KACE® Systems Management Appliance 11.1

Release Notes

Table of Contents

Quest® KACE® Systems Management Appliance 11.1 Release Notes

This document provides information about the KACE Systems Management Appliance version 11.1.

About KACE Systems Management Appliance 11.1

KACE Systems Management Appliance is a virtual appliance designed to automate device management, application deployment, patching, asset management, and Service Desk ticket management. For more information about KACE Systems Management Appliance series, go to https://www.quest.com/products/kace-systems-management-appliance/. This release contains a number of new features, resolved issues, and security enhancements.

NOTE: This is the only document that is translated for this release, however the localized variants do not include information about resolve issues, enhancements, and known issues. Other guides, such as the *Administrator Guide* and in-product help are not localized at this time, and version 10.2 documents are included.

New features

This release of the KACE Systems Management Appliance includes the following features.

Device communications

- **KACE Agent system tray additions**: More functionality added to the agent icon in the system tray, such as opening links. Your system administrators can specify up to ten links that appear in the new **Shortcuts** menu item. This menu item only appears when one or more links are specified in the agent communication settings, in the *Agent Status Icon Shortcuts* section.

  Standard Uniform Resource Identifier (URI) links are supported, such as HTTP, SSH, and FTP URLs. Clicking this link causes your system to launch the application associated with the selected resource. For example, when you click an HTTP-type link, your system opens the link in the default browser.

- **Hyper-V Inventory**: Inventory information and related device commands are added in this release for the Virtual Machine Manager and MS Hyper-V data, for agent-managed devices. Inventory details include a list

of virtual machines and Hyper-V hosts to inventory. This is similar to the VMware inventory feature created in version 10.0.

- **Operating system support updates**: The appliance now supports the following OS versions on agent-managed devices:
  - MS Windows 10 20H2
  - MS Windows Server 2019 20H2
  - macOS 11.0
    - When connecting to the **User Console** using HTTPS from a macOS 11.0 system, the appliance cannot determine the Unique Identifier (KUID) of the agent associated with that system. This impacts the *My Devices* list and Software Library installs. The root cause of this problem is the new requirement for macOS 11.0 that all certificate trust setting must be approved by the user. This issue also causes the following entry to appear in the `konea.log` on the agent:

      ```
      |ERROR|ssl_darwin.go:107:AddCertAsTrustedRoot |
      SecTrustSettingsSetTrustSettings failed|{"err":"The authorization was
      denied since no user interaction was possible."}
      ```

    - The appliance does not support operating system patching for this version. Application patching is available. OS-level patching for macOS 11.0 devices is available with KACE Cloud Mobile Device Manager (MDM), if you have a subscription.

Patching

- **Linux package upgrades**: The appliance now allows you to automate the process of installing and managing Linux package upgrades that keeps the Linux OS up to date on your managed Linux RedHat, SUSE, Ubuntu, CentOS, and Raspbian devices. These upgrades improve the overall performance of your managed Linux devices and protect them from potential vulnerabilities.

  Use this feature to create upgrade schedules which allow you to either detect package upgrades, or detect and upgrade all applicable packages. You can review the list of the available package upgrades after a detect-only schedule action, for each Linux flavor.

  The upgrade process relies on the assumption that your managed Linux devices point to the appropriate package repositories. Only the packages that include security updates are identified. The appliance does not attempt to detect or upgrade all packages, or to the entire OS to the latest version.

  NOTE: Raspbian Linux does not make a distinction between regular and security updates. Detecting and upgrading packages for managed Raspbian devices results in all updated packages being installed on those devices.

  NOTE: The term *update* in KACE Systems Management Appliance assumes the following: if there are new versions of the packages available in the distribution's repositories, the appliance uses the standard system commands to ensure that the system installs the latest version possible. This is not in any way meant to be exactly the same way that the word *update* (or *upgrade*) is used in the underlying system commands.

- **Integration with the new Dell hardware update catalog**: Starting in this release, the appliance uses a new version of the Dell hardware catalog. The process of detecting and deploying hardware updates is very similar to the one used for device patching. Start by creating schedule updates to either detect, deploy, or both detect and deploy hardware updates. You can review the list of the available Dell updates on the catalog page. This page lists the updates for which signature files exist on the appliance.
  - This feature requires the latest version of the KACE Agent to run on managed Dell devices.
  - Existing data related to Dell hardware updates such as schedule history is not migrated from earlier versions of the appliance.
  - User reports associated with Dell hardware updates and created with a previous version of the appliance are not migrated to version 11.1.

Infrastructure

- **Oval for Linux and Mac**: In this release, the appliance extends Oval support beyond existing MS Windows-only using the world's biggest and best selection of CVE data in the world.
- **License renewal alerts**: When the appliance maintenance expires, some features such as patching support become unavailable. This causes an error alert to appear on the Home Dashboard. To renew your license, visit https://support.quest.com/contact-us/renewals.

Service Desk

- **Service Desk ticket category hierarchy**: The Administrator Console is improved to allow you to make setting up categories and subcategories for Service Desk more streamlined. You can create and edit ticket category and subcategory nodes using a tree widget. The tree view allows you to better understand and manage the relationships between the categories. You can easily add new category nodes, rename, delete, or sort them, as needed. A search function is also available, to quickly locate a specific category or sub-category.
- **Ability to specify Service Desk ticket prefix**: Starting in this release, you can use a different prefix for each queue to organize your Service Desk workflow, and to associate them with applicable categories, such as `HELP:` for Helpdesk or `HDREQ:` for hardware and software requisitions.
- **Support Microsoft 365 GCC High service**: Your MS Office 365 OAuth credentials now allow you to specify your Azure AD tenant type and endpoint URL, to acquire tokens for the national cloud associated with your environment. When select an Office 365 OAuth for inbound Service Desk emails, you can point to an applicable Microsoft 365 API Service, such as Microsoft 365 GCC, Microsoft 365 GCC High, and others. Microsoft 365 GCC High in particular is used in high-security environments.

Enhancements

The following is a list of enhancements implemented in this release.

Enhancement	Issue ID
Windows Installer now preserves the `NoHooks userinit` registry setting during upgrade.	K1A-2393
Managed Installation can continue if the Agent disconnects.	K1A-2392
KACE Agent no verifies the Konea tunnel and alerts the server if broken.	K1A-2384
The user is alerted when reboot is pending and patching operations are skipped as a result.	K1A-2381
11.1 KACE macOS agents use PKG installer file rather than DMG disk image.	K1A-2374
API access can now be restricted through the *Access Control List Details* page.	K1-30596
This version includes the ability to sort by custom ticket fields in KACE GO.	K1-30562
SAML-enabled systems can now be locked down to allow access only to SAML-authenticated users and the local `admin` user.	K1-30246
This version includes an option to reject SAML users who do not already have an account on the appliance.	K1-30211

Enhancement	Issue ID
Approval Status column is added to the *Quarantine* list and *Quarantine Detail* pages.	K1-30105
In the *General Settings* page, an option is added to indicate interest in participation in a future Beta program.	K1-30071
The appliance now includes the ability to select an Azure AD *GCC High account* during the creation of credentials for a Office365 OAuth account, and to set the URL endpoint for a .us domain.	K1-22281
In the email notification text editor, the **$** button now allows insertion of tokens.	K1-22082
Added the ability to select a *single-tenant* Azure AD account type during the creation of credentials for a Office365 OAuth account.	K1-21914
User's manager can now be reset to *Unassigned* either manually through the **Administrator Console**, or during LDAP import with an empty manager mapped field.	K1-19328
Discovery schedules for devices associated with an Active Directory server, now include a new option for enabling the appliance to use a secure port for LDAP communication, **Use Secure LDAP (LDAPS)**. This check box is available in the *Active Directory* section on the *Discovery Schedule Detail* page, when you select **Active Directory** as the *Discovery Type*.	N/A
Access Control List restrictions can be now applied based on sub-domains. You can specify the sub-domain name on the *Access Control List* page, in the *IP Address/ Doomain* column of the *Allow List*.	N/A

Resolved issues

This section contains the issues resolved in this release:

- Resolved Service Desk issues
- Resolved KACE Agent issues
- Resolved Inventory issues
- Other resolved issues

Resolved Service Desk issues

The following is a list of Service Desk issues resolved in this release.

Table 1. Resolved Service Desk issues

Resolved issue	Issue ID
Creating a Service Desk process template that included a separator could result in an error when used from the User Portal.	K1-30698

Resolved issue	Issue ID
Time Closed, *Time Stalled* and *Time Opened* are not updated for a parent ticket with approvals.	K1-30685
When copying text from a Word application to a ticket, the formatting could not be retained.	K1-30545
When duplicating a process, the ticket template was not duplicated.	K1-30460
Tickets with very long summary fields could result in an error when the *Tickets* list page loads.	K1-23726
Default ticket template is not set when creating a new ticket by email.	K1-23422
Unexpected rendering behavior (scrolling) could be seen when viewing ticket details when multiple categories and sub-categories are present.	K1-22645
In the Service Desk list view, *Time Open* and *Time Opened* are renamed to *Time Since Last Opened* and *Last Opened*, respectively.	K1-22630
Emails sent with display names with a comma or multi-language character to a Service Desk queue through POP3 was not handled correctly, in some cases.	K1-22610
Image was broken using several variables in email templates.	K1-21347
Email On Event ticket notification emails were formatted differently than Custom Ticket Rule emails.	K1-21198
Default value was not displayed on ticket detail page for drop-down fields with *Always Required* option.	K1-21187
Service Desk: Token emails from Gmail to Gmail leaved behind empty spaces.	K1-21186
When a ticket is submitted by email with embedded dark colors, the text was hidden if the **Administrator Console** is also set to a dark theme.	K1-21147
Process parent ticket did not close if child tickets were closed from *Tickets* list view.	K1-21143
Service Desk email notifications broke if templates exceeded character limits.	K1-21118
Advanced Search: Filters did not work as expected when using Unassigned Owner.	K1-21116
Advanced Search in *Tickets* list: Filters did not work as expected when using *Status* and *Process Status*.	K1-21107
Populating a Service Desk ticket multi-selection custom field with double quotes in the select value resulted in unexpected behavior.	K1-21094
Ticket attachment links sent in email notifications did not work as expected in some cases.	K1-19964

Resolved KACE Agent issues

The following is a list of KACE Agent issues resolved in this release.

Table 2. Resolved KACE Agent issues

Resolved issue	Issue ID
CentOS receives all updates with the Linux Update feature. The security filter is not available for the Linux Package Upgrades page.	K1A-3810
KACE Agent 11.0 failed to download file from HTTPS source, impacting use of replication shares that are accessed through the HTTPS protocol.	K1A-2330
Client certificate install operation could timeout on newly provisioned Windows devices, preventing the agent from receiving any commands from the appliance until a reconnect event happened.	K1A-2329
VMM managed Hyper-V host was not added to appliance during VMM inventory when the Agent is installed on some Hyper-V hosts.	K1A-2328
Replication did work when password had an '@' symbol.	K1A-2326
macOS 11.0 (Big Sur): Installing KACE Agent with the Agent Status icon enabled resulted in warnings during installation.	K1A-2318
`konea.exe` and `clientidentifier.exe` could crash in some environments.	K1A-2291
Recurring Alert messages kept spawning new Windows on endpoint.	K1A-2289
Wake-on-LAN (WoL) through relay did not display error when the relay agent selected was down.	K1A-2285
Tokens were treated as invalid by agents (error: Agent token signed by another server) if the appliance database became out of sync with the file system.	K1-30642
SNMP inventory data from Dell servers could cause inventory to fail.	K1-30615
In the **System Administration Console**, on the *Agent Token Detail* page, *Organization* is represented with its ID instead of name.	K1-29969
Offline KScripts did not run when scheduled for *Run on the* instance/day of week.	K1-21173
MSI Policy wizard script could fail to set the registry value correctly.	K1-21049
Scripting option *Allow run without a logged-in user* cleared still allowed script to run.	K1-19576
SMB URLs did not properly handle passwords with special characters.	K1-17342

Resolved Inventory issues

The following is a list of Inventory issues resolved in this release.

Table 3. Resolved Inventory issues

Resolved issue	Issue ID
SNMP inventory mistakenly identified non-hex strings as hex strings, causing incorrect values in some cases.	K1-30668
Dell Warranty retrieval errors were not logged to the new `dell_warranty_log` error file.	K1-30531
Overdue Service Desk widgets included tickets that were not yet overdue.	K1-30480
In the **Quarantine** list page, it was not possible to view the details of a quarantined device.	K1-24508
Viewing script logs from the *Device Detail* page displayed blank logs.	K1-21349
Reset Tries button in *Windows Feature Updates Status* on *Device Detail* page did not always work.	K1-21172
Gateway IP Address was not an available column on the *Devices* list page.	K1-21131
Machine deletion could lead to software installation counts being inaccurate.	K1-20437
No history was tracked when Smart Label was edited.	K1-17612

Other resolved issues

The following is a list of other issues resolved in this release.

Table 4. Other resolved issues

Resolved issue	Issue ID
The *Windows Feature Update Summary* page did not correctly list all updates, in some cases.	K1-30887
Knowledge Base articles with multiple labels could be hidden for users.	K1-30671
LDAP Import: Scheduled imports set to *None* could still run automatically.	K1-30666
Compliance by Patch and *Compliance by Machine* widgets sometimes did not display correct values.	K1-30630
Images did not appear correctly in knowledge base articles, in some cases.	K1-30565

Resolved issue	Issue ID
Emails with multiple CC's sent to a Service Desk queue through a POP3 server could not be handled correctly.	K1-30533
File attachments of type .eml or .msg were missing from tickets submitted by email.	K1-30527
Managed Installation with **Override default installation** configured would show **Default installation** set after saving.	K1-30481
An error could be seen while creating custom view on the *Quarantine* page in the **System Administration Console**.	K1-29978
Do not associate file Managed Installation option was not displayed correctly after saving.	K1-29927
In some cases, the network settings for the proxy settings were not honored by the Credential manager when using an Office365 OAuth account.	K1-29063
Access to the **Administrator Console** could be disrupted when changing an organization's virtual IP address or host name.	K1-25452
Email sent to Service Desk queues that use a multi-part MIME format could fail to parse correctly.	K1-22656
When a non-administrative queue owner attempts to retrieve the list of Service desk tickets using the API, tickets they did not submit could be omitted from the results.	K1-22653
SFTP- and FTP-specific *Offboard Backup Transfer Settings* fields containing backslashes caused offboard backup failure.	K1-22608
The *Object History* page sometimes failed to load when it contained Windows Feature Update data.	K1-21575
Agent upstream tunnel client certificate validation failed when an aging konea certificate was archived.	K1-21354
In KACE GO it was not possible to accept barcode searches that have embedded spaces or new line characters.	K1-21195
SAML LDAP attribute mapping option could cause authentication failures.	K1-21193
Asset import did not change Assignee information.	K1-21185
Code can now be saved in the *Notes* field of KScripts.	K1-21184
Monitoring: Create Ticket in Profile configuration did not select proper queue ID.	K1-21175
Search on *Device Issues* page did not function as expected.	K1-21169
SAML: Editing SP Metadata for `NameIDFormat` did not save changes.	K1-21139

Resolved issue	Issue ID
Unexpected behavior observed when trying to map and update *Manager* field using SAML.	K1-21102
Default role for new users did not always honor the role chosen in *Settings*.	K1-21082
Alternate location for Managed Installation was not used behind a replication share.	K1-21016
Location was unassigned on asset when a new or previously removed device connects.	K1-20468
The **Generate Self-Signed Certificate** button was incorrectly enabled before the configuration information was saved in the SSL wizard.	K1-18300

Known issues

The following issues are known to exist at the time of this release.

Known issue	Issue ID
KACE Agent for SUSE 11.1 requires `libxslt` to be installed in order to install. This is a newly introduced dependency.	K1A-3813
Disk Usage history is not recorded by a macOS KACE Agent of an APFS file system.	K1A-3805
The appliance reports the MS Windows 10 build number 20H2 through its technical release version of 2009.	K1A-3803
Dell Updates: Custom View does not report any results when Smart Label is a criteria.	K1-31860
Email attachments in `.eml` and `.msg` file format are marked as *discarded* if subject contains slashes '/'.	K1-31786
Linux package upgrades: *Deploy All* can push some updates that change system configuration which requires manual reconfiguration, such as on Ubuntu 18.04LTS (Desktop version with UI).	K1-31770
KACE GO: Non-admin queue owners cannot to set ticket device/asset to arbitrary device.	K1-31764
Windows Feature Update (WFU) schedule fails when using a deployment type of *Detect and Stage* type and the Agent version is 10.2.	K1-31743
Wake-on-LAN (WoL) options are not present in the **Choose Action** menu on the *Device Detail* page for supported devices.	K1-31729
Duplicating patch schedule from list of schedules does not work as expected.	K1-31714
Duplicating Dell Updates schedule from list of schedules does not work as expected.	K1-31713

Known issue	Issue ID
Users with no queue permissions cannot see tickets they are CC-ed on.	K1-31710
Downloading status count is not displayed in *Patch Schedules* list page.	K1-31066
Managed Installation Detail page incorrectly shows that PKG files cannot be used.	K1-30820
Patching step with reboot in *Task Chain* shows Failed status.	K1-30812
Patch schedule with On-Demand Deploy ends Task Chain task when staging is completed.	K1-30811
Patch schedule information is not showing correctly after disabling a patch schedule.	K1-30733
Schedule information is not showing correctly after disabling a Linux package upgrade schedule.	K1-30725
Pasting an image into a knowledge base article causes other pasted images to reset alignment and justification.	K1-30721
Package download process incorrectly updates offline *Last Modified* instead of *Last Update* status.	K1-30588
Invalid filters (Smart Labels) can be saved, resulting in Smart Labels that never populate.	K1-20268

System requirements

The minimum version required for installing KACE Systems Management Appliance 11.1 is 11.0. If your appliance is running an earlier version, you must update to the listed version before proceeding with the installation.

The minimum version required for upgrading the KACE Agent is 10.2. We recommend running the latest agent version with KACE Systems Management Appliance 11.1.

NOTE: The KACE Agent RPM package can be installed on managed SUSE Linux devices only when the `libxslt-tools` package is installed before the agent package.

To check the appliance version number, log in to the **Administrator Console** and click **Need Help**. In the help panel that appears, at the bottom, click the circled **'i'** button.

Before upgrading to or installing version 11.1, make sure that your system meets the minimum requirements. These requirements are available in the KACE Systems Management Appliance technical specifications.

- For virtual appliances: Go to https://support.quest.com/technical-documents/kace-systems-management-appliance/11.1-common-documents/technical-specifications-for-virtual-appliances/.
- For KACE as a Service: Go to https://support.quest.com/technical-documents/kace-systems-management-appliance/11.1-common-documents/technical-specifications-for-kace-as-a-service/.

Product licensing

If you currently have a KACE Systems Management Appliance product license, no additional license is required.

If you are using KACE Systems Management Appliance for the first time, see the appliance setup guide for product licensing details. Go to More resources to view the appropriate guide.

NOTE: Product licenses for version 11.1 can be used only on KACE Systems Management Appliance running version 11.1 or later. Version 11.1 licenses cannot be used on appliances running earlier versions of the appliance, such as 10.0.

Installation instructions

You can apply this version using an advertised update or by manually uploading and applying an update file. For instructions, see the following topics:

- Prepare for the update
- Update the KACE Systems Management Appliance server using an advertised update
- Upload and apply an update manually
- Post-update tasks

NOTE: To ensure accuracy of software discovery and install counts for devices running particular software, beginning in the KACE Systems Management Appliance 7.0 release, the software catalog re-installs with every upgrade.

Prepare for the update

Before you update your KACE Systems Management Appliance server, follow these recommendations:

- **Verify your KACE Systems Management Appliance server version**:

  The minimum version required for installing KACE Systems Management Appliance 11.1 is 11.0. If your appliance is running an earlier version, you must update to the listed version before proceeding with the installation.

  To check the appliance version number, log in to the **Administrator Console** and click **Need Help**. In the help panel that appears, at the bottom, click the circled '**i**' button.

- **Verify your KACE Agent version**.

  The minimum version required for upgrading the KACE Agent is 10.2. We recommend running the latest agent version with KACE Systems Management Appliance 11.1.

  NOTE: The KACE Agent RPM package can be installed on managed SUSE Linux devices only when the `libxslt-tools` package is installed before the agent package.

- **Back up before you start**.

  Back up your database and files and save your backups to a location outside the KACE Systems Management Appliance server for future reference. For instructions on backing up your database and files, see the **Administrator Guide**, https://support.quest.com/technical-documents/kace-systems-management-appliance/11.1-common-documents/administrator-guide/.

- **Appliances installed prior to version 7.0**.

For appliances initially installed prior to version 7.0 that have not been re-imaged (physical appliances) or reinstalled (virtual), Quest Software strongly recommends exporting, re-creating (an image, or a virtual machine installation from an OVF file), and re-importing the database before upgrading to version 11.1. For complete information, visit https://support.quest.com/kace-systems-management-appliance/kb/111810/how-to-re-image-the-k1000-appliance.

If your appliance version is many versions behind, the following article contains useful upgrade-related tips: https://support.quest.com/kace-systems-management-appliance/kb/155574/upgrading-a-kace-systems-management-appliance-that-is-multiple-versions-behind-upgrade-path-6-x-to-10-0-.

There are many reasons why you should re-image the appliance. The new disk layout, for example, offers better compatibility with version 11.1. It also features better security and performance.

To determine if your system would benefit from such an upgrade, you can use a `KBIN` file to determine the exact age of your appliance and its disk layout. To download the `KBIN`, visit https://support.quest.com/kace-systems-management-appliance/kb/210267/how-to-run-the-kace-systems-management-appliance-configuration-report.

- **Ensure that port 52231 is available**.

  Prior to any `.kbin` upgrade, port 52231 must be available so that the KACE Upgrade Console page is accessible. If the upgrade is initiated without making this port available, you will not be able to monitor upgrade progress. Quest KACE highly recommends allowing traffic to the appliance through port 52231 from a trusted system and monitoring the upgrade from the Upgrade Console. Without access to the Upgrade Console, the upgrade redirects to an inaccessible page which appears in the browser as a timeout. This may lead someone to believe that the upgrade has crashed the system, causing them to reboot the box when, in fact, the upgrade is still in progress. If unsure about the progress of the upgrade, contact KACE Support and **do not reboot the appliance**.

Update the KACE Systems Management Appliance server using an advertised update

You can update the KACE Systems Management Appliance server using an update that is advertised on the *Dashboard* page or on the *Appliance Updates* page of the **Administrator Console**.

CAUTION: Never manually reboot the KACE Systems Management Appliance server during an update.

1. Back up your database and files. For instructions, see the **Administrator Guide**, https://support.quest.com/technical-documents/kace-systems-management-appliance/11.1-common-documents/administrator-guide/.
2. Go to the appliance *Control Panel*:
   - **If the Organization component is not enabled on the appliance, click Settings.**
   - **If the Organization component is enabled on the appliance: Log in to the appliance System Administration Console: `http://`KACE_SMA_hostname`/system`, or select System in the drop-down list in the top-right corner of the page, then click Settings.**
3. On the left navigation bar, click **Appliance Updates** to display the *Appliance Updates* page.
4. Click **Check for updates**.

   Results of the check appear in the log.
5. When an update is available, click **Update**.

IMPORTANT: During the first ten minutes, some browsers might appear to freeze while the update is being unpacked and verified. Do not navigate away from the page, refresh the page, or click any browser buttons on the page during this time because these actions interrupt the process. After the update is unpacked and verified, the *Logs* page appears. Do not manually reboot the appliance at any time during the update process.

Version 11.1 is applied and the KACE Systems Management Appliance server restarts. Progress appears in the browser window and in the **Administrator Console**.

6. When the server upgrade finishes, upgrade all of your agents to version 11.1.

Upload and apply an update manually

If you have an update file from Quest, you can upload that file manually to update the KACE Systems Management Appliance server.

CAUTION: Never manually reboot the KACE Systems Management Appliance server during an update.

1. Back up your database and files. For instructions, see the **Administrator Guide**, https://support.quest.com/technical-documents/kace-systems-management-appliance/11.1-common-documents/administrator-guide/.
2. Using your customer login credentials, log in to the Quest website at https://support.quest.com/kace-systems-management-appliance/download-new-releases, download the KACE Systems Management Appliance server `.kbin` file for the 11.1 GA (general availability) release, and save the file locally.
3. On the left navigation bar, click **Appliance Updates** to display the *Appliance Updates* page.
4. In the *Manually Update* section:
    a. Click **Browse** or **Choose File**, and locate the update file.
    b. Click **Update**, then click **Yes** to confirm.

    Version 11.1 is applied and the KACE Systems Management Appliance server restarts. Progress appears in the browser window and in the **Administrator Console**.
5. When the server upgrade finishes, upgrade all of your agents to version 11.1.

Post-update tasks

After the update, verify that the update was successful and verify settings as needed.

Verify successful completion

Verify successful completion by viewing the KACE Systems Management Appliance version number.

1. Go to the appliance *Control Panel*:
    - **If the Organization component is not enabled on the appliance, click Settings.**
    - **If the Organization component is enabled on the appliance: Log in to the appliance System Administration Console:** `http://`**KACE_SMA_hostname**`/system`**, or select System in the drop-down list in the top-right corner of the page, then click Settings.**
2. To verify the current version, click **Need Help** in the upper-right corner of the page, and in the help panel that appears, at the bottom, click the circled **i** button.

Verify security settings

To enhance security, database access over HTTP and FTP is disabled during the update. If you use these methods to access database files, change the security settings after the update as needed.

1. Go to the appliance *Control Panel*:
   - **If the Organization component is not enabled on the appliance, click Settings.**
   - **If the Organization component is enabled on the appliance: Log in to the appliance System Administration Console: `http://`KACE_SMA_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 **Security Settings** to display the *Security Settings* page.
3. In the top section of the page, change the following settings:
   - **Enable Secure backup files**: Clear this check box to enable users to access database backup files using HTTP without authentication.
   - **Enable Database Access**: Select this check box to enable users to access the database over port 3306.
   - **Enable Backup via FTP**: Select this check box to enable users to access database backup files using FTP.

   CAUTION: Changing these settings decreases the security of the database and is not recommended.
4. Click **Save**.
5. **KBIN upgrades only**. Harden root password (2FA) access to the appliance.
   a. In the System Administration Console, click **Settings > Support**.
   b. On the *Support* page, under *Troubleshooting Tools*, click **Two-Factor Authentication**.
   c. On the *Support Two-Factor Authentication* page, click **Replace Secret Key**.
   d. Record the tokens and place this information in a secure location.

More resources

Additional information is available from the following:

- Online product documentation (https://support.quest.com/kace-systems-management-appliance/11.1/technical-documents)
  - **Technical specifications**: Information on the minimum requirements for installing or upgrading to the latest version of the product.

    For virtual appliances: Go to https://support.quest.com/technical-documents/kace-systems-management-appliance/11.1-common-documents/technical-specifications-for-virtual-appliances/.
    For KACE as a Service: Go to https://support.quest.com/technical-documents/kace-systems-management-appliance/11.1-common-documents/technical-specifications-for-kace-as-a-service/.
  - **Setup guides**: Instructions for setting up virtual appliances. Go to https://support.quest.com/kace-systems-management-appliance/11.1/technical-documents to view documentation for the latest release.
  - **Administrator guide**: Instructions for using the appliance. Go to https://support.quest.com/technical-documents/kace-systems-management-appliance/11.1-common-documents/administrator-guide/ to view documentation for the latest release.

Globalization

This section contains information about installing and operating this product in non-English configurations, such as those needed by customers outside of North America. This section does not replace the materials about supported platforms and configurations found elsewhere in the product documentation.

This release is Unicode-enabled and supports any character set. In this release, all product components should be configured to use the same or compatible character encodings and should be installed to use the same locale and regional options. This release is targeted to support operations in the following regions: North America, Western Europe and Latin America, Central and Eastern Europe, Far-East Asia, Japan.

The release is localized to the following languages: French, German, Japanese, Portuguese (Brazil), Spanish.

About us

Quest creates software solutions that make the benefits of new technology real in an increasingly complex IT landscape. From database and systems management, to Active Directory and Office 365 management, and cyber security resilience, Quest helps customers solve their next IT challenge now. Around the globe, more than 130,000 companies and 95% of the Fortune 500 count on Quest to deliver proactive management and monitoring for the next enterprise initiative, find the next solution for complex Microsoft challenges and stay ahead of the next threat. Quest Software. Where next meets now. For more information, visit www.quest.com.

Technical support resources

Technical support is available to Quest customers with a valid maintenance contract and customers who have trial versions. You can access the Quest Support Portal at https://support.quest.com.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to-videos
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product.

Legal notices

If you have any questions regarding your potential use of this material, contact:

Quest Software Inc.

Attn: LEGAL Dept

4 Polaris Way

Aliso Viejo, CA 92656

Refer to our Web site (https://www.quest.com) for regional and international office information.

Patents

Quest Software is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at https://www.quest.com/legal.

Trademarks

Legend

CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

IMPORTANT, NOTE, TIP, MOBILE, or VIDEO: An information icon indicates supporting information.

KACE Systems Management Appliance Release Notes

Updated - July 2021

Software Version - 11.1