

Quest®



KACE® Systems Management Appliance 13.2

## Release Notes



# Table of Contents

<b>Quest® KACE® Systems Management Appliance 13.2 Release Notes</b> .....	<b>3</b>
About KACE Systems Management Appliance 13.2.....	3
New features.....	3
Deprecated features.....	3
Enhancements.....	3
Resolved issues.....	4
Resolved Service Desk issues.....	4
Resolved Server issues.....	5
Resolved KACE Agent issues.....	6
Known issues.....	7
System requirements.....	7
Product licensing.....	8
Installation instructions.....	8
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.....	11
More resources.....	12
Globalization.....	12
About us.....	12
Technical support resources.....	12
Legal notices.....	13

# Quest® KACE® Systems Management Appliance 13.2 Release Notes

---

This document provides information about the KACE Systems Management Appliance version 13.2.

## About KACE Systems Management Appliance 13.2

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/>. This maintenance release contains only resolved issues.

## New features

This release of the KACE Systems Management Appliance does not include any new features.

## Deprecated features

The following feature is no longer available as of this release:

- Upgrades on 13G hardware

The following features will be deprecated in a future release:

- Legacy approval method in KACE GO
- Scripting configuration policies
- Mac Profiles
- OVAL and SCAP

## Enhancements

The following enhancements are implemented in this release.

Enhancement issue	Issue ID
Urgent mode message to be displayed in more visible format.	K1A-3994
Upgrade to FreeBSD 13.2 and associated packages.	K1-34255
Upgrade to PHP 8.2.	K1-34172
Updated third-party components for PHP 8.2 support and remediation of security vulnerabilities.	K1-34165
Upgrade to MariaDB 10.6.	K1-34138
Certified Fedora Linux 38 for agentless support.	K1-34081
Certified Debian Linux 12 for agentless support.	K1-34079
Certified Ubuntu 23.04 for agentless support.	K1-34077
Added appliance shutdown/restart event to remote <code>syslog</code> .	K1-33990
Added the ability to run a size report from Diagnostic Utilities.	K1-33920

## 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 Service Desk issues resolved in this release.

Table 1. Resolved Service Desk issues

Resolved issue	Issue ID
Service Desk attachments with invalid file names could cause slowness due to failure to perform scan.	K1-34407
Service Desk attachments with line breaks or unsupported unicode characters caused TAR failure during backup.	K1-34402
Process Approval due date set incorrectly when multiple approval stages and business hours were enabled.	K1-34298
Email attachments were not added to the ticket if content disposition was not found.	K1-34232

<b>Resolved issue</b>	<b>Issue ID</b>
Ticket search did not return CC-ed user or submitter's tickets if the user was not a valid submitter for the queue.	K1-34082
Fixed issue where ticket change notifications no longer sent a list of ticket changes done within a minute, except for the last one.	K1-34078
Fixed issue where text file attachments sent over email were not being added to Service Desk tickets.	K1-34069
Fixed issue where default ticket template pre-defined fields were not populated when ticket was created by email.	K1-33747
Due Date was not set by default for process parent ticket with Due Offset.	K1-32697

## Resolved Server issues

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

Table 2. Resolved server issues

<b>Resolved issue</b>	<b>Issue ID</b>
Issues reported when a deleted organization could be referenced by software metering enabling/disabling process.	K1-34477
Disk space requirement calculations for appliance backups were inaccurate in certain scenarios.	K1-34401
Fixed auto renewal issue with Let's Encrypt SSL certificate.	K1-34395
Dell Warranty failed to update for some devices when Service Level Group was not returned.	K1-34391
SMTP server fields not displayed under <i>Enable SMTP Remote Server (Outbound Relay)</i> on the <i>Network Settings</i> page.	K1-34353
Fixed an issue where KScript log and <i>Run Now</i> status data was purged randomly when related table sizes exceeded the allowed thresholds.	K1-34269
Email <i>Test Connection</i> in <i>Network Settings</i> failed for on-premise Exchange configuration.	K1-34258
Backup file symbolic links could point to non-existent backup files.	K1-34254
Fixed issue with approval tab in User Console summary not showing all data.	K1-34252
Patch Catalog remained in the <i>Deleting Unused Patch Files</i> status without being able to complete the deletion.	K1-34242
Unable to login to KACE GO app from ORG ID 20 or higher.	K1-34217

Resolved issue	Issue ID
Munin graphs were not displayed due to permissions issue.	K1-34212
Fixed issue with asset archival due to deadlock situation when trying to get lock.	K1-34139
Fixed "no database selected" issue with <i>View By</i> in the <i>Managed Installations</i> list page.	K1-34091
Expired or weak MySQL certificate caused MySQL issues post-upgrade.	K1-34089
Patch schedule phase was not set properly when the <code>MAX_SIMULTANEOUS_PATCH</code> flag was enabled.	K1-34067
Previously mapped user SAML attributes were cleared for user on first log in after KACE SMA server upgrade.	K1-34004
Processor (CPU) inventory displayed in a single line, making it difficult to read.	K1-33963
Updated data tables to address CVE-2020-28458 and CVE-2021-23445.	K1-33932
It was not possible to enable SSL on a single-org appliance with monitoring Trap settings.	K1-33144
Empty inventory values <code>GATEWAY_IP</code> and <code>GATEWAY_IPV6</code> were constantly written to history at every inventory cycle.	K1-32627



**NOTE:** The option **Enable webserver compression** is removed from **Settings > Control Panel > Security Settings** in this release.

## 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
Agent tunnel creation failed and blocked agent connection for all devices.	K1A-4037
Agent made the boot up process longer than necessary due to boot up managed installations.	K1A-4029
Ubuntu devices with CRAN packages installed failed to complete inventory.	K1A-4028
All KACE macOS agent Munki files are now signed.	K1A-4018
Offline KScripts that run on a schedule looped indefinitely.	K1A-4002
Fixed issue with display/monitor reporting for macOS inventory.	K1A-3971
Fixed issue with macOS secondary video card inventory reporting.	K1A-3969

Resolved issue	Issue ID
Fixed issue with Linux CDRom inventory reporting.	K1A-3958

## Known issues

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

**i** | **NOTE:** Inventory of Agentless Ubuntu 21.04 devices fails for users who have a non-default shell of bash.

Known issue	Issue ID
Replication using UNC share does not work for macOS 14.	K1-34662
Agentless inventory of macOS 12 incorrectly shows two volumes mounted to '/.	K1-33162
Manually provisioning an SNMP device from <i>Discovery Results</i> page shows missing settings when SNMP walk is selected and that walk failed.	K1-33154
Nmap discovery type with TCP or UDP port scan options selected does not return opened ports.	K1-33005
Device Actions can sometimes fail when accessing them through a direct URL.	K1-32305
Login field does not update after user authenticates through SAML and the mapping was changed.	K1-32304
Large metering data can cause page to load slowly.	K1-32249
Managed Install snooze time is ignored. Snooze option does not reappear until next inventory interval.	K1-20832
Managed Install attempts used up during inventory when user alert is snoozed.	K1-20826

## System requirements

**i** | **NOTE:** Starting in version 13.2, 13G hardware is no longer supported.

The minimum size of the `/var`, `/tmp`, and `/usr` partitions is 12 GB. If the upgrade process detects that the size of these partitions does not meet these minimum requirements, it fails with a related message. A migration of backup files is required to a new virtual machine before you can proceed with the upgrade.

The minimum version required for installing KACE Systems Management Appliance 13.2 is 13.1. 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.

**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.

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

Before upgrading to or installing version 13.2, 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/13.2-common-documents/technical-specifications-for-virtual-appliances/>.
- For KACE as a Service: Go to <https://support.quest.com/technical-documents/kace-systems-management-appliance/13.2-common-documents/technical-specifications-for-kace-as-a-service/>.

### End of support for Dell 13G physical servers

13th Generation Dell PowerEdge R430 servers are no longer supported. Any attempts to upgrade the appliance using this hardware result in failure. Contact your KACE Sales Representative to plan for a migration to a virtual platform.

## 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.

**i** **NOTE:** Product licenses for version 13.2 can be used only on KACE Systems Management Appliance running version 13.2 or later. Version 13.2 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](#)

**i** **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 size of the `/var`, `/tmp`, and `/usr` partitions is 12 GB. If the upgrade process detects that the size of these partitions does not meet these minimum requirements, it fails with a related message. A migration of backup files is required to a new virtual machine before you can proceed with the upgrade.

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

- **Verify your KACE Agent version.**

The minimum version required for upgrading the KACE Agent is 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/13.2-common-documents/administrator-guide/>.

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

For appliances initially installed prior to version 7.0 that have not been re-imaged (physical appliances) or reinstalled (virtual), Quest Software strongly recommends exporting, re-creating (an image, or a virtual machine installation from an OVF file), and re-importing the database before upgrading to version 13.2. 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 13.2. 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/13.2-common-documents/administrator-guide/>.
2. Go to the appliance *Control Panel*:
  - If the **Organization** component is not enabled on the appliance, click **Settings**.
  - If the **Organization** component is enabled on the appliance: Log in to the appliance **System Administration Console**: [http://KACE\\_SMA\\_hostname/system](http://KACE_SMA_hostname/system), or select **System** in the drop-down list in the top-right corner of the page, then click **Settings**.
3. On the left navigation bar, click **Appliance Updates** to display the *Appliance Updates* page.
4. Click **Check for updates**.

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

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

Version 13.2 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 13.2.

## 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/13.2-common-documents/administrator-guide/>.
2. Using your customer login credentials, log in to the Quest website at <https://support.quest.com/kace-systems-management-appliance/download-new-releases>, download the KACE Systems Management Appliance server `.kbin` file for the 13.2 GA (general availability) release, and save the file locally.
3. On the left navigation bar, click **Appliance Updates** to display the *Appliance Updates* page.
4. In the *Manually Update* section:
  - a. Click **Browse** or **Choose File**, and locate the update file.

- b. Click **Update**, then click **Yes** to confirm.

Version 13.2 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 13.2.

## 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](http://KACE_SMA_hostname/system), or select **System** in the drop-down list in the top-right corner of the page, then click **Settings**.**
2. To verify the current version, click **Need Help** in the upper-right corner of the page, and in the help panel that appears, at the bottom, click the circled **i** button.

## Verify security settings

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

1. Go to the appliance *Control Panel*:
    - If the **Organization component is not enabled on the appliance, click Settings.**
    - If the **Organization component is enabled on the appliance: Log in to the appliance System Administration Console: [http://KACE\\_SMA\\_hostname/system](http://KACE_SMA_hostname/system), or select **System** in the drop-down list in the top-right corner of the page, then click **Settings**.**
  2. On the left navigation bar, click **Security Settings** to display the *Security Settings* page.
  3. In the top section of the page, change the following settings:
    - **Enable Secure backup files:** Clear this check box to enable users to access database backup files using HTTP without authentication.
    - **Enable Database Access:** Select this check box to enable users to access the database over port 3306.
    - **Enable Backup via FTP:** Select this check box to enable users to access database backup files using FTP.
- CAUTION:** Changing these settings decreases the security of the database and is not recommended.
4. Click **Save**.
  5. **KBIN upgrades only.** Harden root password (2FA) access to the appliance.
    - a. In the System Administration Console, click **Settings > Support**.
    - b. On the *Support* page, under *Troubleshooting Tools*, click **Two-Factor Authentication**.
    - c. On the *Support Two-Factor Authentication* page, click **Replace Secret Key**.
    - d. Record the tokens and place this information in a secure location.

# More resources

Additional information is available from the following:

- Online product documentation (<https://support.quest.com/kace-systems-management-appliance/13.2/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/13.2-common-documents/technical-specifications-for-virtual-appliances/>.  
**For KACE as a Service:** Go to <https://support.quest.com/technical-documents/kace-systems-management-appliance/13.2-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/13.2/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/13.2-common-documents/administrator-guide/> to view documentation for the latest release.

# Globalization

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

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

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

# About us

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

© 2023 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 - October 2023

Software Version - 13.2