



KACE® Systems Management Appliance 15.0

Release Notes



Table of Contents

Quest® KACE® Systems Management Appliance 15.0 Release Notes	3
About KACE Systems Management Appliance 15.0.....	3
New feature.....	3
Enhancements.....	3
Resolved issues.....	5
Resolved Server Issues.....	5
Resolved Service Desk Issues.....	9
Resolved KACE Agent Issues.....	11
Known Issues.....	12
System Requirements.....	12
Product licensing.....	13
Installation instructions.....	13
Prepare for the update.....	13
Update the KACE Systems Management Appliance server using an advertised update.....	14
Upload and apply an update manually.....	15
Post-update tasks.....	15
Verify successful completion.....	16
Verify security settings.....	16
More resources.....	17
Globalization.....	17
About us	18
Technical support resources.....	18
Legal notices.....	18

Quest® KACE® Systems Management Appliance 15.0 Release Notes

This document provides information about the KACE Systems Management Appliance version 15.0

About KACE Systems Management Appliance 15.0

KACE Systems Management Appliance is 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/>.

New feature


This release of the KACE Systems Management Appliance includes the following new feature.

- **Favorites Feature for UI Navigation:** The Favorites feature improves navigation efficiency by allowing users to bookmark frequently accessed pages. This feature is useful for administrators managing large environments where quick access to repetitive workflow is essential. The Favorites feature offers the following capabilities
 - It is available in both Admin and System UI.
 - It supports up to 50 favorites per UI.
 - It includes drag-and-drop reordering, search, and delete options.
 - It supports only static pages and it does not support dynamic or context-driven pages.

Enhancements

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

1. **Dashboard Revamp:** The Dashboard has undergone a major redesign to a more modern, customizable, and data-rich experience.
 - Modern Layout and Themes: Users can design dashboards with flexible layouts, color themes, and widget arrangements. The drag-and-drop interface allows easy customization to fit different monitoring needs.
 - Multiple Dashboards per User: Instead of being limited to a single view, users can now create, manage, and switch between the multiple dashboards. Each dashboard can be named, tailored, and set as a personal default for quick access.
 - Widget-Level Enhancements: Widgets have been upgraded with richer functionality
 - Create widgets from scratch or based on existing reports using step-by-step wizard or SQL queries for advanced customization.
 - Configure charts in multiple formats including bar, line, doughnut, gauge, score, progress, geo charts, and so on.
 - Add multiple versions of the same widget type (for example, different filtered views of Active Tickets).
 - Use built-in widget controls to refresh data, export results, modify charts, reposition legends, or override colors at the widget level.
 - Resize and rearrange widgets simply by drag-and-drop.
 - Limit the widget visibility based on user roles or labels.
 - Share and distribute insights:
 - Email dashboards as HTML snapshots, either immediately or on a schedule (daily, weekly, monthly).
 - Choose the number of widgets to display per row in the email.
 - Performance and data refresh:
 - Benefit from caching optimizations for large environments.
 - Refresh data on-demand at the dashboard level or the individual widget level.
2. **Patch Catalog Enhancements:** The patch catalog has been significantly enriched with advanced intelligence to help IT teams assess and prioritize patching with greater accuracy.
 - Additional data points now include CVSS Scores, EPSS Scores, Known Exploit Vulnerabilities, and Ransomware Campaign Usage, sourced from trusted threat intelligence feeds such as NIST, MITRE, and FIRST.org.
 - Enhanced filtering capabilities allow admins to search patches based on these metrics and build more targeted dashboards and reports.
 - New widgets, such as Exposure by CVSS Score, Patch Status Breakdown by CVSS, Patch by CVSS Score, and Device Patch Status Breakdown by CVSS, deliver actionable insights at a glance.
 - Users can directly access CVE links within patch details and request missing CVE data from the catalog team.
3. **Linux Patch Scheduling Update:** Users can now decide whether to apply only security patches or all available patches during Linux package upgrades. This provides greater flexibility and ensures better alignment with enterprise compliance needs.

 **NOTE:** Some Linux distributions do not differentiate between patch types and will always upgrade all packages.
4. **Enhanced Security and Logging Revamp:** The legacy FreeBSD syslog has been fully replaced with modern, secure logging mechanisms.
 - Support for logging system over secure TCP with TLS ensures logs are transmitted safely.

i **NOTE:** We support integration with any logging system that can be configured to use TLS. While our documentation provides examples for integrating with syslog-ng and rsyslog, our support is not limited to these tools.

- Logging now captures SSH login/logout, remote console activity, and invalid login attempts for better auditability.
- The SMA generates certificates and keys for secure authentication, while remote servers must configure corresponding credentials.

i **NOTE:** The existing syslog configurations will no longer work after upgrading. Admins must reconfigure syslog settings with the new secure options.

5. **Script Log Retention Redesign:** The script log retention model has been redesigned for performance and scalability.

- Logs are now retained based on the number of script runs (default: 7) instead of a time-based model.
- This ensures predictable storage management and faster system performance in large environments.

i **NOTE:** Due to schema changes, all existing agent logs will be wiped during upgrade. You must export critical log data before upgrading if needed.

6. **Splashtop Integration Enhancements:** Splashtop functionality has been enhanced to provide smoother remote management.

- Improved RMM code assignment during installation.
- Displayed streamer version in device details.
- Enabled uploading of streamer logs to SMA for troubleshooting.
- Added remote control button in ticket details.
- Supported one-time custom session settings during remote access.
- Configured blank screen logo (PNG only) during sessions.
- Supported two simultaneous remote sessions

7. **Quick Links for Admin Navigation:** Quick links have been introduced to reduce navigation friction for users. These include direct access to Label Management, Smart Labels, LDAP Labels, Security Settings, and Service Desk Pages.

Resolved issues

This section contains the issues resolved in this release:

- [Resolved Server Issues](#)
- [Resolved Service Desk Issues](#)
- [Resolved KACE Agent Issues](#)

Resolved Server Issues

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

Table 1. Resolved server issues

Resolved issue	Issue ID
Software Catalog title search takes too long in license asset page. The Retain Uncataloged data in the 'Software Catalog' option is now moved from Organizations: General Settings to System: General Settings for Multi-Org license.	K1-36466
Barcode section is visible on License Asset detail page, even without Barcode tag configuration on License Asset Type detail page.	K1-36065
Machine with blank user info has owner set to the first user found in USER table.	K1-36143
Not able to set a value of '0' on a required asset field of type 'Number'.	K1-36125
Getting incorrect device count when user performs Remote control session reset for a device.	K1-36063
Error while duplicating a Discovery schedule of External Integration type.	K1-34918
Patch detect schedule fails with error 'Task Configuration changed since scheduling'.	K1-36138
Update patch signature download check to be less restrictive.	K1-36576
While deploying a patch, the user is not prompted again after snooze duration and Patch schedule status shows error.	K1-36080
Patch Schedules appear to be stuck in 'process-log' phase for up to 15 minutes.	K1-36124
Windows Feature Update schedules stuck in 'process-log2' phase.	K1-36147
Search action on Agent Token list page doesn't consider selected filter on View By drop-down.	K1-35500
Allow more than 195 GB for Offboarding Backups to Azure Blob Storage.	K1-36127
Admin user unable to change the SystemUI settings while navigated using AdminUI links.	K1-35497
Remote Connection can fail if session password is not updated fast enough on streamer due to low memory.	K1-35982
Unable to track history while changing Authentication settings from 'Local Authentication' to 'LDAP Authentication'.	K1-35036
Error observed when user selected for deletion is set as Manager to itself.	K1-35488
Search action on User list page doesn't consider selected filter on View By drop-down.	K1-35496
Virtual Hostname and Virtual IP on organizations is not working.	K1-35962

Resolved issue	Issue ID
Option to add Barcodes not available when creating a new asset.	K1-36006
User logged out when loading a device with an image attachment on its asset, if assets permission is set to HIDE.	K1-36434
Barcode Data not added/updated when asset import is done through a scheduled import or Run option from the asset import list view.	K1-35545
Newly created locations not visible after adding a new Location subtype.	K1-35468
Unable to edit custom field in Asset Type when adding for the first time.	K1-36078
Deleting a barcode tag does not validate if it is in use before removing it causing errors for Kace Go app users.	K1-36170
Location field HTML tags become visible on custom view when a second field named 'Location' exists.	K1-36225
Advanced search result shows blank custom field values if custom field contains ampersand (&) within the field name.	K1-35149
Alerts set to 'All Devices' without confirmation when no device or label restriction has been set.	K1-36086
Replication share schedule changes require to click into very specific spots on the time grid.	K1-35979
Task Chains with online Shell script remain on status 'Running'.	K1-33958
Task chains results inconsistent across ORGs for failed online scripts.	K1-35092
Task chain tasks after a patch task fail to be executed.	K1-36087
Task chain results are inconsistent when multiple patch tasks are executed.	K1-36388
Label Management choose action menu not interpreting html character '' for apostrophe.	K1-35759
Error shown when applying a label to a device and there are no labels with Remote Control enabled.	K1-36083
Unable to apply a label in User detail if label and user IDs are the same.	K1-36131
Error when loading a smart label while logged in with a device scoped user role.	K1-36298
Installed Versions not loading for Software Catalog application item of type Suite.	K1-35515
SAM Inventory Processing fails when processing software with foreign language characters in filename.	K1-35822

Resolved issue	Issue ID
Application versions fail to load for locally titled software.	K1-36500
Devices on non-SMA Splashtop licensed appliance shown in device issues if Splashtop is installed.	K1-36239
HTML Scheduled report notification email does not display new lines properly.	K1-36149
Error displayed when clicking link on Dell Updates report.	K1-35638
Report shows incomplete or blank results due to PHP ParseError.	K1-35924
Wizard created report fails with error Unknown column 'RUN_AS_CREDENTIAL' in 'order clause'.	K1-35935
Scripting list view 'Run' action do not work for multi-selects.	K1-35960
A new Agent Script Log Retention setting has been added to control how many script run logs are preserved. The default retention is set to 7 runs.	K1-36113
Antivirus Quarantine advanced search, custom view and report queries are malformed when filtering by a user type field.	K1-34259
Error when an advanced search is done on Dell Updates Catalog.	K1-35550
Device Linux Package Repository Information not updated on server side when repository is removed from device.	K1-35539
Patch job shows status 'Reboot Snoozed' when device is actually rebooting.	K1-35596
Patch schedule set in Agent Time Zone fails to be scheduled for devices in different time zones.	K1-36089
Fixed sorting for patch schedule list columns.	K1-36456
Suppress newsyslog email sent to root by Cron Daemon.	K1-35998
HAProxy process consumes high CPU usage after certificate update.	K1-36306
HAProxy fails to stop when services are restarted.	K1-36441
Validate License fails to check maintenance renewal status.	K1-36120
Diagnostic Tools Top does not load for Spanish locale.	K1-35201
Backups are not running at the newly scheduled time.	K1-36056
Backups cannot be re-enabled if disabled in 14.x or prior upgrade.	K1-36652
User credential password is incorrectly changed on save when editing other fields.	K1-34797

Resolved issue	Issue ID
Custom logo does not show when 'Acceptable Use Policy' is enabled.	K1-36202
Old agent binaries not removed after update when device is not in default org.	K1-35933
Local import on multi-org appliance does not allow importing more than one resource at a time.	K1-36153
Local Admin role is overwritten when SAML user has same email address as local Admin.	K1-34924
System UI LDAP browser credentials input fields are missing.	K1-36074
Task Schedule page takes a long time to load or hangs when there are task chains with too many tasks on a frequent schedule.	K1-34207
Make Asset Unique ID field visible for Devices Asset type and subtype list view.	K1-36168
Address User Sessions table can grow large over time and become sluggish.	K1-36093
Update netdiag utility to display SMA serial number.	K1-36201
Splashtop remote control session to allow 2 connections to the device at a time.	K1-36040
An option to hide the general 'Ask any general topic' link in the User Portal Need Help page.	K1-36480
Partial hybrid inventory deletes custom inventory data.	K1-36169
MI table column 'NOTES' is renamed to 'Name'.	K1-36075
Add an option to disable API access to the SMA.	K1-36884

Resolved Service Desk Issues

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

Table 2. Resolved Service Desk issues

Resolved issue	Issue ID
Announcement text in the user portal is overlapped for long 'Message Title' when dragged to the Urgent section.	K1-36062
Archived and Closed columns in Archived Ticket list do not sort correctly.	K1-35648
Child tickets are not automatically created when parent ticket is approved via email.	K1-35407
Custom view option is not present in View By drop-down if All Queue option is selected.	K1-36244

Resolved issue	Issue ID
CC List users for an archived ticket not able to see the ticket in the archive ticket list view after queue is deleted.	K1-35578
Ticket fields not shown in UserUI if SAT_SURVEY permission is set to 'Owners Only - Visible' or 'Owners Only - Hidden'.	K1-36002
Service desk email tokens support for org virtual hostname.	K1-33897
Error when a Default Ticket Template that contains a separator is used on an Exported queue.	K1-36743
Process initiated by e-mail creates the parent ticket, but no child tickets if submitter in process template is left unassigned.	K1-34142
Browser 'URI too long' error when large tables are added to an email on event template.	K1-35642
Service Desk Process sends out duplicate notifications when process approval is completed and process only has a parent ticket.	K1-35873
Handle ticket attachments when content-disposition header is not present.	K1-36042
User receives a CC list notification after adding a comment to a ticket, if their email appears after the first address in the CC list.	K1-36242
Closing process last child ticket via email should allow to close/complete process when option 'Allow last child ticket to close parent ticket' is enabled.	K1-34143
Comment field is missing from process templates when Summary is hidden and Comment field is marked visible for queue.	K1-36041
Default value of a 'Read Only' Ticket Template field is not displayed on parent/child tickets.	K1-36346
Wizard report shows tickets from all queues although report topic is set to a specific ticket queue.	K1-34088
Allow more than five field conditions for ticket templates.	K1-36311
Ticket template conditional logic for 'Begins With' does not work if condition string has spaces.	K1-36330
Changing field to 'Always required' before updating the template causes conditional logic to be lost.	K1-36460
Last selected Service Desk view only retained for the last queue the user was working on before navigating out.	K1-36095
Blank option shown on Related Tickets drop-down menu when title for the ticket is 'Hidden'.	K1-36121

Resolved issue	Issue ID
Allow administrator or queue owner users to see all archived tickets for a queue, after it is deleted.	K1-35575
Unable to import ticket field values if custom field type is single/multiselect and using QUERY to populate options list.	K1-36288
Ticket Asset field not loading when 'Filter on submitter assigned assets' is checked, and custom asset type exists that includes a User field type.	K1-36334

Resolved KACE Agent Issues

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

Table 3. Resolved KACE Agent issues

Resolved issue	Issue ID
Removed Network adapters without MAC addresses from inventory.	K1A-3932
Agent reports incorrect BIOS name and manufacturer on Debian Linux.	K1A-4088
ShellCommandDateReturn Custom Inventory Rule fails on Linux Platform.	K1A-4093
Support Windows environment variable with custom inventory rules.	K1A-4095
Windows agent failing to upload inventory.xml due to MDM Server field containing '&' character.	K1A-4121
Windows Defender Patch detection fails due to RegExpandSz.	K1A-4130
On-Demand Patch deployment doesn't run if agent is not connected when the service starts.	K1A-4134
Inventory fails on Ubuntu devices with r-cran packages installed.	K1A-4135
RegistryValueEquals Custom inventory and KScript 'Verify a registry value is exactly' task fails.	K1A-4137
Agent will not start when a 'configure log access' group policy is applied to a system and the agent in not granted access.	K1A-4139
Linux patch detection fails on Ubuntu 24 LTS.	K1A-4157
Windows Installer not honoring NoHooks installation when upgrading agent from 13.2 to 14.x.	K1A-4158
Addition of hyperthreading virtual processors inventory data.	K1A-4159
Linux Updates: Support all packages upgrade in addition to security only.	K1A-4165

Resolved issue	Issue ID
Agent recreates client certificate too aggressively and cause identity to reset.	K1A-4187

Known Issues

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

Known issue	Issue ID
Google Workspace discovered devices with NULL mac addresses can be provisioned multiple times as agentless automatic, resulting in duplicate entries.	K1-36841
Emojis added to Response Templates are not visible during editing.	K1-36814
SQL syntax error occurs when saving a new report in Managed Install.	K1-36718
Filtering Provisioning Schedules list page using IP Range triggers an error.	K1-36682
Access Control functionality is not working with IPv6 IP.	K1-36411
Due to RabbitMQ upgrade, the SMA will lose user notifications during the upgrade process.	K1-36216
Reports in System UI for ORG-enabled appliances fail when the password includes the '\$' character placed anywhere except at the end. Other special characters do not cause this issue.	K1-35051

System Requirements

The minimum version required for installing KACE Systems Management Appliance 15.0 is 14.1. If your appliance is running an earlier version, you must update to the listed version before proceeding with the installation.

The required version for the Remote Control feature to run is KACE Systems Management Appliance 14.1 and KACE Agent 14.1. Please upgrade the KACE Agent and the KACE Systems Management Appliance to version 15.0.

The minimum version required for upgrading the KACE Agent is 13.0. We recommend that you always use the same version of the agent and the KACE Systems Management Appliance.

Starting in version 12.0 of the appliance, earlier KACE Agent versions, such as 11.1, must be signed specifically for your appliance version. For example, if you are using KACE Agent 11.1 with the 12.1 version of the appliance, you must obtain and install the KACE Agent 11.1 KBIN file that is signed with the 12.1 appliance key. You can download signed KACE Agent KBIN files from the KACE Systems Management Appliance *Software Downloads* page.



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 the '?' icon at the top right, and then click the circled 'i' button.

Before upgrading to or installing version 15.0, 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/15.0/technical-specifications-for-virtual-appliances>.
- For KACE as a Service: Go to <https://support.quest.com/technical-documents/kace-systems-management-appliance/15.0/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 15.0 can be used only on KACE Systems Management Appliance running version 14.1 or later. Version 15.0 licenses cannot be used on appliances running earlier versions of the appliance, such as 13.0.

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:

- **IMPORTANT: Enable legacy BIOS booting:**

An issue in the UEFI BIOS booting can be triggered during an upgrade. To prevent it, you must ensure that legacy BIOS booting is enabled. A power-down of the appliance prior to making a switch is required. Also, for ESX-based virtual machines, ensure that the hardware version is 13 or later.

Prior to applying the appliance upgrade, you must ensure that your browser's cache is clean and that port 52231 is available from your browser to the appliance. Users working from home may need to have their corporate firewall configured to allow port 52231 communications.

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

The minimum version required for installing KACE Systems Management Appliance 15.0 is 14.1. 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 the '?' icon at the top right, and then click the circled 'i' button.

- **Verify your KACE Agent version.**

The minimum version required for upgrading the KACE Agent is 13.0. We recommend that you always use the same version of the agent and the KACE Systems Management Appliance.

Starting in version 12.0 of the appliance, earlier KACE Agent versions, such as 11.1, must be signed specifically for your appliance version. For example, if you are using KACE Agent 11.1 with the 12.1 version of the appliance, you must obtain and install the KACE Agent 11.1 KBIN file that is signed with the 12.1 appliance key. You can download signed KACE Agent KBIN files from the KACE Systems Management Appliance *Software Downloads* page.

i **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/15.0/administration-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 14.1. For complete information, visit <https://support.quest.com/kace-systems-management-appliance/kb/4281031/how-to-re-image-kace-system-management-appliance-sma>.

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/4284819/sma-server-and-agent-upgrade-path>.

There are many reasons why you should re-image the appliance. The new disk layout, for example, offers better compatibility with version 15.0. It also features better security and performance.

- **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/15.0/administration-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 Server updates**.

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

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 15.0 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 15.0.

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/15.0/administration-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 15.0 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 **Apply KBIN**, then click **Yes** to confirm.

Version 15.0 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 15.0.

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 the '?' icon at the top right, and then 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. Go to **Settings > Control Panel** and under *Security Settings*, click **Configure network security and accessibility**.
3. Under the **Security Options** tab, 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/15.0/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/15.0/technical-specifications-for-virtual-appliances>.
For KACE as a Service: Go to <https://support.quest.com/technical-documents/kace-systems-management-appliance/15.0/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/15.0/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/15.0/administration-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 Software creates technology and solutions that build the foundation for enterprise AI. Focused on data management and governance, cybersecurity and platform modernization, Quest helps organizations address their most pressing challenges and make the promise of AI a reality. Around the globe, more than 45,000 companies including over 90% of the Fortune 500 count on Quest Software. For more information, visit www.quest.com or follow Quest Software on X (formerly Twitter) and LinkedIn.

Technical support resources

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

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

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

Legal notices

© 2025 Quest Software Inc. ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Quest Software Inc.

The information in this document is provided in connection with Quest Software products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Quest Software products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, QUEST SOFTWARE ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL QUEST SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF QUEST SOFTWARE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Quest Software makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Quest Software does not make any commitment to update the information contained in this document.

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

Quest Software Inc.

Attn: LEGAL Dept

4 Polaris Way

Aliso Viejo, CA 92656

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

Patents

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

Trademarks

Quest, the Quest logo, Join the Innovation, and KACE are trademarks and registered trademarks of Quest Software Inc. For a complete list of Quest marks, visit <https://www.quest.com/legal/trademark-information.aspx>. All other trademarks and registered trademarks are property of their respective owners.

Legend



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



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

KACE Systems Management Appliance Release Notes

Updated - December 2025

Software Version - 15.0