

Quest®



KACE® Systems Management Appliance 13.0

Release Notes



Table of Contents

Quest® KACE® Systems Management Appliance 13.0 Release Notes	3
About KACE Systems Management Appliance 13.0.....	3
New features.....	3
Enhancements.....	4
Resolved issues.....	6
Resolved Service Desk issues.....	6
Resolved API issues.....	7
Resolved Reporting issues.....	7
Resolved Server issues.....	8
Resolved KACE Agent issues.....	9
Known issues.....	9
System requirements.....	10
Product licensing.....	10
Installation instructions.....	11
Prepare for the update.....	11
Update the KACE Systems Management Appliance server using an advertised update.....	12
Upload and apply an update manually.....	13
Post-update tasks.....	13
Verify successful completion.....	13
Verify security settings.....	14
More resources.....	14
Globalization.....	15
About us.....	15
Technical support resources.....	15
Legal notices.....	15

Quest® KACE® Systems Management Appliance 13.0 Release Notes

This document provides information about the KACE Systems Management Appliance version 13.0.

About KACE Systems Management Appliance 13.0

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/>. This release contains a number of new features, resolved issues, and security enhancements.

New features

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

- **Actionable User Notifications:** A wide range of predefined notification configurations are now included with the appliance. Several available categories focus on your environment's specific aspects, such as Security or Patching. When you review triggered notifications, background colors indicate the alert severity: info (blue), warning (yellow), warning (red). Some notifications include actionable links allowing you to drill down to the object associated with the notification. For example, if you see a license expiration notice, the link in the notification takes you directly to the license instance that is about to expire.



NOTE: Information from the Alert section on the *Dashboard Detail* page moved to the Notification pane. A *server upgrade is available* alert still uses a dashboard summary alert and not the new user notification system.

- **Simplified Software Uninstallation:** You can now quickly either add or remove a Software Catalog item from a Managed Installation using the *Software Catalog Detail* page.
- **Let's Encrypt Easy Certificate Management Integration:** Let's Encrypt is a free, automated, open certificate authority (CA). When you get a certificate from Let's Encrypt, their servers validate that you control the domain names in that certificate using a challenge. You must have a Let's Encrypt account registered in the unlikely event the certificate expires.
- **Google Workspace Authentication Integration:** The appliance can authenticate users using Google Workspace credentials starting in this release. This process is leveraged in Inventory, Distribution,

Scripting, and Service Desk. The following appliance-managed components can be authenticated through Google API:

- **Google Workspace Device Discovery and Inventory:** This includes both Chromebooks and mobile devices managed by a Google Workspace Domain (formerly *G Suite*).
- **Service Desk Queue Inbound Email:** This includes email accounts that are part of a Google Workspace or a public Gmail account.
- **Service Desk Attachment Virus Scanning:** The appliance now includes a malware scanning feature for Service Desk file attachments. This automated process ensures that the virus definition lists are updated regularly. All ticket attachments will be scanned before they are added to the tickets. Manage Quarantined files through the *Antivirus Quarantine* page. Use this page to review and manage quarantined Service Desk attachments. A notification appears when a threat is detected, with a link to the device associated with the file. You can also create notifications when specific kinds of threats are detected or based on their status change.
- **Service Desk Attachment Distribution through email:** The appliance can now send files attached to the ticket instead of providing file links. You can also add file attachments to email templates when needed.



NOTE: Minimum memory requirements to run (or upgrade a 12.1 system) to 13.0 have changed. A minimum of 8 Gb is required to successfully operate the appliance. Also, monitoring is now supported for managed macOS 12.0 devices. For more details, see the *Technical Specifications*.

Enhancements

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

Enhancement	Issue ID
Agent support for Windows 10 22H2.	K1A-3959
Agent support for Red Hat Enterprise Linux 9.	K1A-3945
Agent support for Windows 11 22H2.	K1A-3944
Support for Microsoft System Center Virtual Machine Manager and Hyper-V 2022.	K1A-3931
Agent support for Raspbian Linux 11 (Bullseye).	K1A-3923
Agentless support for macOS 13 Ventura.	K1A-3922
Agent support for macOS 13 Ventura.	K1A-3921
Agent support for Ubuntu 22 LTS.	K1A-3913
Konea module security enhancements.	K1A-3909
Linux package upgrades: Ability to pull repository information from the <code>sources.list.d</code> directory.	K1A-3903
Added DirectX version to inventory data.	K1A-3898
Agentless support for Red Hat Enterprise Linux 9.	K1-33030

Enhancement	Issue ID
Agentless support for Windows 11 22H2.	K1-33028
Agentless support for Raspbian Linux 11 (Bullseye).	K1-32835
Added logical disks to Dell Data Protection Encryption inventory on Windows.	K1-32746
Migrated Google OAuth support for Google Workspace Integration.	K1-32682
Added ticket history for deleted Service Desk tickets.	K1-32646
Agentless support for openSUSE Leap 15.4.	K1-32604
Agentless support for Fedora 35 and 36.	K1-32603
Agentless support for Ubuntu 22 LTS.	K1-32602
Ability to limit system generated approval workflow comments to owners only.	K1-32547
Added ability to create a managed uninstall directly from the SW Catalog Detail Page using a Add Managed Uninstall button.	K1-32530
The TLS 1.2 ciphers are adjusted to provide the highest possible security rating while maintaining client compatibility.	K1-32476
Added a link to the Microsoft Defender Advanced Threat Protection console to the Microsoft Defender section on the <i>Device Detail</i> page, when applicable.	K1-32422
<i>My Recent Sessions</i> pop-up includes country, if available.	K1-32412
Updated User Notification system to forward new notifications to push server.	K1-32277
Added ability to remove incoming SMTP capability from appliance.	K1-32096
Removed framesets from the Administrator Console, System Administration Console, and User Console .	K1-30094
Drop-down fields (<i>Category, Impact, Priority, and Status</i>) can be left blank when required	K1-22073

Resolved issues

This section contains the issues resolved in this release:

- [Resolved Service Desk issues](#)
- [Resolved API issues](#)
- [Resolved Reporting 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
A new ticket from email could show a blank title and summary.	K1-33146
Ticket did not get created when more than one address was added in the To or CC field using Gmail OAuth.	K1-32862
The ticket title from the email subject field in some cases was encoded twice in UTF-8.	K1-32781
Ticket <i>Reassign To</i> owner ticket counts included closed state tickets .	K1-32750
<i>Ticket List Queue</i> drop-down was empty when user Locale is set to French (France)	K1-32739
When logging in, a blank screen sometimes appeared, requiring a page reload.	K1-32711
Ticket search did not return CC-ed user or submitter's tickets if user was not a valid submitter for the queue.	K1-32699
User downloads approval request ticket <i>Summary</i> field was blank.	K1-32694
Physical to virtual backup migration preserved any physical card network settings.	K1-32692
Tickets made from templates did not always show parent info on the ticket list.	K1-32680
The <i>Patch Schedules</i> list page could be slow to load.	K1-32575
Asset History entries could be missing from configuration.	K1-32554
Updating ticket category field through email failed if category name contained underscore.	K1-32553

Resolved issue	Issue ID
Tickets: Commentor not added to CC list when only clicking Save or Apply Changes .	K1-32533
Single quote in ticket title was not displayed correctly in email sent from <i>Ticket Detail</i> page.	K1-32514
Service Desk Reporting: Approver information was not shown on parent process tickets.	K1-32496
Default Custom View caused Submitter Ticket History link to redirect to inaccurate list page results.	K1-32481
Service Desk: Closing ticket on list page with Satisfaction Survey required resulted in an error.	K1-32454
Process approval timeout did not calculate as expected.	K1-32452
Queue email addresses in the To field was copied in the CC list (when using SMTP).	K1-32417
The timestamp on Service Desk announcements were not updating after modification	K1-32237
Updating ticket custom field through email by label name failed if label name contained space and underscore.	K1-31767



NOTE: The *Ticket Detail* page allows the browser to auto-complete the Title field when creating new tickets, if KB article suggestions are disabled. However, if a password manager is linked to the browser, the browser's auto-complete option is typically disabled.

Resolved API issues

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

Table 2. Resolved API issues

Resolved issue	Issue ID
Get owned queues API returned incorrect queue count.	K1-33322
The appliance API <code>GET /api/inventory/machines/</code> did not include <code>gateway_ip</code> <code>gateway_ipv6</code> .	K1-32675

Resolved Reporting issues

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

Table 3. Resolved Reporting issues

Resolved issue	Issue ID
An SQL error could be seen when generating report from archived ticket list advanced search.	K1-32644
Reporting: Special characters were incorrectly displayed in PDF reports generated in foreign language browser.	K1-32541
Scheduled XLS reported error with The file format and extension of '<filename.xls>' don't match.	K1-17412

Resolved Server issues

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

Table 4. Resolved server issues

Resolved issue	Issue ID
Could not save Managed Install with empty <i>Devices</i> field when logged-in user's role had Device Scope Label applied.	K1-32771
When logging in, a blank screen sometimes displayed, requiring a page reload.	K1-32711
Physical to virtual backup migration preserved any physical card network settings.	K1-32692
Restoring backup from the setup wizard did not always correctly set the DB time-zone.	K1-32688
The <i>Patch Schedule</i> list page may be slow to load.	K1-32575
FileVault encryption was missing Conversion Status/Percentage and Encryption Status/Type.	K1-32568
Asset History entries could be missing from configuration.	K1-32554
Computer Inventory: Inventory failed when unknown characters existed in Machine Process.	K1-32551
Patch Download: Failed payload download shows updated when last payload succeeded.	K1-32540
Attachments of type <i>.eml</i> or <i>.msg</i> were missing from tickets submitted by email.	K1-32111
Monitoring: Log Profile alerts did not create tickets.	K1-21174



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 5. Resolved KACE Agent issues

Resolved issue	Issue ID
macOS installer prompted user to install Rosetta on Mac with Apple silicon (M1/M2) chip.	K1A-3942
Agents were going offline after failing to update the Konea certificate after it had expired.	K1A-3934
Process names could be reported incorrectly in inventory for Linux.	K1A-3914
Offline Scripts looping due to DST change.	K1A-3906

Known issues

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



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

Known issue	Issue ID
Performing a search in the quarantine device list may not work as expected.	K1-33719
Server: API requests that do not provide a user agent header always fail.	K1-33709
Creating a report that includes the <i>Number of Records Analyzed</i> may produce an error when running the report.	K1-33707
Expired software license asset user notifications are generated for licenses with no expiration date set.	K1-33702
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

Known issue	Issue ID
Large metering data can cause page to load slowly.	K1-32249
Schedule info does not show correctly after disabling a Linux Package Upgrade Schedule.	K1-30725
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

The minimum version required for installing KACE Systems Management Appliance 13.0 is 12.1. 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.



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 13.0, 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/13.0-common-documents/technical-specifications-for-virtual-appliances/>.
- For KACE as a Service: Go to <https://support.quest.com/technical-documents/kace-systems-management-appliance/13.0-common-documents/technical-specifications-for-kace-as-a-service/>.

End of support for Dell 12G physical servers

11th and 12th Generation Dell PowerEdge (R610/R410/R420) 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.



NOTE: Product licenses for version 13.0 can be used only on KACE Systems Management Appliance running version 13.0 or later. Version 13.0 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 13.0 is 12.1. 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 **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/13.0-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 13.0. For complete information, visit <https://support.quest.com/kace-systems-management-appliance/kb/111810/how-to-re-image-the-k1000-appliance>.

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

There are many reasons why you should re-image the appliance. The new disk layout, for example, offers better compatibility with version 13.0. It also features better security and performance.

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

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

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

Update the KACE Systems Management Appliance server using an advertised update

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



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

1. Back up your database and files. For instructions, see the **Administrator Guide**, <https://support.quest.com/technical-documents/kace-systems-management-appliance/13.0-common-documents/administrator-guide/>.
2. Go to the appliance *Control Panel*:
 - If the **Organization** component is not enabled on the appliance, click **Settings**.
 - If the **Organization** component is enabled on the appliance: Log in to the appliance **System Administration Console**: `http://KACE_SMA_hostname/system`, or select **System** in the drop-down list in the top-right corner of the page, then click **Settings**.
3. On the left navigation bar, click **Appliance Updates** to display the *Appliance Updates* page.
4. Click **Check for updates**.

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



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

Version 13.0 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 13.0.

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/13.0-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 13.0 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 **Update**, then click **Yes** to confirm.

Version 13.0 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 13.0.

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 **Need Help** in the upper-right corner of the page, and in the help panel that appears, at the bottom, click the circled **i** button.

Verify security settings

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

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

More resources

Additional information is available from the following:

- Online product documentation (<https://support.quest.com/kace-systems-management-appliance/13.0/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/13.0-common-documents/technical-specifications-for-virtual-appliances/>.
For KACE as a Service: Go to <https://support.quest.com/technical-documents/kace-systems-management-appliance/13.0-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/13.0/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/13.0-common-documents/administrator-guide/> to view documentation for the latest release.

Globalization

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

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

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

About us

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

Technical support resources

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

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

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

Legal notices

© 2022 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 2022

Software Version - 13.0