

Quest®



KACE® Systems Management Appliance 14.0

## Release Notes



# Table of Contents

<b>Quest® KACE® Systems Management Appliance 14.0 Release Notes</b> .....	<b>3</b>
About KACE Systems Management Appliance 14.0.....	3
New features.....	3
Deprecated features.....	4
Resolved issues.....	4
Resolved Service Desk issues.....	4
Resolved Server issues.....	5
Resolved KACE Agent issues.....	7
Known issues.....	7
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.....	11
Post-update tasks.....	11
Verify successful completion.....	11
Verify security settings.....	12
More resources.....	12
Globalization.....	13
<b>About us</b> .....	<b>14</b>
Technical support resources.....	14
Legal notices.....	14

# Quest® KACE® Systems Management Appliance 14.0 Release Notes

---

This document provides information about the KACE Systems Management Appliance version 14.0

## About KACE Systems Management Appliance 14.0

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 features

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

- **Enhanced User Interface :**  
Elevating customer success through UI optimization is paramount. In version 14.0, we initiated a project to streamline interactions, minimizing clicks and scrolling. The KACE Systems Management Appliance UI is now responsive and dynamic, enhancing usability across all devices.
- **64-bit Agent for Windows and All Linux Flavors:**  
Agents for both Windows and Linux are now exclusively 64-bit. This simplification significantly eases and streamlines the authoring and delivering workloads across all operating systems.
- **MDM Enrollment Status in Inventory:**  
macOS and Windows agents will now communicate the device enrollment status to modern management providers, such as KACE Cloud or Microsoft Intune.
- **Monitoring Support added for Non-Server OS:**  
The Monitoring feature now extends support to Windows clients such as Win 10, 11, and so on. Additionally, the Monitoring feature is now provided at no cost up to the maximum node count of 200. Please note that activating the 200-seat entitlement at no charge requires an updated license key.

# Deprecated features

The following features will be deprecated in future releases:

- HP Warranty
- OVAL and SCAP security
- Configuration policy and Mac profiles
- 32 bits agent installer for Windows
- Global Search textbox from all pages
- host SMA on server 2016 HyperV images

# Resolved issues

This section contains the issues resolved in this release:

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

## Resolved Service Desk issues

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

Table 1. Resolved Service Desk issues

Resolved issue	Issue ID
Service Desk tickets can be edited without having set <i>Always Required Due Date</i> .	K1- 34759
Owners only permissions cause process ticket submitter to be unassigned.	K1- 34320
Oops! error when creating new ticket when invalid query is used to set custom field Default value.	K1- 33985
Conditional logic fields disappear after ticket is created from ticket template.	K1- 33382
Process Template breaks when approver is deleted.	K1- 33129
Widget bar chart shows a '0' at the bottom of the chart when having more than 10 owners.	K1- 32795
Age column on the Ticket list page displays 0 for custom views.	K1- 32538
Email notifications are sent when a different Category with no CC is set.	K1- 34736

Resolved issue	Issue ID
'Please complete category selection' error shown when <b>Category</b> field is not visible when using ticket template.	K1- 34661

## Resolved Server issues

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

Table 2. Resolved server issues

Resolved issue	Issue ID
Users with labels assigned unable to log in to Kace Go app.	K1-35437
Remove login method used from error message when user authentication failed for LDAP users.	K1-35421
Assets by location dashboard widget shows incorrect percentage.	K1-35391
Lenovo Warranty automatic update not working.	K1-35382
ESXi hosts missing from inventory if the host does not have a ' <i>management</i> ' network adapter type.	K1-35369
Inventory takes a long time to complete after 13.2 upgrade.	K1-35191
Open SSH Vulnerability CVE-2023-48795.	K1-35085
LDAP User import preview for invalid data shows blank rows.	K1-35070
Wizard created reports show MySQL error <i>Column in field list is ambiguous</i> when sorting by <i>USER</i> fields.	K1-35069
Unable to create or edit multi-line batch files in scripting.	K1-34761
Dell Updates schedules list non-Dell devices under <i>Schedule status</i> .	K1-34724
Self-signed certificate is not being renewed when deploying over an existing one.	K1-34719
Windows 11 readiness report includes machines already updated to Windows 11.	K1-34709
Error when creating Asset:License reports using the wizard.	K1-34706
Linux package upgrade schedule not shown under device details status when schedule action is Detect and Upgrade All.	K1-34704
Exim CVE-2023-42117 and CVE-2023-42119	K1-34695
cURL and libcURL CVE-2023-38545 & CVE-2023-38546.	K1-34668

<b>Resolved issue</b>	<b>Issue ID</b>
Drag and drop of files in a ticket adds a link to the file attachment with no payload.	K1-34653
Default Subtype is not assigned while moving device to new ORG.	K1-34608
SAML authentication fails to redirect to Identity Provider if ORG name includes certain special characters.	K1-34597
Dell Updates catalog Error and Install count are incorrect for some updates.	K1- 34594
Error when importing LDAP user from Google Workspace.	K1- 34534
Hyperlink is not displaying properly on announcements page in user portal.	K1- 34363
Dell Updates smart label creation takes a long time to complete.	K1- 34358
Unable to login to KACE GO app from ORG ID 20 or higher.	K1- 34217
Multiple emails are created when an API connectivity issue occurs.	K1- 34193
New asset's user-type field defaults to blank of unassigned.	K1- 33976
Agentless devices are shown under 'Device to install software on' in user portal.	K1- 33572
Patch Compliance by Machine shows inaccurate count for compliant devices.	K1- 33424
Special characters in label and label group names display HTML on Detail page.	K1- 33267
Script update via API unsets selected OS and 'Run on next connection if offline' options.	K1- 33193
Unable to export selected updates from Patch and Dell Updates Catalog with advance search.	K1- 33117
SAML - Unable to login when cert fails before monthly refresh.	K1- 33027
Device report with subtopic <i>Software Catalog - Inventory Executables</i> fails.	K1- 32783
Use AES encryption for AD SSO computer object.	K1- 32776
Disabled Patch Schedules show in Task Schedule.	K1- 32736
Inventory breaks from long running inventory task with aggressive inventory interval.	K1- 32710
Allow category name to be set via scripting API.	K1- 32366
Suppress the email sent to root by Cron Daemon.	K1- 35436
FileVault 2 inventory is sometimes incomplete on Apple devices with multiple drives containing a lot of partitions.	K1- 35481

# 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
Offline scripts do not execute properly per day of week schedule specified.	K1A- 4075
CVE-2024-23772/CVE-2024-23773 KACE Systems Management Appliance Agent can create or delete unintended files if user intentionally manipulated the user data directory.	K1A- 4074
CVE-2024-23774 KACE agent does not properly quote launching path in all cases.	K1A- 4073
vCenter Agentless inventory crashes if unable to obtain timezone information for ESXi host.	K1A- 4052
cURL and libcURL security vulnerabilities (CVE-2023-38545 & CVE-2023-38546).	K1A- 4050
Support dnf in addition to RPM install for RHEL.	K1A- 4044
Configurable konea tunnel timeout check for bootup MI.	K1A- 4036
Chassis type for some Mac devices show as other instead of desktop or laptop.	K1A- 4012
Enable support for Windows defender patches.	K1A- 3998
Agent does not connect when using clone prepping a VM template using custom VMware configuration.	K1A- 3953
Old KACE agent installers are not cleaned up during upgrade.	K1A- 3872

# Known issues

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

Known issue	Issue ID
Access denied for report user if reporting password has the '\$' character in any position other than the last character.	K1-35051
Location - Parent/Child relationship not set in ASSET_HIERARCHY after Import.	K1-20535
LDAP Org Filter LDAP browser button logs user out.	K1-20254
Importing Location Assets doesn't import with Parent-Child Relationship.	K1-32995

Known issue	Issue ID
Mac profile scripts show blank dependencies and task.	K1-35245
A warning regarding network interfaces appears in Mac 14 SNMP Agentless Inventory.	K1-34680
SDA 9.2 and below requires OpenSSL cipher hotfix to link with SMA 14.0.	K1-35480

## System requirements

The minimum version required for installing KACE Systems Management Appliance 14.0 is 13.2. 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 11.0. 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 14.0, 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/14.0-common-documents/technical-specifications-for-virtual-appliances/>.
- For KACE as a Service: Go to <https://support.quest.com/technical-documents/kace-systems-management-appliance/14.0-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 14.0 can be used only on KACE Systems Management Appliance running version 14.0 or later. Version 14.0 licenses cannot be used on appliances running earlier versions of the appliance, such as 12.0.



# 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 14.0 is 13.2. 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 11.0. 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.

- **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/14.0%20common%20documents/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 14.0. 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 14.0. 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/14.0%20common%20documents/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 14.0 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 14.0.

## 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/14.0%20common%20documents/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 14.0 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 14.0 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 14.0.

## 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](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/14.0/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/14.0-common-documents/technical-specifications-for-virtual-appliances/>.

**For KACE as a Service:** Go to <https://support.quest.com/technical-documents/kace-systems-management-appliance/14.0-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/14.0/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/14.0%20common%20documents/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 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](http://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

© 2024 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.