KACE® Systems Management Appliance 12.0

Release Notes

Table of Contents

Quest® KACE® Systems Management Appliance 12.0 Release Notes

This document provides information about the KACE Systems Management Appliance version 12.0.

About KACE Systems Management Appliance 12.0

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.

> **NOTE:** This is the only document that is translated for this release, however the localized variants do not include information about resolve issues, enhancements, and known issues. Other guides, such as the *Administrator Guide* and in-product help are not localized at this time, and version 10.2 documents are included.

New features

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

Infrastructure

- **Azure and AWS S3 storage support**: You can now configure the appliance to use cloud-based off-board backup such as the Microsoft Azure Blob and Amazon S3 storage. This requires an MS Azure or Amazon S3 storage account, as applicable.
- **Ability to change the name of the admin user**: If your environment includes multiple appliances, you can simplify and speed up periodic administrative changes to comply with your security policies. The name of the default admin account can be easily changed, however use caution when changing the login and password of the admin account. The `admin` account login names and passwords on all linked appliances

and organizations must be the same if you want to switch between them using the drop-down list in the top-right corner.

- **Administrative user security enhancements**: The local `admin` account can now be disabled or renamed, as needed.
- **Changing default configuration passwords**: Starting in this release, you can easily change the passwords of the default service accounts, such as `konfig`/`konfig` and `netdiag`/`netdiag`.
- **Scalability enhancements**: The appliance now allows you to manage up to 50K devices using the default configuration.
- **FreeBSD 12.2**: FreeBSD included with the appliance is updated to version 12.2, that addresses a number of security advisories.
- **LDAP/SAML for the System Administration Console**: LDAP support is now extended to the **System Administration Console**. It allows a user to access the **System Administration Console** using an LDAP profile, and to access each organization's **Administrator Console** as an administrator with full read/write permissions.
- **Initial Setup wizard enhancements**: The *Initial Setup* wizard now allows you to restore the appliance data from a backup, and to re-set network configuration, as needed.
- **Ability to exclude network settings from a restore job**: Backup, restore, and migration processes often run in multiple environments, such as testing and development. It is often required for both target and destination devices to remain online. The restore process now have the option to exclude network settings, allowing the appliance administrator to keep selected devices online.
- **Nutanix support**: The appliance can now be hosted on Nutanix. Note that Nutanix support for Guest Tools on FreeBSD is not supported at this time, so certain Nutanix features such as VSS (snapshot), self-service restore, and VM Mobility are not available.

Device communications

- **Native M1-Series CPU Agent for macOS**: Starting in this release, the KACE Agent can run natively on Apple Silicon (M1) chips.
- **macOS 12.0 (Monterey) support**: The appliance now supports endpoints running macOS 12.0. Monitoring is not supported on this OS. For a full list of OS requirements for agent-managed devices, see the *Technical Specifications for Virtual Appliances*.

Service Desk

- **Knowledge Base articles suggested at ticket creation**: As you create a Service Desk ticket, a list of suggested knowledge base articles appears based on the information provided in the ticket.

  Ticket import tool: The appliance now includes a custom mapping capability to import tickets from external systems, to allow you easily migrate your tickets from another system.

Enhancements

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

> **NOTE:** The appliance API now supports API clients that use `x-kace-api-version` and `x-kace-csrf-token` headers when communicating with the appliance. However, older clients that use `x-dell-api-version` and `x-dell-csrf-token` are still supported, as long as they include the `x-dell-api-version` request header in the login request. Please note that the method of communicating using the old Dell headers is now deprecated, and will be removed in a future release.

Enhancement	Issue ID
KACE Agent is supported natively for macOS devices with Apple silicon chip.	K1A-3783

Enhancement	Issue ID
KACE Agent system tray shortcuts now support a list of default KACE specific replacement variables.	K1A-707
KACE Agent only supports 64-bit Linux operating systems for RHEL, Ubuntu, SUSE, and CentOS.	K1-31940
Patch status now changes to *Active* if a previously superseded patch is no longer superseded.	K1-31917
Global Administrator role is added to the **System Administration Console**.	K1-31910
Last inventory processing time for each device is now available on the *Device Details* page.	K1-31828
Samba-enabled boxes now have a method of disabling guest access.	K1-30808
10.x KACE Agents no longer connect to the KACE Systems Management Appliance Server. All agents must be upgraded prior to upgrading the appliance to version 12.0. See Prepare for the update.	K1-30178
Changes to ticket rules are now logged in object settings history.	K1-22114

Resolved issues

This section contains the issues resolved in this release:

- Resolved Service Desk issues
- Resolved KACE Agent issues
- Resolved Inventory issues
- Resolved Security issues
- Other resolved 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
Requiring 2FA (two-factor authentication) for the **Administrator Console** could cause unexpected behavior with ticket creation from the **User Console**.	K1-32102
In the Service Desk *Tickets* list page, sorting by category did not behave as expected.	K1-31939
System message in ticket process comment could display HTML content.	K1-31938

Resolved issue	Issue ID
Conditional Logic did not behave as expected with check boxes.	K1-31928
In Service Desk *Ticket Templates*, Conditional Logic did not work as expected for the *Category* field.	K1-31907
Error message could be seen when converting a ticket to a process.	K1-31893
When using the text editor and adding a link with the option to open it on a new tab did not behave as expected.	K1-31886
In a queue with SMTP inbound email, any emails from users with a comma in the display name showed up in the ticket as deleted users.	K1-31874
Changing screen label for Service Desk queue to include apostrophe caused the label to include ASCII code.	K1-31830
Child ticket submitter was set to parent ticket's submitter instead of the logged-in user when creating a ticket using a process.	K1-31797
Accented letters in the subject of an email sent to a Service Desk queue were replaced with question marks '?'.	K1-31784
When adding an image during ticket creation, the image was not always saved, as expected.	K1-31779
Users with no queue permissions were not able to see tickets they are copied on.	K1-31710
A double space in an email sometimes did not appear as expected in a Service Desk ticket.	K1-30843
Queue Email notifications were not working for approvers if they were not also ticket owners.	K1-30815
Pasting an image into a Knowledge Base article caused other pasted images to reset alignment and justification.	K1-30721
Ticket Archive: *Owners Only* comments were not visible after a ticket was archived	K1-30652
Service Desk Custom View was inaccurate for *All Queues* if permissions were limited in one of the queues.	K1-30608
Ticket ID could not be found in a search using the *All Queues* view.	K1-30606
User Download did not show in the user portal when restricting by device label.	K1-20682
Ticket was not added to process ticket table on using **Save and Create Child** button from the process child ticket.	K1-19052

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
Agent alert message was seen for skipped tasks with no way of preventing or permanently hiding them. This will be reintroduced in a future version as an optional feature.	K1A-3871
Offline scripts with the **Also run once at next client checkin** option selected failed to run.	K1A-3843
KACE Agent could fail to run Powershell scripts during inventory if script execution policy is disabled by default on non-English OS.	K1A-3842
KACE Agent returned `Core.0` as part of the OS name on CentOS.	K1A-3841
KACE Agent Client Certificate handshake failed when another Konea certificate was imported by an external tool.	K1A-3840
macOS KACE Agent was instructed to download bad path when triggered to run with command only during Software Catalog-based managed installation.	K1A-3815
Windows 10 20H2 and 21H1 were reported by their display version instead of the technical version of 2009.	K1A-3803
An expected reboot could cause a patching task to enter an error state.	K1A-467

Resolved Inventory issues

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

Table 3. Resolved Inventory issues

Resolved issue	Issue ID
Age column on the *Quarantine* list page did not sort correctly.	K1-30818
In rare situations, machine deletion could fail and produce unexpected results.	K1-30770
Quarantine record is hidden from the organization if the device is moved to another organization.	K1-29987
Performance degradation seen on the *Software Detail* page when the software was associated with large number of devices.	K1-20576

Resolved Security issues

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

Table 4. Resolved Security issues

Resolved issue	Issue ID
Downloading and *Paused* columns on the *Patch Schedules* list page were not showing expected data.	K1-31926
Dell Updates: *Custom View* did not report any results when Smart Label was a criteria.	K1-31860
All Linux machines in inventory (including v.11.0 KACE Agents) were included in the *Linux Package Upgrade Schedules* list before a schedule is run.	K1-31836
Windows Feature Update Catalog Installed, *Missing*, and *Error* counts did match the device list results.	K1-31819
Windows Feature Update *Detect, Stage and On-demand Deploy* schedule was not processing the correct output when files were not staged on the agent machine.	K1-31766
Permission was denied when a read-only user attempted to **Show Labels** on the *Patch Catalog* and *Dell Update Catalog* list pages.	K1-31750
Duplicating a patch schedule from a list of schedules did not work as expected.	K1-31714
Duplicating a Dell Update schedule from list of schedules did not work as expected.	K1-31713
Performance could degrade when doing an *Advanced Search* on the *Patch Catalog* list page.	K1-29975

Other resolved issues

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

Table 5. Other resolved issues

Resolved issue	Issue ID
Reset Tries button was disabled on *Device Details* page for patches and Dell Updates.	K1-31900
Extra rows could be seen when CSV reports were created.	K1-31885
Built-in report *Label Associations* did not work as expected	K1-31884
Patch Smart Labels with the *Operating System* field set to *Mac* did not include "Big Sur".	K1-31871

Resolved issue	Issue ID
Performance issues were seen for agent connections after server restart for large deployments.	K1-31864
Windows Feature Update task displayed as successful when still running in a task chain.	K1-31794
For KACE GO, non-administrative queue owners could not set ticket device/asset to arbitrary device.	K1-31764
Duplicating ticket with custom field could fail from the User Portal.	K1-30856
Dashboard's *Managed Operating Systems Widget* results could be inaccurate.	K1-30813
Patching step with reboot in *Task Chain* incorrectly showed failed status.	K1-30812
During LDAP Import, *Additional Emails* could get overwritten if not mapped.	K1-30713
Package download process incorrectly updated offline last modified instead of last update status.	K1-30588
Importing LDAP users could unintentionally block attributes from mapping, that the administrator specifically listed under *Attributes to retrieve*.	K1-30083
Wizard report for *Asset - License* could return incorrect results.	K1-21350
License asset *Custom View* and *Advanced Search* could prevent some columns from displaying values.	K1-21342
Reporting: Special characters in the ticket *Title*, *Summary*, and *Comments* showed up incorrectly in report.	K1-21140
Read Only Administrators could not export assets.	K1-21096
It was not possible to manually update the *Additional Emails* field.	K1-21084
User *Custom Field* label was not used in column selector drop-down on the *Users* list page.	K1-20763
Edit Report wizard that uses Asset Subtype could display duplicate entries.	K1-20415
Advanced Search in the *Assets* list page could cause columns to be hidden, which also affected export.	K1-20059

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 dash.

Known issue	Issue ID
When accessing user portal Downloads items, the preselected device is not the current device when using Firefox and SSL.	K1A-3874
KMenu utility does not work on Windows 7 and Windows Server 2008 R2 unless .NET framework 4.5 is installed.	K1A-3864
The Scripting API fails to create or update an existing script.	K1-32195
Approver, Category CC user unable to add comment through email if queue submitter is restricted.	K1-32173
In the *Devices* list, export of CSV fails when the Client Version column is sorted.	K1-32164
Duplicating replication share configuration allows same replication device to be saved.	K1-32128
Asset import preview shows asset IDs instead of the name of the asset.	K1-32090
ZFS-mounted file system is not represented correctly with Agentless inventory. This primarily affects FreeBSD.	K1-31824

System requirements

The minimum version required for installing KACE Systems Management Appliance 12.0 is 11.1. 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 12.0 version of the appliance, you must obtain and install the KACE Agent 11.1 KBIN file that is signed with the 12.0 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 12.0, 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/12.0-common-documents/technical-specifications-for-virtual-appliances/.
- For KACE as a Service: Go to https://support.quest.com/technical-documents/kace-systems-management-appliance/12.0-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 12.0 can be used only on KACE Systems Management Appliance running version 12.0 or later. Version 12.0 licenses cannot be used on appliances running earlier versions of the appliance, such as 11.0.

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 12.0 is 11.1. 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 12.0 version of the appliance, you must obtain and install the KACE Agent 11.1 KBIN file that is signed with the 12.0 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/12.0-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 12.0. 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 12.0. 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/12.0-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 12.0 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 12.0.

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/12.0-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 12.0 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 12.0 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 12.0.

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/12.0/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/12.0-common-documents/technical-specifications-for-virtual-appliances/.
For KACE as a Service: Go to https://support.quest.com/technical-documents/kace-systems-management-appliance/12.0-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/12.0/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/12.0-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

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.**

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

KACE Systems Management Appliance Release Notes

Updated - November 2021

Software Version - 12.0