PATCHLINK_SCHEDULE_RUN_MACHINE	Security: Patch Scheduling
PATCH_FILTER	Security: Patch Management
PATCH_SETTINGS	Security: Patch Scheduling
PORTAL	Service Desk: User Console
PORTAL_LABEL_JT	Service Desk: User Console
PROCESS	Inventory: Processes

Table	Component
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
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	Inventory: License Compliance
SAM_COMPLIANCE_SUMMARY	Inventory: License Compliance

Table	Component
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
SCAP_BENCHMARK	Security: SCAP
SCAP_GROUP	Security: SCAP
SCAP_PROFILE	Security: SCAP
SCAP_RESULT	Security: SCAP
SCAP_RESULT_RULE	Security: SCAP
SCAP_RESULT_SCORE	Security: SCAP
SCAP_RULE	Security: SCAP
SCAP_RULE_IDENT	Security: SCAP
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

Table	Component
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 31. 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

Table	Component
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
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

Table	Component
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
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

Table	Component
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
OVAL_DEFINITION	Security: OVAL
OVAL_UPDATE_STATUS	Security: OVAL
PATCHLINK_ARCHITECTURE	Security: Patch Management
PATCHLINK_BULLETIN	Security: Patch Management
PATCHLINK_BULLETIN_CATALOG	Security: Patch Management
PATCHLINK_BULLETIN_OS_JT	Security: Patch Management
PATCHLINK_BULLETIN_UPDATE_STATUS	Security: Patch Management
PATCHLINK_ERROR_CODE	Security: Patch Management
PATCHLINK_IMPACT	Security: Patch Management
PATCHLINK_LANGUAGE	Security: Patch Management
PATCHLINK_LST	Security: Patch Management
PATCHLINK_LST_OSPX_MAP	Security: Patch Management
PATCHLINK_LST_PATCH_JT	Security: Patch Management
PATCHLINK_OS_TYPE	Security: Patch Management
PATCHLINK_PACKAGE	Security: Patch Management
PATCHLINK_PACKAGE_FILE	Security: Patch Management

Table	Component
PATCHLINK_PACKAGE_FLAGS	Security: Patch Management
PATCHLINK_PACKAGE_LANGUAGE_JT	Security: Patch Management
PATCHLINK_PACKAGE_OS_TYPE_JT	Security: Patch Management
PATCHLINK_PATCH	Security: Patch Management
PATCHLINK_PATCH_LANGUAGE_JT	Security: Patch Management
PATCHLINK_PATCH_OS_JT	Security: Patch Management
PATCHLINK_PATCH_PREREQ	Security: Patch Management
PATCHLINK_PATCH_PRODUCT	Security: Patch Management
PATCHLINK_PATCH_SUPERCEDES	Security: Patch Management
PATCHLINK_PLATFORM	Security: Patch Management
PATCHLINK_PUBLISHERS	Security: Patch Management
PATCHLINK_RESOURCE	Security: Patch Management
PATCHLINK_SCR_CONTENT	Security: Patch Management
PATCHLINK_UPDATE_STATUS	Security: Patch Management
PATCHLINK_VENDORATTRIBUTE	Security: Patch Management
PATCHLINK_VENDOR_SEVERITY	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

Table	Component
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
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

Table	Component
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
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

Changes to the ORG1 database

The following table shows the table names that have changed in the organization-level (ORG1) database between the 6.3 and 6.4 versions of the K1000 appliance.

Table 32. ORG1 database table changes between versions 6.3 and 6.4

Table	Change description
ASSET_CLASS	Added
AUTH_CREDENTIALS	Removed
AUTH_GOOGLE_API	Removed

Table	Change description
AUTH_NT_USER	Removed
AUTH_SNMP_V3	Removed
AUTH_USER_PWD	Removed
CREDENTIAL	Added
DEVICE_DETAIL_FIELD	Added
DEVICE_DETAIL_GROUP	Added
DEVICE_DETAIL_GROUP_ASSET_CLASS_JT	Added
DEVICE_DETAIL_SECTION	Added
DEVICE_DETAIL_SECTION_ASSET_CLASS_JT	Added
DEVP_PROFILE_APPLIED	Added
DEVP_PROFILE_APPLIED_MACHINE	Added
DEVP_PROFILE_APPLIED_PAYLOAD	Added
DEVP_PROFILE_APPLIED_PAYLOAD_ATTRIBUTE	Added
HD_ANNOUNCEMENT	Added
HD_ANNOUNCEMENT_LABEL_JT	Added
HD_HOME_PAGE_WIDGET	Added
HD_LINK	Added
KMON_INSTALL_LEP_DEVICE_JT	Added
KMON_LEP	Added
KMON_LEP_INSTALL	Added
MACHINE_BITLOCKER_VOLUME	Added
MACHINE_DCM_AMT_SETTINGS	Added
MACHINE_DCM_BATTERY	Added
MACHINE_DCM_DESKTOP_MONITOR	Added

Table	Change description
MACHINE_DCM_FLAT_PANEL	Added
MACHINE_DCM_LOG_ENTRY	Added
MACHINE_DCM_PHYSICAL_MEMORY	Added
MACHINE_DCM_PROCESSOR	Added
MACHINE_DCM_VPRO_SETTINGS	Added
MACHINE_DDPE	Added
MACHINE_DDPE_VOLUME	Added
MACHINE_DRIVE_ENCRYPTION_SUMMARY	Added
MACHINE_FILEVAULT_VOLUME	Added
MACHINE_LOCATION	Added
MACHINE_MOBILE	Added
MACHINE_TPM	Added
MSP_MI_TEMPLATE	Removed
REMOTE_DMM_HOST	Added
REPORT	Removed
SAM_COMPLIANCE_DETAIL	Added
SAM_COMPLIANCE_SUMMARY	Added
SAM_COMPLIANCE_DETAIL	Added
SAM_COMPLIANCE_SUMMARY	Added
SAM_VIEW_ALL_SOFTWARE	Removed
SAM_VIEW_DISCOVERED_APPLICATIONS	Removed
SAM_VIEW_DISCOVERED_SOFTWARE	Removed
SAM_VIEW_DISCOVERED_SUITES	Removed
SAM_VIEW_INVENTORY_ADD_REMOVE_PROGRAMS	Removed

Table	Change description
SAM_VIEW_INVENTORY_MOBILE_APPS	Removed
SAM_VIEW_MACHINE_DISCOVERED_SOFTWARE	Removed
SAM_VIEW_TITLED_SOFTWARE	Removed

Changes to the KBSYS database

The following table shows the table names that have changed in the System-level (KBSYS) database between the 6.3 and 6.4 versions of the K1000 appliance.

Table 33. KBSYS database table changes between versions 6.3 and 6.4

Table	Change description
AGENTLESS_TASK_LOG	Removed
CREDENTIAL_CONSUMER	Added
DAC_AGENTLESS	Removed
HD_EMAIL_EXCLUSION	Added
JOIN_METADATA	Added
REPORT	Removed
PATCH_SETTINGS	Removed
SAM_ADD_REMOVE_PROGRAM	
SAM_APPLICATION_FILE	Removed
SAM_HARDWARE	Added
SAM_MOBILE_APPLICATION_FILE	
SAM_SOFTWARE_TAG	Added
SHAPING_METADATA	Added

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 34. 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 "{message}" and timeout "{timeout}" seconds.	X	X	X	X	X
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		X	X		

Step	Description	V	OS	R	ORS	ORF
	Specifying Windows registry paths.					
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}". i NOTE: This step requires you to choose from a list of application packages already uploaded using the functionality in the <i>Inventory</i> > <i>Software</i> page. See Adding and deleting applications in Software page inventory.		X	X		
Kill a process	Kill 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 a registry value	Log "%{key}!\n%{name}":			X		
Log file information	Log "%{attrib}" from "%{path}\n%{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}!\n%{name}" to "%{newValue}":	X	X			

Step	Description	V	OS	R	ORS	ORF
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
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	X				

Step	Description	V	OS	R	ORS	ORF
	greater than "%{expectedValue}".					
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				

Step	Description	V	OS	R	ORS	ORF
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				
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				

Step	Description	V	OS	R	ORS	ORF
i	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			

Step	Description	V	OS	R	ORS	ORF
Verify a registry key's value count is exactly	Verify that "%{key}" has exactly "%{expectedValue}" values.	X				
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	Verify that "%{key}! %{name}"	X				

Step	Description	V	OS	R	ORS	ORF
does not exist	does not exist.					
Verify a registry value exists	Verify that "%{key}!\n%{name}" exists.	X				
Verify a registry value is exactly	Verify that "%{key}!\n%{name}" is equal to "%{expectedValue}".	X				
Verify a registry value is greater than	Verify that "%{key}!\n%{name}" is greater than "%{expectedValue}".	X				
Verify a registry value is greater than or equal to	Verify that "%{key}!\n%{name}" is greater than or equal to "%{expectedValue}" .	X				
Verify a registry value is less than	Verify that "%{key}!\n%{name}" is less than "%{expectedValue}".	X				
Verify a registry value is less than or equal to	Verify that "%{key}!\n%{name}" is less than or equal to "%{expectedValue}".	X				
Verify a registry value is not	Verify that "%{key}!\n%{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 35. 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
Kill a process	Kill 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				

Step	Description	V	OS	R	ORS	ORF
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				
Verify an environment variable equals		X				
Verify an environment variable exists		X				
Verify an environment variable greater than		X				

Step	Description	V	OS	R	ORS	ORF
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 36. Adding steps to scripts for RHEL

Step	Description	V	OS	R	ORS	ORF
Always fail		X		X		
Kill a process	Kill 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				

Step	Description	V	OS	R	ORS	ORF
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				
Verify file info less than		X				

LDAP variables

The K1000 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 K1000 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 37. Device or machine variables and mappings

K1000 variable	K1000 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_USERNAME	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 K1000 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 38. User variables and mappings

K1000 variable	K1000 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

K1000 variable	K1000 USER database table column	LDAP attribute mapping
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 in the K1000 6.4 release.
KBOX_LOCALE_BROWSER_ID	LOCALE_BROWSER_ID	
KBOX_HD_DEFAULT_QUEUE_ID	HD_DEFAULT_QUEUE_ID	
KBOX_LDAP_UID	LDAP_UID	objectGUID

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 K1000 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 K1000 appliance. To access the Administrator Console, go to `http://<K1000_hostname>/admin` where `<K1000_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://<K1000_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://<K1000_hostname>/admin`.

Agent

The K1000 Agent is an application that can be installed on devices to enable device management through the K1000 appliance. Agents that are installed on managed devices communicate with the K1000 appliance through AMP (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 K1000 Agent](#).

Agentless management

Agentless device management is a method of managing devices without the need to deploy and maintain the K1000 Agent software on those devices. Agentless management uses SSH, Telnet, SNMP, and other methods to connect to Agent-intolerant devices, such as printers, network devices, and storage devices, and report inventory in the K1000 Administrator Console. This is useful for operating system versions and distributions that are not supported by the K1000 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 K1000 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 K1000 to alert staff about errors and issues being reported in the event and system logs of the devices. See [Monitoring servers](#).

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](#).

AMP

Agent Messaging Protocol.

AMP (Agent Messaging Protocol) is the communications protocol used for communication between the K1000 Agent, which is installed on Agent-managed devices, and the K1000 appliance. AMP provides optimized real-time communications for system-management operations. See [Provisioning the K1000 Agent](#).

AppDeploy Live

See [ITNinja](#) .

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 K1000 is available as a physical or hardware-based appliance, and as a virtual appliance. The virtual appliance (VK1000) uses a VMware infrastructure. The same system management features are available on both the physical and virtual appliances. See [About K1000 components](#).

Application Control

Application Control enables you to mark applications as Not Allowed and blacklist 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 K1000 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 K1000 inventory. See [About Asset Subtypes, custom fields, and device detail preferences](#).

Assets that count toward your K1000 license limit

Your K1000 license agreement entitles you to manage a specified number of devices that are categorized as Assets, and these Assets differ from assets used in the Asset Management component. Assets that count toward your license limit include devices that 1) have been added to the K1000 inventory but do not meet the definition of Managed Computers or Monitored Servers 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 K1000 license 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

blacklisting

See [Application Control](#) .

benchmark

A SCAP benchmark is a security configuration checklist that contains a series of rules for evaluating the vulnerabilities of a device in a particular operational environment. The NIST (National Institute of Standards and Technology) maintains the National Checklist Repository that contains a variety of security configuration checklists for specific IT products and categories of IT products. See [About benchmarks](#).

C

Cataloged applications

Cataloged applications are executables that are in the official Software Catalog database. This includes both applications that appear in the K1000 inventory (Discovered applications) and applications that do not appear in K1000 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 K1000 appliance.



NOTE: Notifications and daily reports come from the default address, Charlie Root, (root@<K1000_hostname>) and you cannot modify this address.

Classic Metering

Classic Metering is the metering system that was available on the K1000 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 K1000 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 K1000 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 K1000 Client Drop location](#).

clients

See [devices](#) .

Command Line Console

The Command Line Console is a terminal window interface to the K1000 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 K1000. Examples of Computers include personal computers, servers, laptops, tablets, and smart phones. Your K1000 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 K1000, 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 K1000 uses the WMI (Windows Management Instrumentation) interface to collect detailed hardware inventory and health status. See [About Dell Command | Monitor](#).

Quest Identity Broker

Quest Identity Broker (QIB) is a cloud-based single sign on (SSO) solution that enables users to request access to the K1000 Administrator Console or User Console using identity providers, such as your organization's Identity Provider. QIB can be configured to automatically approve user requests and create K1000 accounts that enable authenticated users to log in to the K1000 User Console or to require administrator approval before user accounts are created and access to either the Administrator Console or User Console is granted. See [About Quest Identity Broker](#).

Dell Mobility Management

Dell Mobility Management (DMM) enables users to manage and provision access to smartphones and tablets from any device with a browser and internet connection. It also manages applications and content on the devices. DMM integration in the K1000 enables administrators to configure a discovery schedule that reaches out to a DMM system and discovers managed mobile devices. In addition, an administrator can choose to provision managed mobile devices into K1000 inventory and asset management. See [Add a Discovery Schedule for a Dell Mobility Management \(DMM\) device](#).

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 K1000. Your K1000 license agreement entitles you to manage a specified number of devices, which are classified as Managed Computers, Assets, and Monitored Servers. Managed devices report data, such as software, hardware, and networking information, to the K1000. See [View K1000 license information](#).

Discovered applications

Discovered applications are executables in the K1000 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 K1000 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](#).

DMM

See [Dell Mobility 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 Synchronizations](#).

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 K1000 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 K1000 Agent](#).

IP Scans

See [Discovery](#) .

ITNinja

Sponsored by Quest KACE, ITNinja.com (formerly AppDeploy.com) is a product-agnostic IT-focused community website. It is the Internet's leading destination for IT professionals to share information and ask questions about system management related topics. The website provides a question and answer section and a blogging platform. If you choose to share anonymous usage data with ITNinja, the ITNinja feed appears on pages such as the software, Managed Installation, and File Synchronization detail pages in the Administrator Console. The feed is not available on *Software Catalog* detail page. See [Enable the ITNinja feed](#).

Quest publishes a base set of Windows Reliability and Performance Monitor (PerfMon) templates and non-Windows open-source Perl scripts on ITNinja, so that users can extend their server monitoring capability and identify system and application performance issues. These unmanaged templates and scripts are available for download so that users do not have to create them from scratch.

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](#).

K1000 series appliances

The K1000 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 K1000 series, go to the Quest website, <https://quest.com/products/kace-k1000-systems-management-appliance/>.

K2000 series appliances

The K2000 series includes system deployment appliances designed to fully automate the deployment of operating systems (OS). For more information about the K2000 series, go to the Quest website, <https://quest.com/products/kace-k1000-systems-management-appliance/>.

Knowledge Base

Quest has a Knowledge Base of articles about the K1000, 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 K1000 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 K1000 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 K1000 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 K1000 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](#) .

Mac profiles

Mac profiles are files that are used to configure user-level and system-level policies on Mac devices. You can use the K1000 appliance to distribute Mac profiles to Agent-managed devices running Mac OS X. See [Managing Mac profiles](#).

Managed Computers

Your K1000 license agreement entitles you to manage a specified number of devices that are categorized as Managed Computers. Managed Computers are devices in K1000 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 K1000 license information](#).

Managed Installations

Managed Installations (MI) are the primary mechanism for deploying or removing applications from K1000 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 K1000. In this way, the K1000 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 K1000 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 Servers

Your K1000 license agreement entitles you to manage a specified number of devices that are categorized as Monitored Servers. Monitored Servers are servers that 1) meet the requirements for Managed Computers and 2) have Monitoring enabled. You can monitor 5 servers with your K1000 license. If you want to be able to monitor up to 200 servers, you must obtain a license for the Monitoring Module. See [View K1000 license 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 [Add MSI Installer scripts](#).

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 or blacklisted 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 K1000 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 K1000 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

A K1000 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 a K1000 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](#).

OVAL

OVAL (Open Vulnerability and Assessment Language) is an internationally recognized standard for detecting security vulnerabilities and configuration issues on Windows devices. OVAL security checks determine assets that are out of compliance and let you customize security policies to enforce rules, schedule tests to run automatically, and run reports based on the results.

OVAL is compatible with the Common Vulnerabilities and Exposures (CVE) list. CVE content is determined by the CVE Editorial Board, which is composed of experts from the international information security community. New information about security vulnerabilities discussed on the Community Forum is sent to the CVE Initiative for possible addition to the list. For more information about CVE, MITRE Corporation, or the OVAL Board, go to <http://cve.mitre.org>.

The ability to describe vulnerabilities and exposures in a common language makes it easier to share security data with other CVE-compatible databases and tools.

See [Understanding OVAL tests and definitions](#).

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 K1000 Agent on devices you want to manage using Agent software. See [Managing provisioning schedules](#).

provisioning

The process of installing the K1000 Agent on managed devices. See [Provisioning the K1000 Agent](#).

Q

QIB

See [Quest Identity Broker](#) .

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 a K1000 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 K1000 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 K1000 appliance. See [Enable file sharing at the System level](#).

SCAP

SCAP (Secure Content Automation Protocol), is a set of open standards that enumerate software flaws, monitor security-related configurations and product names, and examine systems to determine the presence of vulnerabilities and rank (score) the impact of the discovered security issues on Windows devices. SCAP is maintained by the National Institute of Standards and Technology (NIST), and its use is mandated by government agencies such as the US OMB (United States Office of Management and Budget).

SCAP uses the US government's National Vulnerability Database (NVD), which is a standards-based vulnerability management data repository. NVD includes databases of security checklists, security-related software flaws, misconfigurations, product names, and impact metrics. For more information on SCAP and NVD, go to the NIST websites at <http://scap.nist.gov/index.html> and <http://nvd.nist.gov/>.

See [About SCAP](#).

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 K1000 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 K1000 User Console. The Service Desk enables end users to submit trouble tickets through email or through the User Console, http://<K1000_hostname>/user, where <K1000_hostname> is the hostname of your appliance. Your help desk team manages these tickets through email, the Administrator Console, http://<K1000_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 K1000 Administrator Console and User Console without having to re-enter their credentials on the K1000 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 Support](#).

task throughput

The task load on the K1000 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 K1000 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 K1000 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://<K1000_hostname>/user` where `<K1000_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](#) .

Vulnerability Testing

Vulnerability testing is the process of scanning, and establishing schedules to scan, Windows devices for known vulnerabilities using the Open Vulnerability Assessment Language (OVAL) battery of tests. Vulnerability testing is a useful complement to patching and other forms of security hardening to verify whether those measures are addressing known issues. See [About OVAL security checks](#).

W

Wake-on-LAN

Wake-on-LAN enables you to power-on devices remotely from the K1000 appliance regardless of whether the devices have the K1000 Agent installed. See [Using Wake-on-LAN](#).

We are more than just a name

We are on a quest to make your information technology work harder for you. That is why we build community-driven software solutions that help you spend less time on IT administration and more time on business innovation. We help you modernize your data center, get you to the cloud quicker and provide the expertise, security and accessibility you need to grow your data-driven business. Combined with Quest's invitation to the global community to be a part of its innovation, and our firm commitment to ensuring customer satisfaction, we continue to deliver solutions that have a real impact on our customers today and leave a legacy we are proud of. We are challenging the status quo by transforming into a new software company. And as your partner, we work tirelessly to make sure your information technology is designed for you and by you. This is our mission, and we are in this together. Welcome to a new Quest. You are invited to Join the Innovation.

Our brand, our vision. Together.

Our logo reflects our story: innovation, community and support. An important part of this story begins with the letter Q. It is a perfect circle, representing our commitment to technological precision and strength. The space in the Q itself symbolizes our need to add the missing piece — you — to the community, to the new Quest.

Contacting Quest

For sales or other inquiries, visit www.quest.com/company/contact-us.aspx or call 1-949-754-8000.

Technical support resources

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

Copyright 2017 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

Trademarks

Quest, KACE, and the Quest logo are trademarks and registered trademarks of Quest Software Inc. in the U.S.A. and other countries. For a complete list of Quest Software trademarks, please visit our website at www.quest.com/legal. All other trademarks, servicemarks, registered trademarks, and registered servicemarks are the property of their respective owners.

Legend



CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.



WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.



IMPORTANT, NOTE, TIP, MOBILE, or VIDEO: An information icon indicates supporting information.

KACE Systems Management Appliance (K1000) Administrator Guide

Updated - February 2017

Software Version - 7.1

A

- Acceptable Use Policy 103
- action buttons on User Console 694
- Active Directory
 - settings for Mac OS X 530
 - single sign on access with 164
 - single sign on configuration 91, 162
- adding
 - announcements to User Console 696
 - applications to Software page inventory 395, 473
 - applications to the Software Catalog 415
 - Asset Types 184, 203
 - Custom Views 51
 - devices to inventory manually 375
 - File Synchronizations 491
 - LDAP Labels 134
 - License assets for Software Catalog inventory 208, 419
 - License assets for Software page inventory 212
 - Locations 202
 - Managed Installations 473
 - manual labels 118
 - notification schedules 639
 - scripts 501
 - Service Desk ticket queues 746
 - Smart Labels 120
 - Software assets in Assets section 397
 - Software assets in Inventory section 397
- Admin level 28
 - Dashboard 37
 - General Settings 60
- administration
 - backing up data 778
 - Daily Run Output 796
 - email notifications for administrators 142
 - logs, downloading 795
 - logs, viewing 792
 - restarting the appliance 787
 - restoring appliance settings 782
 - restoring factory settings 785
 - restoring most recent backup 782
 - troubleshooting 792
 - updating appliance software 785
 - updating OVAL definitions 787
 - updating the license key 787
- Administrator Console 28, 28
 - about 26
 - components
 - with the Organization component 33
 - without the Organization component 31
 - locale settings for 66, 70
- Advanced Search
 - and Custom Views 51
 - and Smart Labels 51
 - for organizations 258
 - for Software page inventory 400
- Agent
 - about 26, 338
 - add Windows registry key for access to DDP|E information 330
 - AMP 353
 - communication settings for 349
 - configuration 95
 - deploying manually 357
 - enabling file sharing for 339
 - enabling organization-level file sharing for 340, 341
 - features available to managed devices 288
 - GPO Provisioning Tool for Windows 341
 - history 338
 - installing on multiple devices 344
 - log settings for 349
 - messages, deleting 354
 - messages, viewing 353
 - methods for provisioning 338
 - obtaining installation files 357
 - preparing to install with onboard provisioning 343
 - provisioning 339, 340, 341, 341
 - provisioning results 348
 - provisioning schedules
 - deleting 347
 - duplicating 346
 - editing 346
 - running 346
 - viewing 346
 - provisioning using Discovery results 286
 - starting and stopping on Linux 360
 - starting and stopping on Mac OS X 363
 - system requirements for installation 343
 - task status 352
 - updates 354, 354
 - configuring automatic 354
 - uploading manually 356
- Agent debugging 796
 - on Linux 797
 - on Mac OS X 797
 - on Windows 796
 - amp.conf file 796
 - command line 797
- Agent deploy
 - Linux devices 359
 - startup/login 360
 - updating 360
 - verifying the version 361

- viewing the version on Linux 361
- Linux devices, removing 361
- Mac OS X devices
 - deploy/upgrade 361
 - remove 363
 - using shell scripts 362
 - using terminal window 362
 - verify 363
 - verifying the version 363
- Windows devices 357
- Agent Messaging Protocol 95
- Agent Provisioning Assistant
 - provision Windows devices with GPO Provisioning Tool 342
 - using to deploy Agent on devices 344
- Agentless management 364
 - add Windows registry key for access to DDP|E information 333
 - delete device details 372
 - device details 372
 - enable manually 366
 - enable using Discovery information 365
 - features available to managed devices 288
 - supported operating systems 364
- AirWatch
 - Discovery Schedule for device 283
- alerts 495
 - AMP connection required for 495
 - automatic deletion of 661
 - automatic dismissal of 661
 - creating for broadcast 496
 - creating Service Desk tickets from 669, 712
 - deleting 677
 - dismissing 676
 - filter unwanted 672, 673, 673, 674
 - for device configuration changes 662
 - retrieve dismissed 677
 - searching for 672
 - stopping for maintenance 662
 - summary of 43
- alternate download locations
 - about 472
 - distributing packages from 472
 - for scripts 499
- AMP
 - about 95
 - connections required for patching 582
- Android 104
- announcements
 - adding and editing on User Console home page 696
 - prioritizing on User Console home page 698
- Apache
 - graphs 792
 - log paths 653
 - webserver diagnostic graphs 85
- API
 - access to the appliance 85
 - enabling for manual inventory 380
- AppDeploy Live (see ITNinja) 402
- Apple iOS 104
- appliance backups 781, 781
 - about 778
 - daily backup schedule 779
 - deleting 781
 - downloading files 780
 - FTP access to 780
 - manual 780
 - status of 790
- appliance linking
 - disabling 111
 - enabling 109
 - enabling access to Federation API settings 110
- appliance network interface status 789
- appliance resources
 - about importing and exporting 259
 - exporting from appliance 260
 - exporting from organizations 261
 - importing to appliances 260
 - importing to organizations 262
- appliance settings
 - advertised updates 785
 - general 60
 - license key updates 787
 - manual updates 786
 - restore to factory settings 785
 - restoring 782
 - restoring from backup 782, 784
 - security 85
 - uploading backup files 783
 - verify updates 786
- appliance up-time and load averages 789
- appliance version 45
- application classifications 405
- Application Control
 - applying labels for 435
 - editions sharing executables 435
 - limitations of 435
 - marking as Not Allowed 436
 - messages that appear 435
 - removing designation 438
 - reporting on 437
 - requirements 434
 - using 434
 - viewing Not Allowed applications 436
- Application Layer Firewall, settings for Mac OS X 621
- application patches, viewing 571
- applications
 - cataloged 405
 - finding using Advanced Search 400
 - Locally Cataloged 405
 - Not Allowed 406
 - viewing Discovered 409
 - viewing Locally Cataloged applications 411
 - viewing Not Discovered 409
 - viewing Uncataloged applications 410
- approval requests for QIB 166
- APPROVAL_INFO field 773
- approvals, requiring for tickets 773
- approving tickets by email 774

- archival
 - deleting tickets from 744
 - enabling for tickets 742
 - restoring tickets from 744
 - ticket queue settings for 743
- Asset Management
 - about 179, 190
 - adding and deleting asset fields 184
 - adding barcodes 182
 - adding Software assets 397
 - asset administrator role 201
 - Asset Subtypes 190, 190
 - adding 191
 - deleting 196
 - editing 194
 - setting as default 194
 - Asset Types
 - about 184
 - adding 184, 203
 - adding custom fields for devices 187
 - adding fields for locations 188
 - customizing 184, 203
 - deleting 189
 - parent relationships for locations 189
 - renaming 184
 - assigning assets to subtypes 195, 195
 - classic metering 423
 - comparing assets to inventory 180
 - data format 216
 - device assets
 - archiving 200
 - identifying assets to track 181
 - importing license data 216
 - about 216
 - preparation 216
 - License Asset Type, customizing 207
 - License Compliance 218
 - customizing the warning threshold 221
 - setting up 206
 - viewing configuration information 222
 - locations
 - about 202
 - Locations
 - adding 202
 - editing 202
 - maintaining assets manually 201
 - managing 218
 - physical assets
 - about 199
 - adding 199
 - relationships between asset fields 188
 - reporting on assets 201
 - searching for assets 181, 183
 - Software assets 197, 197
 - adding from Assets section 198
 - adding from Inventory section 197
 - customizing Asset Types 197
 - software metering
 - about 423
 - about enabling 424
 - configuring options 428
 - device selection for 424
 - disabling 432
 - disabling for devices with manual labels 432
 - disabling for devices with Smart Labels 432
 - enabling for applications 428
 - enabling for devices with Smart Labels 427
 - enabling with manual device labels 425
 - information collected 423
 - scheduling inventory collection intervals 433
 - scripts that collect information 424
 - software suites 424
 - viewing device details 431
 - viewing metering details 430, 430
 - updating assets manually 196
 - viewing Asset Subtypes on the Assets page 195
 - viewing assets 181, 183
 - viewing available Asset Subtypes 194
 - workflow for SNMP devices 190
 - assigning user roles 226
 - attachments to tickets 702, 723
 - authentication
 - Google OAuth credentials 174
 - managing credentials 172
 - SNMP credentials 176
 - viewing credential usage 178
 - authentication and K1000 user accounts 139
 - authentication credentials for Chrome 277
 - auto-refresh settings 98, 98

B

 - backup files
 - downloading 780
 - restoring 784
 - uploading 783
 - backups
 - about 778
 - deleting backup data 781
 - disabling 781
 - enabling 781
 - manual 780
 - scheduling and retention of 779
 - settings for backups 85
 - bandwidth for Replication Shares 169
 - benchmarks for SCAP 609
 - best practices for patching 560
 - blacklisting applications
 - about 434
 - applying Application Control labels 435
 - editions sharing executables 435
 - limitations of 435
 - marking as Not Allowed 436
 - messages that appear 435
 - removing designation from apps 438
 - reporting on 437
 - requirements 434
 - viewing Not Allowed apps 436
 - broadcasting alerts 495, 496
 - Business Hours for Service Desk 680
 - buying licenses 46

C

 - Cataloged applications 405

- cataloging requests
 - canceling 418
 - how custom names are resolved 416
 - submitting 417
- certificate, for SSL 85
- certification, DIACAP 103
- change history
 - deleting 115
 - for assets 113
 - for objects 114
 - for settings 112
 - organization-level settings history 112
 - reports 632
 - System level 112
 - viewing, searching, and exporting 115, 115, 116
- changing custom ticket fields using email 717
- changing ticket approval fields by email 717
- changing ticket fields using email 716
- checking patch details for a device 594
- child tickets, creating for any ticket 770
- Chrome
 - authentication credentials 277
 - Discovery Schedule for device 278
- classic metering 423
- clearing ticket fields using email 716
- Client Drop File Size Filter 70
- Client Drop Location
 - copying files to 399
 - filter settings for organizations 247
- Client ID
 - used in Chrome authentication credentials 277
- Client Secret
 - used in Chrome authentication credentials 277
- code attributions 45
- Command Line Console
 - about 26
 - accessing 59
- command-line deployment
 - Mac OS X Agent 362
 - Windows Agent 357, 358
- commands that must be run as root 361
- Comment Field Options 765
- comments 722
- comments, adding to tickets 721
- Common Vulnerabilities and Exposures 599
- compliance
 - DIACAP 103
 - for software licensing 206
- components
 - enabled on the appliance 46
 - overview of 26
- computer report 604
- computers
 - searching for in inventory 335
 - statistics 43
- conditional rules
 - writing in Custom Inventory 450
- configuration
 - auto-refresh properties 98
 - date and time 77
 - General Settings, Admin level 66
 - K1000 Agent 96
 - local routing tables 83
 - local web server 83
 - locale settings 99
 - Mobile Device Access 104
 - disabling for the appliance 107
 - disabling for users 107
 - enabling for the appliance 105
 - enabling for users 105
 - network settings 80
 - POP3 email accounts 230
 - security settings 85
 - Service Desk setup tasks 679
 - Service Desk ticket settings 688
 - session timeout 98, 98
 - SSL certificate 94
 - whitelist hosts 83
 - with the Organization component 60
 - without the Organization component 70
- configuration policies 515
 - about 515
 - automatic updates on Windows 516
 - Automatic Updates on Windows 516
 - Dell Command | Monitor 521
 - Desktop Shortcuts 522
 - Event Log Reporter 523
 - MSI Installer 524
 - Power Management for Mac OS X 531
 - Power Management for Windows devices 526
 - registry settings scripts 527
 - Remote Desktop Control 527
 - UltraVNC 528
 - Uninstaller 529
- conflict warning dialog
 - enabling and disabling 687
- creating
 - POP3 email accounts 230
 - security policies 613
- creating a custom ticket layout 768
- credentials
 - adding Google OAuth 174
 - adding SNMP 176
 - adding User/Password 173
 - creating reports of 178
 - deleting 179
 - exporting 179
 - identifying the use of 178
 - managing 172
- CSV format for License data 216
- custom data fields
 - adding 301
- custom fields
 - for Asset Subtypes 190

- Custom Inventory rules
 - about 447
 - checking for conditions 450
 - creating 447
 - defining rule arguments 464
 - getting values from a device 458
 - how implemented 448
 - regular expressions for matching filenames 461, 463
 - syntax 449
 - testing 468
 - types 447
- custom ticket fields
 - changing through email 717
 - defining 765
- custom ticket layouts 762, 768
- custom Ticket Rules
 - creating 737
 - deleting 740
 - duplicating 740
- Custom Views
 - creating from Advanced Search criteria 51
 - for Service Desk tickets 721
- CustomerResponded Ticket Rule 736
- customize ticket detail 765, 767
- customizing
 - Asset Types 184, 203
 - ticket details 688
 - User Console action buttons and widgets 694
 - User Console logo 691, 693
 - User Console welcome message 691, 693
- CVE 599

D

- daily run output 788
- Dashboard
 - about 36
 - Admin level 37
 - customizing 38
 - System level 37
- data retention settings 66, 70
- data sharing preferences 102
- database access to reports 85
- database tables
 - Organization-level 801
 - System-level 801
- date and time settings 77
- debugging Agent software 796
- default organization, about 243
- default queue 748
- default roles 223
- default ticket
 - categories, status, and priorities 688
 - setting a view as the default 721
 - views, using 719
- DefaultTicketOwners
 - email notifications for 227

- deleting
 - Agent messages from command queue 354
 - alerts 677
 - alerts automatically 661
 - appliance backup data 781
 - Asset Subtypes 196
 - Asset Types 189
 - credentials 179
 - Discovery schedules 287
 - label groups 133
 - LDAP Labels 137
 - Mac profiles from devices 551
 - Mac profiles from the K1000 555
 - manual labels 120
 - MIA devices 391
 - notification schedules 641
 - organization filters 257
 - organizations 253
 - provisioning schedules 347
 - Service Desk ticket queues 747
 - Smart Labels 131
 - Software page inventory 397
 - user downloads 754
- Dell
 - device warranty information 393
 - obtaining warranty information 393
 - renewing warranties 394
 - system maintenance and updates 596
 - warranty reports 394
- Dell Command | Monitor
 - adding
 - Dell Command | Monitor scripts 521
 - information on Device Detail page 305
 - installing with Managed Installation 521
 - supported hardware 517
 - supported operating systems 517
- Dell Data Protection | Encryption
 - enabling inventory collection on Agentless-managed Windows clients 333
 - enabling inventory collection on Agent-managed Windows clients 330
 - information viewed in device details 324
 - inventory collection on Windows clients 330
- Dell Mobility Management
 - Discovery Schedule for device 280
- Dell Updates
 - configuring Dell Updates 597
 - patching, compared 596
 - using to maintain your Dell systems 596
 - workflow 597
- dependencies, for scripts 499
- deploying Mac profiles on a schedule 547
- deployment status, of device patches 594
- deployments
 - compared with updates 596
- Deploy-only patch schedules 583
- desktop settings
 - Desktop Shortcuts configuration scripts 522
 - wallpaper configuration script 522
- Detect and Deploy patch schedules 582
- Detect and Rollback patch schedules 583
- detection, inventory term used instead 596

- Detect-only patch schedules 581
- device
 - add monitoring profile to 654
 - adding manually using Administrator Console 376
 - adding manually using API 380
 - alert on configuration change 662
 - apply SNMP configuration to 374
 - detail page for organizations 259
 - Discovery Schedule for AirWatch 283
 - Discovery Schedule for Chrome 278
 - Discovery Schedule for DMM 280
 - Discovery Schedule for SNMP-enabled 281
 - enabling monitoring for 644, 644, 645
 - finding in inventory 335
 - patching status for one 587
 - reassigning to organizations 258
 - running Device Actions 337
 - viewing DDPJE information 324, 330
 - viewing statistics for 43
 - viewing status 791
- Device Actions 66, 70
 - running 337
 - running from Ticket Detail page 725
- device management 287, 300, 375
- DIACAP compliance 103, 103
- Diagnostic Utilities 791
- digital assets for distribution 471
- digital assets, attaching to applications 398
- disabling 781
 - Acceptable Use Policy 103
 - appliance linking 111
 - Mobile Device Access
 - for the appliance 107
 - for users 107
 - secure attachments for tickets 702
 - Service Desk satisfaction survey 702
 - single sign on 161, 164
 - SSH for the appliance 85
- Discovery 264
 - about 264
 - adding schedules for AirWatch devices 283
 - adding schedules for Chrome devices 278
 - adding schedules for DMM devices 280
 - adding schedules for non-computer devices 281
 - adding schedules for quick scans 265
 - adding schedules for thorough scans 274
 - Agentless management
 - enable 365
 - delete schedules 287
 - Nmap 273
 - results 285
 - results and Agent provisioning 286
 - statistics 43
 - stop a running schedule 286
 - using Smart Labels with 127
 - viewing and searching results 285
- disk status 788
- dismissing alerts automatically 661
- distributing
 - Mac profiles 547
 - software 469
- distribution packages
 - about 471
 - about attaching digital assets 471
 - for Mac OS X 472
 - inventory requirement for 471
 - using alternate download locations 472, 472
- DMM
 - device detail 305
- DNS Service Discovery (DNS-SD) requests 85
- documentation
 - for MySQL 630
 - searching the K1000 Help system 52
- domains
 - joining the K1000 server to 91, 162
 - unjoining K1000 server from 164
- domains that must be accessible for patching 563
- download locations, alternate 472, 472
- downloading
 - appliance backup files 780
 - KACE GO 106
 - patches 568
 - SCAP benchmarks 613
- duplicating
 - Agent provisioning schedules 346
 - Mac profiles 546
 - organization roles 246
 - reports 631
 - scripts 512
 - Service Desk ticket queues 747
 - Smart Labels 123

E

- editing
 - Locations 202
- email
 - approving tickets using 774
 - authentication using POP3 229
 - automatically adding addresses to tickets 241
 - changing approval fields using 717
 - changing custom ticket fields 717
 - changing ticket fields using 716, 716
 - clear text using POP3 229
 - clearing ticket fields using 716
 - configuring external SMTP email servers 775
 - configuring internal SMTP servers 775
 - configuring secure SMTP email servers 775
 - customizing email templates 234
 - event triggers 232
 - modifying ticket attributes using 716
 - notifications for Service Desk 228, 229
 - notifications, recommended 232
 - open ticket notification 232
 - POP3 server, using 229
 - Service Desk exclusions for 241
 - setting an approval field value using 717
 - testing and troubleshooting 798
 - testing incoming email 798
 - testing outgoing email 798
 - ticket closure notification 232
- email floods
 - Service Desk prevention of 242

- email notifications for administrators 142
- Email on Events, configuring 232
- email system health 789
- EmailOnClose Ticket Rule 736
- enabling 781
 - Acceptable Use Policy 103
 - API for manual inventory 380
 - appliance linking 109
 - fast switching for organizations 107
 - file sharing
 - organization-level 340, 341
 - System level 339
 - without the Organization component 341
 - file sharing for Windows devices 343
 - LDAP Labels 136
 - Mobile Device Access
 - enabling for users 105
 - for the appliance 105
 - for users 105
 - parent-child ticket relationships 769
 - secure attachments for tickets 702
 - single sign on 161
 - SSH for the appliance 85
 - switching between organizations 107
 - tether to Quest 791
 - ticket creation by email 715
- enabling access to Federation API settings
 - appliance linking 110
- encryption
 - device detail 305
- enforce Internet Explorer settings 614
- Enforce Symantec Antivirus Settings option 619
- enforce XP SP2 firewall settings 615
- error logs
 - for email 799, 800
- escalating tickets 725, 726, 727
 - time limit 726
- Event Log Reporter 523
- examples
 - importing asset license data 216
 - Mac profile removal 554
 - Managed Installation, EXE 479
 - Managed Installation, MSI 479
 - Managed Installation, TAR.GZ 486
 - Perl script for inventory uploads 381
 - XML schema for Windows devices 384
- exporting
 - credentials 179
 - Mac profiles 551
 - Managed Installations 495
 - resources from appliances 260
 - resources from organizations 261

F

- factory settings, restoring 785
- fast switching, enabling for organizations 107
- file sharing
 - enabling at the System level 339
 - with the Organization component 340

- File Synchronizations
 - about 471
 - creating 491
 - viewing ITNinja information in 404
- files supported by Managed Installations 473
- files, attaching to tickets 723
- filters
 - about Data Filters 117
 - adding Data Filters 254
 - data and LDAP, for organizations 253
 - devices by organization 335
 - redirecting devices to organizations 258
- Firefox settings for single sign on 164
- Fixed Ticket Fields 763
- FTP
 - access to appliance backups 780
 - security settings for 85

G

- General Settings 60
- Google OAuth credentials, adding and editing 174
- Google Play 104
- GPO Provisioning Tool
 - deploy Agents with 341, 342
 - preparing system to use 342

H

- hardware specifications for K1000 57
- HEAT Software, Inc. 559
- Help Desk 678
- Help system and PDF 52
- history settings
 - about 111
 - and the Organization component 112
 - asset subscriptions 113
 - assets, viewing 114
 - object subscriptions 114
 - objects, viewing 114
 - subscriptions for organizations 112
 - System level 112
 - viewing 113
- Holidays for Service Desk 680
- Home page, Administrator Console 36
- Hours of Operation for Service Desk 680

I

- identifying credential use 178
- identifying devices with Mac profiles installed 549
- importing
 - K1000 resources, about 259
 - License asset data 216
 - Mac profiles 547
 - resources to appliances 260
 - resources to organizations 262
 - SCAP benchmarks 609
 - users from LDAP servers 152
- inactive patches 595
- increasing license capacity 46
- install Agent using provisioning schedule 344
- installation files for Agent 357

- installer files
 - identify parameters supported by 474
- installing Mac profiles on devices 549
- Intel AMT
 - information displayed in Device Details 334
- Internet Explorer
 - single sign on settings for 164
- Inventory
 - adding
 - devices manually using API 380
 - devices manually, about 375
 - devices manually, Administrator Console 376
 - Software assets 397
 - software manually 395
 - API, enabling 380
 - change history 301, 375
 - custom fields, adding 301
 - data collection schedule 302
 - delete devices 338
 - Dell warranty information 393
 - device detail 304, 305, 324
 - device notifications 335
 - devices, searching for 335
 - force update 388
 - appliance 389
 - Linux devices 389
 - Mac OS X devices 389
 - Windows devices 389
 - labels for devices 336
 - managing devices 287, 375
 - manual inventory information 388
 - metering schedules for 433
 - MIA devices
 - applying labels to 391
 - configuring 390
 - deleting 391
 - overview 300
- Processes
 - about 439
 - adding labels for 440
 - applying and removing labels for 440
 - assigning threat levels to 441
 - categorizing 441
 - deleting 441
 - viewing and editing 440
- running Device Actions 337
- searching for devices 335
- Services
 - about 444
 - adding labels for 445
 - applying and removing labels 445
 - assigning threat levels to 446
 - categorizing 445
 - deleting 446
 - viewing and editing 444
- Smart Labels for 336
- software
 - adding labels for 401
 - applying and removing labels 401
 - categories 400
 - deleting 397
 - digital assets 398
 - ITNinja information for 403
 - Smart Labels 401
 - threat level 400
- Software Catalog
 - adding labels for 401
 - applying and removing labels 401
- Software page
 - about 394
 - viewing items on 395
- startup programs
 - about 442
 - adding labels for 443
 - applying and removing labels 443
 - assigning threat levels for 443
 - categorizing 443
 - deleting 444
 - viewing and editing 442
- submitting information using API 380
- troubleshooting MIA devices 391
- upload XML 388
- view devices 337
- inventory, detection term used instead 596
- iOS 104
- IP scan
 - about 264
 - overview 264
- ITNinja
 - about 402
 - disabling 404
 - enabling 403
 - File Synchronizations 404
 - Managed Installations 403
 - viewing information 403

K

- K1000
 - configuration
 - auto-refresh properties 98
 - session timeout 98
 - SSL certificate 94
 - configuring network settings 57
 - domain access 79
 - hardware specifications 57
 - Home Dashboard widgets 38
 - labels 47
 - license information 644
 - local routing tables 83
 - NTP service, verifying status of 79
 - patch download settings 568
 - port settings 78
 - security settings 85
 - software updates 47
 - software version 45
- K1000 Agent
 - configuring 96
 - provisioning with GPO Tool 341, 342
 - system requirements for installation 343
 - updating automatically 354
 - updating manually 356

- K1000 appliance linking
 - about 108
 - adding names and keys 109
 - disabling 111
 - enabling 109
 - enabling access to Federation API settings 110
- KACE GO 104
 - about 26
 - downloading 106
 - enabling Mobile Device Access 105
- KBSYS database table 801
- Knowledge Base
 - about 754
 - links to articles in User Console 696
- KScripts
 - about 498
 - default 499
 - obtaining dependencies 499
 - token replacement variables for 502

L

- label groups
 - about 117
 - adding and editing 132
 - assigning labels to 133
 - deleting 133
 - removing labels from 133
- labels
 - about 47, 116
 - adding and editing label groups 132
 - adding and editing LDAP Labels 134
 - adding and editing manual labels 118
 - adding Smart Labels 120
 - assigning to label groups 133
 - deleting 120
 - deleting LDAP 137
 - editing Smart Labels 123
 - enabling LDAP Labels 136
 - for application control 435
 - for Service Desk staff 227
 - label groups, about 117
 - LDAP Labels, about 117
 - manual 336
 - organization filters 117
 - searching with LDAP Browser 137
 - Service Desk All Ticket Owners 124
 - Smart Labels, about 116
 - viewing manual label details 119
- laptops, critical patches for 573
- Layout Ticket fields 763
- LDAP Browser 137
- LDAP Labels 117
 - about 47
 - adding and editing 134
 - deleting 137
 - enabling 136
 - searching with LDAP Browser 137
 - variables used in 836
- LDAP server authentication 149
- LDAP server user import 152
- LEP Installation Log
 - viewing 656
- License assets
 - adding for Software Catalog 208, 419
 - adding for Software page inventory 212
 - managing for Software Catalog 418
- License Compliance
 - about 206
 - setting up 208, 419
 - updating 221
 - viewing compliance information 218
- license expiration 45
- license information 46
- license key
 - monitoring counting toward limit 644
 - obtain for expanded server monitoring 646
 - updating appliance with expanded monitoring 646
- license usage warning threshold 221
- linked reports
 - creating using report wizard 633
- linking K1000 appliances
 - about 108
 - adding names and keys 109
 - disabling 111
 - enabling 109
 - enabling access to Federation API settings 110
- links on User Console home page 699
- Linux
 - enabling Agent debugging on 797
 - SELinux and server monitoring 642
 - starting and stopping the Agent on 360
- local authentication for the K1000 140
- local web server 83
- locale settings 66, 70, 100
 - about 99
 - configuring Administrator Console 99
 - configuring Command Line Console 99
 - configuring User Console 100
 - for organizations 101
 - for users 102
- Locally Cataloged applications
 - about 405
 - change to cataloged 416
 - viewing 411
- log date format
 - nonstandard in monitoring 654
- Log Enablement Package
 - editing on Windows Server 2003 device 659
 - editing on Windows Server 2008 or higher device 658
 - for application and threshold monitoring 655
 - installing 656
 - LEP Installation Log 656
 - optional available through ITNinja 655
- log paths
 - Apache 653
 - MySQL 653
- logging in 54
- login credentials, managing 172
- login requirements, for organizations 60
- logos 60, 66, 70, 253, 691, 693

- logs
 - daily run output 796
 - downloading for the appliance 795
 - for email errors 800
 - for patching 595
 - for Scripting 533
 - viewing for the appliance 792
- Lumension Security, Inc.
 - supplier of KACE patches 558

M

- Mac OS X
 - distribution 472
 - enabling Agent debugging on 797
 - Managed Installations for 486
 - manual deployment of Agents on 361
 - patching 595
 - starting and stopping Agents on 363
- Mac OS X configuration policies
 - enforce Active Directory settings 530
 - for VNC 532
 - Power Management 531
- Mac OS X security policies
 - adding scripts 622
 - Application Layer Firewall 621
 - Parental Controls 621
- Mac profiles
 - adding system profiles 542
 - adding user profiles 535
 - deleting from devices 551
 - deleting from the K1000 555
 - deploying on a schedule 547
 - duplicating 546
 - example of deleting from devices 554
 - exporting the Mac profiles list 551
 - identifying devices with profiles 549
 - importing to the appliance 547
 - installing Mac profiles on devices 549
 - viewing the profiles list 550
- Machine Actions (see Device Actions) 66
- maintenance windows
 - scheduling for alert cessation 662
- Managed Installations
 - about 471, 473
 - about creating 473
 - creating for Windows 474
 - EXE example 479
 - exporting 495
 - installer file parameters 474
 - ITNinja 403
 - Mac OS X platform 486
 - MSI example 479
 - parameters for 474
 - RPM example 480
 - TAR.GZ example 486
 - ZIP example 479
- managing credentials 172
- managing devices 287, 300, 375
- managing Mac profiles 535
- managing processes inventory 439
- managing service inventory 444
- managing startup program inventory 442
- manual appliance backups 780
- manual deployment of Agents
 - Command line for Windows 358
 - installation wizard for Windows 357
 - Linux devices 359, 360
 - remove 361
 - logon script 357
 - Mac OS X installer 361
 - Mac OS X terminal window 362
 - using email 357
 - viewing the version 361
 - Windows devices 357
- manual labels 118
- metering
 - about enabling 424
 - data retention settings for 66
 - enabling for applications 428
 - enabling for devices with manual labels 425
 - enabling for devices with Smart Labels 427
 - scheduling inventory collection 433
- MIA devices
 - about 390
 - configuring settings 390
- migrating software License assets 423
- missing patches 594
- Mitre 599
- Mobile Device Access
 - about 104
 - disabling for the appliance 107
 - disabling for users 107
 - downloading KACE GO 106
 - enabling for the appliance 105
 - enabling for users 105
- model number of K1000 45
- monitoring
 - about server 642
 - add profile to device 654
 - create user role for 663
 - creating a new profile 651
 - creating Service Desk tickets from alerts 669, 712
 - disabling on a device 666
 - download profile 654
 - edit a Windows Log Enablement Package 658, 659
 - edit profile 648, 672, 673, 674
 - SNMP traps 649
 - enabling on a device 666
 - enabling on eligible device 644, 644, 645
 - filter unwanted alerts 672, 673, 674
 - pausing for a device 660
 - pausing for multiple devices 661
 - resuming for multiple devices 661
 - return default profile to factory settings 648
 - upload profile 653
 - working with profile 646
- moving resources to network locations 262
- MSI Installer 524
- multicast Domain Name System (mDNS) requests 85
- MySQL
 - documentation link 628, 630
 - log paths 653
 - reporting password for 60

N

- National Vulnerability Database 605
- network scan summary 43
- network settings 57
- Network Utilities 791
- new patches
 - using Smart Labels to view 124
- New Ticket
 - customize 767
- Nmap discovery
 - considerations 273
- non-computer devices
 - adding Asset Subtypes for 191
 - assigning devices to Asset Subtypes 195, 195
 - viewing available Asset Subtypes of 194
- Not Allowed applications
 - about 406
 - Application Control 436
 - removing designation from apps 438
 - viewing 436
- notification schedules
 - adding from list pages 639
 - adding from Reporting section 638
 - deleting 641
 - editing 640
- notifications
 - about 625
 - for administrators 142
 - server monitoring alerts 667
- NTLMv2 341
- NTP service
 - requirement for patching 562
 - verifying status of 79
- NVD 605

O

- object identifiers (OIDs)
 - obtained with K1000 373
 - used in inventory 372, 373
- objects, configuring history subscriptions for 114
- offline KScripts
 - about 498
 - obtaining dependencies 499
- OID
 - obtained with K1000 373
 - used in inventory 372, 373
- online KScripts
 - about 498
 - default 499
 - obtaining dependencies 499
 - token replacement variables for 502
- online shell scripts
 - about 498, 504
- operating systems
 - supported by Agentless management 364
- ORG database tables 801
- Organization component 28, 243
 - appliance General Settings for 60
 - fast switching between organizations 60

- organization filters
 - about 117
 - Data Filters 117
 - LDAP Filters 117
- organization mode 28
- organizations
 - about 243
 - about filtering devices 253
 - adding and editing 247
 - adding Data Filters 254
 - adding LDAP Filters 255
 - Advanced Search for devices 258
 - customizing logos for 253
 - default organization 243
 - deleting 253
 - deleting filters 257
 - Device Details page 259
 - filtering devices 258
 - locale settings for 101
 - managing 243
 - redirecting devices 258
 - require selection at login 60
 - roles, about 244
 - roles, adding and editing 245
 - roles, deleting 247
 - roles, duplicating 246
 - switching between 107
 - testing filters 257
 - user accounts for 253

OVAL

- affected devices, label 604
- computer report 604
- definitions 600
- labels for 601
- reports 604
- run tests 601
- security checks 599
- settings 601
- statistics 43
- tests and definitions 599
- tests, viewing 600
- timestamp 611
- updates 601
- updating definitions 787
- vulnerability report 604

- OverdueClose Ticket Rule 736
- owner-only comments for tickets 722

P

- packages, for Patch Management 558
- parameters for Managed Installations 474
- parent tickets
 - adding existing tickets to 771
 - enabling parents to close child tickets 770
 - using as to-do lists 772
- passwords, managing 173

Patch Management

- about 556
- about critical patches for laptops 573
- about packages 558
- about signature files 558
- about subscriptions 562
- AMP connection requirement 582
- assessment testing 559
- best practices 560
- configuring schedules 573
- Dell devices and updates 596
- Dell Updates workflow 597
- Dell Updates, compared 596
- Dell Updates, scheduling 597, 598
- deployment testing 559
- Deploy-only schedules 583
- details by device 594
- Detect and Deploy schedules 582
- Detect and Rollback schedules 583
- Detect-only schedules 581
- download options 558
- download settings for 568
- download status 571
- for Mac OS X devices 595
- gather information about managed devices 565
- HEAT Software, Inc. 559
- Lumension Security, Inc. 558
- marking patches as inactive 595
- patch catalog 590
- reports for 588
- resetting patch deploy attempts 593, 593
- rollback 589
- Rollback options for patches 588
- Rollback-only schedules 584
- schedule field descriptions 574
- scheduling non-critical patching 573
- Smart Labels for critical OS patches 125
- Smart Labels for desktops 127
- Smart Labels for laptops 130
- Smart Labels for new patches 126
- Smart Labels for servers 129
- speeding up with Replication Shares 560
- subscribing to patches 565
- testing environment 558
- undo the last patch deployment 589
- using Replication Shares for 169
- using Smart Labels with 124
- view missing patches 594
- viewing available patches 571
- viewing downloaded patches 590
- viewing files within patches 588
- viewing logs 595
- viewing patch details 592
- viewing patch status 587
- viewing patch status for devices 587
- viewing schedules 585
- viewing statistics 594
- warning users first, importance of 560
- websites that must be accessible 563
- workflow for critical OS patches 572
- workflow for desktops and servers 572
- workflow for first-time patching 564
- workflow for patching 556

patches

- supplier of, Lumension Security, Inc. 558

Patchlink

- now Lumension Security, Inc. 558

PDF of Help system 52

Perl script

- sample 381

permissions for Service Desk staff role 224

ping probe

- disable 662

policies

- configuration 515

- Windows-based security policies 614

- Windows-based, using 515

POP server settings 80

POP3 email accounts

- DefaultTicketOwners@mydomain.com 230

- supprt@mydomain.com 230

POP3 email server 229

port 443 85

port 80 85

port settings for the appliance

- firewall exceptions for the K1000 78

Power Management for Mac OS X 531

Power Management for Windows 525

preferences for data sharing 102

Preview ticket layout 767

Primary Keys for imported license data 216

Processes

- adding labels for 440

- applying and removing labels for 440

- assigning threat levels to 441

- categorizing 441

- deleting 441

- inventory, about 439

- viewing details of 440

profiles

- about 646

- default monitoring 646

- edit 672, 673, 674

Mac profiles

- about 535

- adding system profiles 542

- adding user profiles 535

- deleting from devices 551

- deleting from the K1000 555

- deploying on a schedule 547

- duplicating 546

- exporting the list of 551

- identifying devices with profiles 549

- importing to the appliance 547

- installing on devices 549

- viewing the profiles list 550

monitoring

- about 646

- add to a device 654

- create new 651, 653

- download 654

- edit 648, 649

- edit a Windows Log Enablement Package 658, 659

- Log Enablement Package for Windows Server 2003 656

- SNMP traps 649

- upload 653
- provisioning
 - schedules for Agent 346
 - viewing results 348
- proxy server settings 80

Q

- Quest Identity Broker
 - about 165
 - configuring 93, 165
 - user approval requests 166
 - using single sign on with 168
- queues
 - about 746
 - adding 746
 - configuring 682
 - customizing ticket details for 688
 - default fields for All Queues list 749
 - deleting 747
 - enabling conflict warnings 687
 - moving tickets between 750
 - setting system default 748
 - setting user default 749
 - transferring Ticket Rules between 741
- quick scans, for Discovery 265

R

- RAID drive status 790
- rebooting the appliance 787
- redirecting devices 258
- registry settings scripts for Windows 527
- reinstalling the Software Catalog 438
- Related Ticket Fields 763
- Remote Desktop Control 527
- removing
 - Agents from Linux devices 361
 - Agents from Mac OS X devices 363
 - Application Control designation 438
 - labels from label groups 133
 - Mac profiles from devices 551
 - Mac profiles from the K1000 555
- renaming Service Desk 686
- ReopenTicket Ticket Rule 736
- Replication Shares
 - about 168, 472
 - adding 169
 - for locale patches 169
 - viewing details of 172
 - weekly schedules of 169

- reports
 - about 625
 - adding schedules 636
 - creating and running 626
 - creating by entering SQL 628
 - creating from list pages 630
 - creating using report wizard 626
 - custom logos for 60, 633
 - deleting custom reports 633
 - deleting notification schedules 641
 - deleting schedules 638
 - Dell warranty 394
 - duplicating existing 631
 - editing 632
 - editing SQL statements 631
 - enabling database access to 85
 - for a single organization 635
 - for blacklisted applications 437
 - for credentials 178
 - for multiple organizations 636
 - for Service Desk 741
 - layout 633
 - notification schedules 638
 - OVAL 604
 - patching-related 588
 - running 625, 635
 - vulnerability reports 604
- requesting Local Cataloging for applications 417
- required fields setting on Service Desk tickets 763
- requiring ticket approvals 773
- resetting patch deploy attempts
 - from patch Catalog page 593
 - from Patch Detail page 593
- resources
 - about transferring 259
 - deleting status of exports 263
 - exporting from appliance 260
 - exporting from organizations 261
 - importing to appliances 260
 - importing to organizations 262
 - moving from local to network locations 262
 - viewing exported or imported 262
 - viewing status of exports 263
- restoring appliance settings 782
- retention of data 66
- roles
 - about 223
 - adding and editing for organizations 245
 - adding and editing, user 143
 - assigning user roles 226
 - default 244
 - for Organizations 244
 - for Service Desk staff 224
 - monitoring-specific 663
- Rollback-only patch schedules 584
- root commands 361
- rules
 - Custom Inventory 447, 447, 458
 - for Service Desk tickets 736

- Run Now command
 - about 512
 - monitoring status of 514
 - using to run scripts 513

- run order
 - of organization filters 254
 - of Smart Labels 131

- run OVAL tests 601

- running Device Actions 725

- running reports 625

S

- Samba share

- Admin-level settings for organizations 66
 - Admin-level settings without organizations 70
 - and Client Drop Location for organizations 247
 - appliance settings 85
 - transferring resources between appliances 259

- satisfaction survey

- modifying the label for 701
 - preventing distribution of 702
 - using 701

- SCAP 605

- about benchmarks 607
 - about scans 608
 - benchmarks, downloading 613
 - benchmarks, viewing 609
 - CCE 605
 - configuring scan schedules 610
 - CPE 605
 - importing benchmarks 609
 - National Vulnerability Database 605
 - NVD 605
 - OVAL 605
 - platforms supported 605
 - protocol 605
 - scan

- accessing scan information 608
 - edit schedule 610
 - how scans are conducted 605
 - resolution files 610
 - results 611

- XCCDF 605

- scheduled task status 594

- scheduling

- daily backups 779
 - Dell Updates 598
 - Discovery scans 265
 - inventory collection for Software Catalog 433
 - inventory collection, devices 302
 - LDAP user imports 152
 - Mac profiles for deployment 547
 - metering for Software Catalog applications 433
 - patch deployment 573
 - reports 636
 - SCAP scans 610
 - Wake-on-LAN requests 494

- screenshots, attaching to tickets 723

- Scripting

- edit policies and scripts 533
 - Mac profiles

- about 535

- adding or editing system profiles 542

- adding or editing user profiles 535

- deleting from devices 551

- deleting from the K1000 555

- deploying on a schedule 547

- duplicating Mac profiles 546

- exporting the Mac profiles list 551

- identifying devices with profiles 549

- importing profiles to the appliance 547

- installing Mac profiles on devices 549

- viewing the profiles list 550

- Run Now status 514

- searching logs 533

- view script tasks 611

- scripts

- adding 504

- adding steps to 821

- default 499

- deleting 510, 511

- duplicating 512

- editing 510

- exporting 534

- importing 511, 512

- Kscripts 504

- log files for 533

- obtaining dependencies 499

- online shell scripts 504

- reusing 512

- run from Script Detail page 514

- run from Scripts page 514

- Run Now 512, 513

- tasks you can automate 498

- token replacement variables for 502

- Windows registry settings 527

- Windows-based policy wizards 515

- workflow 501

- search

- Admin level 48

- advanced

- notifications 50

- Smart Labels 50

- documentation 52

- online Help 52

- page level 48, 49

- searching for devices in Inventory 335

- Secure Content Automation Protocol 605

- security 599

- about OVAL 599

- configuration issues 599

- for Service Desk attachments 702

- monitoring with security run output 623

- settings for the appliance 85

- SSL certificates 94

- vulnerabilities 599

- Security Policies
 - about 613
 - Application Layer Firewall (Mac OS X) 621
 - Internet Explorer 614
 - IXP SP3 Firewall 615
 - Mac OS X 622
 - McAfee AntiVirus 616
 - McAfee SuperDAT 618
 - Parental Controls (Mac OS X) 621
 - Symantec AntiVirus settings 619
- SELinux
 - server monitoring with 642
- serial number of K1000 45
- server monitoring
 - about 642
 - application 655
 - disable 666
 - dismissing alerts 676
 - enable 666
 - enabling on device 644, 644, 645
 - filter alerts 672, 673, 673, 674
 - nonstandard log date format 654
 - number of servers that can be monitored 642
 - obtaining license key for expanded 646
 - pause monitoring 660, 661
 - resume monitoring 661
 - searching for alerts 672
 - threshold 655
 - updating license key to increase limit 646
 - working with alerts 667
 - working with profile 646
- Server-Enhanced Linux
 - effect on server monitoring 642
- Service Desk 723
 - child tickets 769, 769
 - configuring
 - email exclusions 241
 - email settings 241
 - external SMTP email servers 775
 - internal SMTP email servers 775
 - terms used for tickets 686
 - title of Service Desk 686
 - creating child tickets 770
 - customizing
 - ticket categories 688
 - ticket fields 765
 - ticket impacts 688, 762
 - ticket layout 768
 - ticket layouts 688, 762
 - ticket priorities 688, 761
 - ticket settings 757
 - ticket statuses 688, 760
 - default user roles for 223
 - designating parent tickets 771
 - editing 728
 - email
 - configuring settings 228
 - connecting servers to the appliance 774
 - error logs 799
 - errors 800
 - event triggers 232
 - notification strategy 229

- testing incoming email 798
 - testing outgoing email 798
 - troubleshooting 798
 - troubleshooting incoming email 798
 - troubleshooting outgoing email 798
- email testing
 - using Telnet 799
- Knowledge Base
 - adding articles 754
 - attachments, adding 754
 - deleting articles 756
 - external links for 754
 - user ratings and views 756
 - using markdown 754
- labels and roles for staff members 227
- organizing duplicate tickets 772
- overview 678
- parent tickets as to-do lists 772
- parent tickets, enabling 769
- parent-child tickets 769, 770
- preventing
 - unnecessary email traffic 242
- processes
 - adding 728
 - converting to regular tickets 735
 - deleting 735
 - types 732
 - using 727, 733, 733, 734
- queues
 - about 746
 - adding 746
 - configuring 682
 - default fields for All Queues 749
 - deleting 747
 - duplicating 747
 - enabling conflict warnings 687
 - moving tickets between 750
 - setting system default 748
 - setting user default 749
 - viewing tickets in all queues 748
- running reports 741
- Satisfaction Survey 701
- securing attachments 85, 702
- setup tasks for 679
- staff role 224
- system requirements for 678
- ticket approvers, configuring 773
- ticket approvers, using 773
- tickets
 - categories and subcategories, creating 757
 - converting to process tickets 735
 - lifecycle of 703
 - links in User Console 700
 - owner-only comments 722
 - quick-action links on User Console 700
 - viewing in queues 747
- service inventory, managing 444
- session timeout
 - about 60, 70, 98
 - extending 701
 - losing unsaved changes 701
 - resetting 60, 70, 98

- setting up License Compliance 208, 419
- setting up the K1000 server 57
- settings
 - history 111, 112
 - locale 66, 70
 - POP server 80
 - User Console 60
- sharing data 102
- shell scripts 504
- shell support
 - SSH 371
 - Telnet 371
- shut down the appliance 787
- signature files, for patching 558
- single sign on
 - about 159
 - access with Active Directory 164
 - Active Directory method 91, 162
 - configuring Quest Identity Brokerfor 93, 165
 - disabling 161, 164
 - enabling 161
 - using Active Directory for 161
 - using QIB for 160, 165, 168
 - web browser settings
 - Firefox 164
 - Internet Explorer 164
- size restrictions for attachments to tickets 715
- SLA
 - configuring 681
 - configuring Business Hours 680
 - enabling 681
 - Holidays for Service Desk 680
- Smart Labels 116
 - adding 120
 - assigning the run order of 131
 - combining 121
 - deleting 131
 - editing 123
 - for critical OS patches 125
 - for desktops 127
 - for device inventory 336
 - for Discovery Results 127
 - for laptops 130
 - for new patches 126
 - for patching 124
 - for servers 129
 - for Service Desk 123
 - managing 120
- SMTP server
 - connecting to appliance 774
 - using instead of POP3 229
 - verify settings of 790
- SNMP
 - adding and editing credentials 176
 - Discovery Schedule for device 281
 - enabling for the appliance 85
 - full walk 281
 - Inventory Configurations 372, 373, 373, 374

- software
 - deploying from User Console 751
 - removing User Downloads 754
 - Smart Labels 401
 - statistics 43
 - un-installer 529
- Software assets 197, 397
 - adding from Assets section 198, 397
 - adding from inventory 197
 - customizing 197
 - for License Compliance 397
- Software Catalog
 - about 404
 - about cataloged applications 405
 - about data collection 406
 - about Not Allowed applications 406
 - adding applications 415
 - and Application Control 436
 - application categories 406
 - canceling cataloging requests 418
 - change Locally Cataloged to Cataloged 416
 - classifications 405
 - configuring metering options for 428
 - custom names 416
 - data sharing for 406
 - feature comparison with Software page 407
 - for organizations 406
 - ITNinja 406
 - License Compliance for 206
 - license information 208, 419
 - localization of 406
 - Locally Cataloged applications 405, 411
 - migrate License assets 423
 - removing local cataloging 418
 - scheduling inventory collection 433
 - scheduling metering 433
 - Smart Label restrictions for 120
 - software licenses for 418
 - submitting cataloging requests 416, 417
 - updating and reinstalling 438
 - updating License Compliance for 221
 - viewing Discovered applications 409
 - viewing License Compliance for 218
 - viewing Not Allowed applications 436
 - viewing Not Discovered applications 409
 - viewing software details 412
 - viewing Uncataloged 410
- Software distribution
 - about 469
 - adding applications for 473
 - summary of 43
 - testing 470
- software License Compliance
 - about 206
 - updating 221
 - viewing 218

- software metering
 - about 423
 - configuring options 428
 - disabling for devices with manual labels 432
 - disabling for devices with Smart Labels 432
 - disabling for Software Catalog apps 432
 - enabling for applications 428
 - enabling for devices with Smart Labels 427
 - enabling with manual device labels 425
 - viewing device details 431
 - viewing metering details 430, 430
- Software page
 - feature comparison with Software Catalog 407
 - license information 212
- software version, of appliance 45
- special characters
 - escaping in monitoring profiles 674
- specifications, for the appliance 57
- speeding up patching with Replication Shares 560
- SQL queries
 - and Smart Labels 123
 - database table names for 801
 - documentation 630
 - for reports 628
- SSH, enabling for the appliance 85
- SSL certificate wizard 94
- SSL certificates, uploading 85
- SSLv3 (legacy version of SSL) 85
- SSO 159, 160
 - Quest Identity Broker 93, 165
- staff role, creating 224
- starting and stopping the Agent on Linux 360
- starting and stopping the Agent on Mac 363
- startup program inventory
 - adding labels for 443
 - applying and removing labels 443
 - assigning threat levels for 443
 - categorizing 443
 - deleting 444
 - managing 442
 - viewing and editing 442
- statistics
 - computers 43
 - devices 43
 - OVAL 43
 - software 43
- status of patch downloads 571
- status of RAID drives 790
- steps for Task sections of scripts 821
- submitting cataloging requests 416, 417
- subscribing to patches 562, 565
- subtypes for assets
 - about 190
 - adding 191
 - assigning or changing 195, 195
 - deleting 196
 - editing 194
 - setting as default 194
 - viewing available subtypes 194
 - viewing on the Assets page 195
 - workflow for SNMP devices 190

- support information
 - ITNinja 402
- Symantec AntiVirus settings
 - enforcement 619
- synchronizing files 491
- syntax
 - Custom Inventory rules 449
 - for changing custom ticket fields using email 717
 - for clearing ticket fields using email 716
 - for task sections of scripts 821
- System Administration Console 28
- System level 28, 60
 - Dashboard 37
 - user accounts 140
 - with the Organization component 35
- system profiles for Mac 542
- system requirements
 - for Agent installation 343
 - for Service Desk 678
 - for the appliance 57

T

- technical specifications, appliance 26
- technical support tether 791
- Telnet, using to test incoming email 799
- templates
 - for configuration policies 515
 - for security policies 613
 - for Service Desk email 234
- terminal window interface 59
- testing
 - assessment, for Patch Management 559
 - Custom Inventory rules 468
 - deployment, for Patch Management 559
 - incoming email 798
 - LDAP Labels 134
 - LDAP server configuration 150
 - organization filters 257
- tether to Quest 791
- third-party code attributions 45
- threat levels 400
- Ticket Detail
 - customize 765, 767
- Ticket Rules 736
 - creating 737
 - customizing system rules 736
 - defaults for system rules 736
 - deleting 740
 - duplicating 740
 - moving between queues 741
 - transferring between queues 741
 - using system rules 736
- tickets
 - about custom layouts 762
 - approval fields you can change by email 717
 - approvals, configuring 773
 - approvals, requiring 773
 - approving by email 774
 - archival
 - about 741
 - deleting tickets from 744

- enabling 742
- of selected tickets 744
- queue settings for 743
- restoring tickets from 744
- attachment size restrictions 715
- attachments to 723
- attachments, adding 723
- categories and subcategories, creating 757
- categories, CC List values for 240
- change field order 768
- changing approval fields through email 717
- changing custom fields through email 717
- changing fields through email 716
- clearing fields using email 716
- closure notification 232
- comments, adding 721
- comments, viewing 722
- configuring settings for 688
- creating
 - from server monitoring alerts 669, 712
 - from the Administrator Console 705
 - from the Asset Detail page 711
 - from the Device Detail page 710
 - from the User Console 704
- creating statuses for 688
- custom fields you can change using email 717
- custom fields, defining 765
- custom layouts for 768
- Custom Views for 721
- customizing
 - impact values 762
 - priority values 761
 - status values 760
 - ticket settings 757
- default status of 688
- default views, using 719
- deleting from queues 745
- deletion settings for 745
- due dates and SLAs 680, 680, 681
- duplicates, organizing 772
- enabling creation by email 715
- escalation 725
 - about 726
 - email message for 727
 - email recipients 726
 - time limit, about 726
 - time limit, changing 727
- escalation notification 232
- fields you can change by email 716
- history, viewing 724
- lifecycle of 703
- links on User Console home page 700
- modifying by email 716
- navigating among related items 718
- opening notification 232
- owner-only comments, adding 722
- parent-child relationships, enabling 769
- parent-child relationships, using 769
- parents
 - using as to-do lists 772

- using to organize duplicates 772
- quick-action links on User Console 700
- screenshots, adding 723
- sending information by email 724
- setting fields to Required on form 763
- setting the default view for 721
- SLA settings for 681
- states 725
- work information for 718
- time and date settings 77
- time limit on open inactive user sessions 60, 70, 98
- timeout period for user sessions 701
- timing of email from Service Desk 232
- token replacement
 - for Service Desk email 234
 - variables for scripts 502
- tracking changes to settings 112
- transferring resources between appliances 259
- troubleshooting 791, 792
 - Agent provisioning to Windows devices 623, 796
 - Agent software 796
 - appliance issues 792
 - email communications 798
 - Wake-on-LAN requests 495
- types
 - Service Desk processes 732

U

- UltraVNC script for Windows 528
- Uninstaller scripts for Windows 529
- unjoin domain 164
- unpacking the appliance 57
- updates
 - checking for appliance updates 785
 - compared with deployments 596
 - Dell Updates and patching 596
 - viewing K1000 Agent updates 354
- updating
 - K1000 Agents automatically 354, 354
 - K1000 Agents on Linux, manual 360
 - K1000 Agents on Mac OS X, manual 361
 - K1000 appliance software 47
 - OVAL definitions 787
 - Software Catalog 438
 - software License Compliance 221
 - the appliance license key 787
- uploading
 - appliance backup files 783
 - files to the K1000 server 399
 - Mac profiles to the appliance 547
 - SSL certificates for the appliance 85
- usage data sharing 102

- user accounts 149
 - assigning roles to 226
 - authentication with LDAP 149
 - DefaultTicketOwners 227
 - editing profiles 147
 - labels for 123
 - LDAP authentication 149
 - LDAP import, manual 152
 - LDAP import, scheduled 156
 - organization-level 139
 - adding 144
 - editing 144
 - managing 143, 253
 - Organization-level
 - adding 147
 - editing 147
 - Service Desk All Ticket Owners label for 124
 - System-level 139
 - adding 140
 - deleting 143
 - editing 140
 - managing 140
 - time limit on sessions 60, 70, 98
 - viewing profiles 147
- user approval requests, for QIB 166
- user authentication 149
 - LDAP 149
 - LDAP configuration 150
 - local accounts on K1000 server 139
 - single sign on using LDAP 160
- User Console
 - about 26
 - action buttons and widgets 694
 - adding announcements on home page 696
 - adding ticket links to home page 700
 - creating tickets from 704
 - custom links on home page 699
 - customizing 691, 693
 - distribution packages 471
 - links to KB articles from home page 696
 - locale settings for 66, 70
 - logo 693
 - prioritizing announcements on home page 698
 - quick-action ticket links on home page 700
 - settings 60
 - welcome message 693
- User Downloads
 - about 751
 - applying labels to 753
 - creating packages for 751
 - removing labels from 754
 - removing packages 754
- user profiles, adding for Mac 535
- user roles
 - adding 143
 - assigning 226
 - deleting 144
 - editing 143
- User/Password credentials
 - adding and editing 173

V

- variables
 - for Service Desk email 234
 - used in LDAP Labels 836
 - used in scripts 502
- verify the Agent is running on Linux 361
- verify the Agent is running on Mac 363
- version of K1000 software 45
- version of the Agent on Linux devices 361
- version of the Agent on Mac devices 363
- viewing patch schedules 585
- viewing the Mac profiles list 550
- VNC settings, Mac OS X policies for 532

W

- WaitingOverdue Ticket Rule 736
- Wake-on-LAN
 - about 494
 - issuing requests 494
 - scheduling requests 494
 - troubleshooting 495
- wallpaper, controlling for Windows 522
- warning threshold for software licenses 221
- warranty information for Dell devices 393
- websites that must be accessible to the K1000 79
- welcome message, user console 691
- whitelist hosts 83
- widgets
 - Connections 38
 - Critical Patch Compliance 38
 - Current Scripts 38
 - Dell Updates 38
 - Device Check-In Rate 38
 - Devices By Manufacturer 38
 - Devices By Model 38
 - Disk Capacity 38
 - Expiring Dell Warranties 38
 - File Synchronizations 38
 - for User Console 694
 - Latest News Articles 38
 - License Compliance 38
 - Managed Installations 38
 - Managed Operating Systems 38
 - Monitored Devices 38
 - Monitoring Alert Summary 38
 - Monitoring Alerts 38
 - Patch Installation Progress 38
 - Patch Tasks Completed 38
 - Provision Platforms 38
 - Provisioning 38
 - SCAP Summary 38
 - Software License Configuration 38
 - Software Publishers 38
 - Software Titles 38
 - Tasks in Progress 38
 - Top Knowledge Base Articles 38

Windows

- Automatic Update settings 516
- Dell Command | Monitor 521
- enabling Agent debugging on 796, 796, 797
- manual deployment of K1000 Agent 357, 358

Windows configuration policies

- See configuration policies

Windows Group Policy

- using to deploy Agent with provisioning tool 341, 342

Windows policies 515

Windows Server 2003

- monitoring Log Enablement Package from ITNinja 656

Windows-based security policies

- enforce Internet Explorer settings 614
- enforce McAfee AntiVirus Settings 616
- enforce XP SP2 Firewall Settings 615
- McAfee SuperDAT 618
- Symantec AntiVirus settings 619

wizards

- for Agent provisioning 344
- for configuration policies 515
- for generating SSL certificates 94
- for linked reporting 633
- for reporting 626
- for security policies 613
- for Smart Labels 123

work information for Service Desk tickets 718

workflow

- for Asset Subtypes and SNMP 190
- for patch subscription 564
- for patching 556
- for using ticket approvers 773

workstations, patching workflow for 572

X

XML editor, for scripts 510

XML schema

- Linux and Mac 386
- Windows 383