KACE® Systems Management Appliance 15.1

Release Notes

Table of Contents

Quest® KACE® Systems Management Appliance 15.1 Release Notes....3
About KACE Systems Management Appliance 15.1....3
New features and Enhancements....3
Deprecated features....5
Resolved issues....5
Resolved Server Issues....5
Resolved KACE Agent Issues....7
Known Issues....8
System Requirements....8
Product licensing....8
Installation instructions....9
Prepare for the update....9
Update the KACE Systems Management Appliance server using an advertised update....10
Upload and apply an update manually....10
Post-update tasks....11
Verify successful completion....11
Verify security settings....12
More resources....12
Globalization....13
About us....14
Technical support resources....14
Legal notices....14

Quest® KACE® Systems Management Appliance 15.1 Release Notes

This document provides information about the KACE Systems Management Appliance version 15.1

About KACE Systems Management Appliance 15.1

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 features and Enhancements

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

NOTE: Stay current with KACE SMA Updates : To help keep appliances secure and up to date, KACE SMA now displays an upgrade reminder when eligible updates or hotfixes become available. Administrators can review available updates immediately or postpone the reminder until next day. This feature helps ensure that important maintenance and security updates are not overlooked.

- **Windows ARM64 Agent Support**: This release introduces native agent support for Windows on ARM64 devices, enabling inventory, software distribution, scripting, and systems management capabilities on ARM-based Windows endpoints.
  - Added native KACE Agent support for Windows ARM64 devices
  - Enables management of ARM-based Windows systems using the same KACE SMA workflows available for x64 endpoints
  - Supports core endpoint management functions, including inventory collection, software distribution, scripting, and device monitoring
- **Windows Feature Update Enhancements**: This release introduces support for modern Windows Feature Updates beyond Windows 11 23H2, enabling deployment of Microsoft's UUP-based feature upgrades for Windows 11 24H2 and future releases.
  - Added support for Windows 11 24H2 and future UUP (Unified Update Platform) based Feature Updates.
  - Improved compatibility with Microsoft's current and future Windows Feature Update delivery model.
  - Enables organizations to continue managing and deploying Windows Feature Updates through KACE SMA as Microsoft evolves its upgrade technology.
- **HTTPS-Only Appliance Enforcement:**:This release enforces HTTPS-only access, disabling unsecured HTTP connections to enhance security and protect administrative and user communications.
  - The Initial Setup Wizard has been updated to require SSL certificate configuration during appliance setup.
  - Options to disable SSL or revert to unsecured HTTP access have been removed from appliance settings.
  - Customers must enable HTTPS before upgrading to KACE SMA 15.1. If HTTPS is not configured, the upgrade process stops and records an error indicating the required action.
  - Enforcing HTTPS-only access aligns the appliance with modern security best practices and compliance requirements.
- **Online Shell Script Exit Code Handling**: This release introduces optional exit code enforcement for online shell scripts, enabling script success and failure status to accurately reflect the script's returned exit code
  - Added an Enforce exit code option for online shell scripts to provide more accurate execution status reporting.
  - When enabled, online shell scripts returning a non-zero exit code are reported as failed, while scripts returning 0 are reported as successful.
  - When disabled, online shell scripts continue to report successful execution regardless of the script's returned exit code, preserving legacy behavior
- **Microsoft 365 Modern Authentication for Outbound Email**: The release adds support for Microsoft 365 Modern Authentication (OAuth 2.0) for outbound email, providing a secure alternative to legacy SMTP authentication across supported Microsoft 365 cloud environments
  - Added support for Microsoft 365 Modern Authentication (OAuth 2.0) for appliance email delivery
  - Administrators can now choose between Legacy SMTP Authentication and Modern Authentication (Microsoft 365) from the Network Settings page
  - Supports multiple Microsoft 365 cloud environments
- **Email Notifications for User Alerts**: This release introduces email delivery for User Notifications, allowing administrators and stakeholders to receive important appliance alerts and updates without requiring access to the SMA console
  - Added the ability to send User Notifications via email to designated recipients.
  - Administrators can enable or disable email delivery independently for each User Notification
  - Supports multiple recipients using a comma-separated list of email addresses.
- **FreeBSD OS and Security Updates**: The release adds update to Freebsd OS and several package and security updates to the appliance

Deprecated features

This release of the KACE Systems Management Appliance deprecates following feature.

- **Removal of Embedded Chat Support**: This release removes the embedded Chat option from the appliance interface, directing customers to Quest's updated support experience through the Quest Support Portal

Resolved issues

This section contains the issues resolved in this release:

- Resolved Server 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
Dell Updates smart label optimization	K1-35188
SMA task scheduler fails randomly due to failed CPU activity check.	K1-37035
Splashtop connection initiated when searching if a connection was recently initiated and the device page has not been refreshed.	K1-37026
Duplicate directives on HTTP header.	K1-37062
MariaDB hangs during upgrade.	K1-37059
Custom Inventory rules not applied to non-Windows devices	K1-37067
Translation header metadata is shown in the MI name field if the field is blank and the UI is set to non-English.	K1-37359
Unable to associate Software with a Software Asset via API if it is already mapped to a different Software Asset.	K1-37350
Dell Updates Schedule detail table shows ID column when language is set to German.	K1-37354

Resolved issue	Issue ID
Additional column header shown on Linux Package Upgrade schedule detail page when language is German.	K1-37357
Shell scripts suddenly stop running after SMA upgrade to 15.0.	K1-37233
Backups fail with "Can't translate pathname to UTF-8".	K1-37183
Service Desk ticket from email txt or html attachments are not added to ticket.	K1-37222
Offline patching - Unable to patch Windows Server 2025 systems.	K1-37148
Koneas service fails to stop.	K1-36985
Task chain stays running forever when there are shell scripts tasks.	K1-37252
User Detail Page - Ticket "Number" column does not sort correctly once IDs reach 1,000,000.	K1-37196
SMA task scheduler crashes with MYSQL process gone.	K1-37253
Filter options not visible in Archive page when Locale set to German.	K1-37362
User notifications retention not honored if notifications are not loaded in the UI.	K1-37017
Process Parent tickets can't be closed from Ticket List if there are open child tickets, even though "Allow parent ticket to close child tickets" is enabled.	K1-37008
Backup size calculation gets bloated when running scheduled backup if there are spaces at the beginning of the filename.	K1-37199
Unable to Apply Label to Dell Updates.	K1-37146
Network traffic to Google IP addresses observed after server upgrade to 15.0.	K1-37129
Count for devices missing patches takes too long when doing advanced search or smart label test causing UI to be unavailable.	K1-34728
Unable to save OS selection in Dell Updates	K1-33254

Resolved issue	Issue ID
SAML authentication overwrites existing additional email in user details if email is not mapped.	K1-36864
Duplicating a Default Template removes 'Is Default' flag and the duplicate is made the default.	K1-37004
Unable to search by Name in User Downloads when type is Managed Install.	K1-36800
SAML users fail to be redirected to ticket page when using direct link unless the user is already logged in.	K1-34278
SQL error observed on report generated from Managed Install.	K1-36718
New versions of blocked application not blocked until application control is re-toggled.	K1-37011
Samba share file ownership and permissions could be incorrectly modified, preventing users from adding, modifying, or deleting files	K1-36998
Temporary files generated while processing email attachments were not automatically removed, which could result in excessive disk space consumption over time	K1-37042

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
Inventory.xml locked by powershell process during inventory, results in upload failure.	K1A-4264
Fix kscript command registry_pattern_match (Verify a registry pattern matching).	K1A-4219
KInventory process crashes on non-Windows devices that have only IPv6 and no IPv4 addresses.	K1A-4258
Fix load failed error on Mac device when enabling software meter service.	K1A-4237
Agent inventory on Debian Linux is missing the system serial number and model name.	K1A-4240

Resolved issue	Issue ID
KScript command 'Verify a WMI value does not exist' does not work.	K1A-4236
Fix invalid inventory system uptime value for Ubuntu 26.	K1A-4263
Fix incorrect inventory data for currently logged-on user on Ubuntu 26.	K1A-4262
SMA Munki package refresh for Mac patching	K1A-4193

Known Issues

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

Known issue	Issue ID
Oops error shown when creating a new ORG if local admin user has an additional email address	K1-37264
LDAP User Import preview results are left-shifted when intermediate columns are empty	K1-37149

System Requirements

The minimum version required for installing KACE Systems Management Appliance 15.1 is 15.0. 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 14.1. We recommend that you always use the same version of the agent and the KACE Systems Management Appliance.

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 15.1, 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/15.1/technical-specifications-for-virtual-appliances.
- For KACE as a Service: Go to https://support.quest.com/technical-documents/kace-systems-management-appliance/15.1/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 15.1 can be used only on KACE Systems Management Appliance running version 14.1 or later. Version 15.1 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 15.1 is 15.0. 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 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 14.1. We recommend that you always use the same version of the agent and the KACE Systems Management Appliance.

  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/15.1/administration-guide
- **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/15.1/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: `https://`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**.

   Impor **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 15.1 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 15.1.

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/15.1/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 15.1 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 **Apply KBIN**, then click **Yes** to confirm.

    Version 15.1 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 15.1.

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: `https://`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: `https://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/15.1/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/15.1/technical-specifications-for-virtual-appliances.

    For KACE as a Service: Go to https://support.quest.com/technical-documents/kace-systems-management-appliance/15.1/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/15.1/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/15.1/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

© 2026 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

10801 N. Mopac Expressway

Building 3, Suite 400

Austin, Texas 75759

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 - July 2026

Software Version - 15.1