KACE® Systems Management Appliance 12.1

Release Notes

Table of Contents

Quest® KACE® Systems Management Appliance 12.1 Release Notes

This document provides information about the KACE Systems Management Appliance version 12.1.

About KACE Systems Management Appliance 12.1

KACE Systems Management Appliance is designed to automate device management, application deployment, patching, asset management, and Service Desk ticket management. For more information about KACE Systems Management Appliance series, go to https://www.quest.com/products/kace-systems-management-appliance/. 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.

Service Desk

- **Bulk Ticket Update Wizard**: Do you need to update multiple tickets with the same data? With the new *Bulk Ticket Update Wizard*, you can update multiple fields across multiple tickets using an intuitive user interface.
- **Searchable Queue List**: Starting in this release, use a searchable list of queues when you want to move a ticket to a different queue. This is useful if you have a long list of queues and need to find the correct one quickly.

Other

- **Appliance Bell Notifications**: Knowing everything going on at an appliance level can be overwhelming. With the introduction of our Appliance Bell Notification system administrators can track the health of the appliance easier than ever before and open the door to endless possibilities in future appliance releases.
- **Windows Defender Integration**: Windows Defender integration allows administrators to quickly review the current state of Windows Defender through the *Device Details* inventory view. Additionally, administrators can perform Windows Defender actions such as initiating a scan, updating signatures, and enabling one-click Windows Defender.
- **Current Session Tracking**: Part of securing your system is knowing who is accessing it and from where. This is now possible by downloading or importing the latest MaxMind Geolocation database file and

importing it to your appliance, that instantly empowers you with this critical information through our Current Session Tracking.

- **Windows 11 Readiness Report**: Are you tasked with preparing for a Windows 11 upgrade and are unsure whether your hardware is ready? By taking advantage of the new built-in *Windows 11 Readiness Report*, you can quickly identify how prepared you genuinely are.
- **Platform support updates**: The appliance now supports macOS 12.3 and Windows 11 IoT Core Enterprise.

Enhancements

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

Enhancement	Issue ID
Windows 11 readiness report is now built into the appliance.	K1-32308
The appliance now includes an API that reports `HD_SERVICE` records for process tickets.	K1-32293
Ability to turn KB suggestions on or off per queue is added in this release.	K1-32257
The Date Ticket Created field is added to the *Device Details* page.	K1-32248
Script name is clickable in *Run Now Status* to get back to script editing.	K1-32242
It is now possible to use `Message-ID` (as an alternate option) to thread email replies to a ticket.	K1-32221
Separate new ticket email notification is added for queue owners and submitters.	K1-32200
Errors appear in red text in the provisioning log to call out the errors for better visibility.	K1-32136
Option to turn off ability for child to close parent ticket is added.	K1-32130
Ticket template supports the *Required* field with *Conditional Logic*.	K1-31843
Ability to view active and recent sessions is added to the appliance.	K1-31741
Duplicate device detection is improved to add more flexibility.	K1-29740
Label can be created based on the Dell Update Package `MODEL_NUMBER` field.	K1-29612
Update status field is added to the *Update Agent Settings* page, to reflect the date when the new bundle is applied and the bundle version.	K1-20326

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
Service Desk Tickets: Russian Cyrillic characters were not shown in the Summary and Comments when using Russian encoding.	K1-32437
Parent tickets that used process status workflow displayed close parent option.	K1-32346
Not allowed email sometimes failed to send correctly when submitter had display name with multiple quotes.	K1-32325
Ticket templates: Conditional Logic fields could disappear after ticket is created.	K1-32319
Service Desk emails received through SMTP containing special characters inside a quoted string could fail to create tickets.	K1-32317
Service Desk ticket templates: Notes field type did not honor set column width.	K1-32246
It was not possible to search Service Desk queue subcategory if name matches partial or entire category name.	K1-32233
Approver, Category CC user could not add comments by email if queue submitter is restricted.	K1-32173
Non-admin queue owner could not to view image link on ticket update email.	K1-32169
Adding attachment to ticket, emailing ticket and adding another attachment resulted in duplicate history rows in **User Console**.	K1-32168
Ticket change description did not honor user's locale.	K1-32134
It was not possible to search for tickets when adding parent or child if the ID had five or more digits.	K1-31927

Resolved issue	Issue ID
Service Desk Dashboard widgets involving owners greater than ten lost intended value.	K1-31919
Service Desk merged tickets unmerged when the survey was submitted through **User Console**.	K1-31815
Email attachment (.eml, .msg file format) were marked as discarded when the subject contained slashes.	K1-31786
Email addresses in the *To* field of an email were not added to ticket CC list.	K1-30768
Saving or applying changes after adding an attachment through Submit added the attachment again.	K1-22607

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 could fail to run PowerShell scripts during inventory if script execution policy was disabled by default on non-English OS.	K1A-3897 K1A-3890
macOS agent could fail to create `amp.conf` due to debug assertion.	K1A-3886
Windows devices now more reliably report battery charge cycle count in *Device Details*.	K1A-3883
Safeguard OS install date field for devices where the computer date was set incorrectly (before 1970).	K1A-3882
On-demand patch deployment is now prevented if agent is not connected to the appliance.	K1A-3870
KACE Agent and agentless inventory could report different Microsoft Edge version.	K1A-3867
Linux inventory could report incorrect memory information.	K1A-3866
Special characters could appear in software inventory for executable's version number.	K1A-3857
Agent communication now ignore proxy set by the `HTTP_PROXY` environment variable.	K1A-3854
Agent MSI installer did not allow removal without entering server name and token.	K1A-3853
`inventory.xml` could be locked by `powershell.exe` during inventory process, resulting in upload failure.	K1A-3822

Resolved issue	Issue ID
SNMP field data was empty when the data contained 2 characters that could be hexadecimal.	K1-32211
macOS 11 (Apple M1 chip) agentless inventory did not show BIOS version and BIOS manufacturer.	K1-32149
Support is included for `AMPctl` and `AMPAgentBootup` to run as non-root on status command.	K1-21190

Resolved Inventory issues

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

Table 3. Resolved Inventory issues

Resolved issue	Issue ID
Software Inventory: Sorting by last user under detail page caused error.	K1-32318
Modifying labels from *Device Details* could remove the machine from patch schedule	K1-32315
Export All resulted in error page when using advanced search with an external agent.	K1-32272
Asset subtype was not saved when updating an existing SNMP agentless device.	K1-32217
In the *Devices* list, CSV export failed when the *Client Version* column was sorted.	K1-32164
Failure to evaluate filters (Smart Labels) when `inventory.xml` was uploaded manually for agentless devices resulted in error page.	K1-20269
Invalid filters (Smart Labels) could be saved, resulting in Smart Labels that were never populated.	K1-20268

Resolved Security issues

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

Table 4. Resolved Security issues

Resolved issue	Issue ID
Patch Smart Label targeting specific operating systems did not behave as expected after upgrade to 12.0.	K1-32340
Saving a patch schedule with special characters in messages showed escape characters when reopening.	K1-32119
The OVAL catalog list page did not display a Reference value unless it started with `CVE` or `CAN`.	K1-31912

Resolved issue	Issue ID
Samba was inaccessible when *Microsoft Network Client: Digitally Sign Communications (always)* was enabled.	K1-30670
When the Agent time zone changed, the OS install date changed resulting in the reset of patching results.	K1-20895

Other resolved issues

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

Table 5. Other resolved issues

Resolved issue	Issue ID
Replication shares did not consider locale when determining what Windows Feature Update files to replicate.	K1-32291
Under high loads, processing patch detection results could cause administrative interface to suffer and inaccurate detect results.	K1-32281
The credential entered for v3 SNMP Trap monitoring produced unexpected results when the password contained special characters.	K1-32265
The Asset Import preview could display values in incorrect columns.	K1-32253
The Scripting API could fail to create or update an existing script.	K1-32195
Asset name was left blank after agentless inventory of co-managed KACE Cloud Mobile Device Manager (MDM).	K1-32180
Monitoring: Log Enablement Packages (LEP) Installation failed when replacing existing LEP on an Agent-managed device.	K1-32152
Asset import preview showed asset IDs instead of asset names.	K1-32090
Windows 11 was missing from OS picker when creating a new script.	K1-31922
Error appeared when attempting to create an online-KScript from API.	K1-31897
Missing fields for *Patch Download Settings* in the **System Administration Console**, under **Settings** > **History** > **Settings**.	K1-30646
Adding new asset field could cause scheduled imports to import incorrectly.	K1-21353

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
Default Custom View causes *Submitter Ticket History* link to redirect to inaccurate list page results.	K1-32481
Service Desk: Closing a ticket on list page with `SAT_SURVEY` required results in an error.	K1-32454
A new SMA Agent Bundle is available alert does not use the new notification system.	K1-32435
When accessing the user portal *Downloads* items, the preselected device is not the current device when using Firefox and SSL.	K1-32314
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
Attachments of type `.eml` or `.msg` are missing from tickets submitted by email.	K1-32111
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
Task chain status on the *Task Chain Detail* page is inaccurate.	K1-20270

System requirements

The minimum version required for installing KACE Systems Management Appliance 12.1 is 12.0. If your appliance is running an earlier version, you must update to the listed version before proceeding with the installation.

The minimum version required for upgrading the KACE Agent is 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 12.1, make sure that your system meets the minimum requirements. These requirements are available in the KACE Systems Management Appliance technical specifications.

- For virtual appliances: Go to https://support.quest.com/technical-documents/kace-systems-management-appliance/12.1-common-documents/technical-specifications-for-virtual-appliances/.
- For KACE as a Service: Go to https://support.quest.com/technical-documents/kace-systems-management-appliance/12.1-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 12.1 can be used only on KACE Systems Management Appliance running version 12.1 or later. Version 12.1 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 12.1 is 12.0. If your appliance is running an earlier version, you must update to the listed version before proceeding with the installation.

To check the appliance version number, log in to the **Administrator Console** and click **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/12.1-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 12.1. 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 12.1. 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/12.1-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 12.1 is applied and the KACE Systems Management Appliance server restarts. Progress appears in the browser window and in the **Administrator Console**.
6. When the server upgrade finishes, upgrade all of your agents to version 12.1.

Upload and apply an update manually

If you have an update file from Quest, you can upload that file manually to update the KACE Systems Management Appliance server.

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

1. Back up your database and files. For instructions, see the **Administrator Guide**, https://support.quest.com/technical-documents/kace-systems-management-appliance/12.1-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 12.1 GA (general availability) release, and save the file locally.
3. On the left navigation bar, click **Appliance Updates** to display the *Appliance Updates* page.
4. In the *Manually Update* section:
   a. Click **Browse** or **Choose File**, and locate the update file.
   b. Click **Update**, then click **Yes** to confirm.

   Version 12.1 is applied and the KACE Systems Management Appliance server restarts. Progress appears in the browser window and in the **Administrator Console**.
5. When the server upgrade finishes, upgrade all of your agents to version 12.1.

Post-update tasks

After the update, verify that the update was successful and verify settings as needed.

Verify successful completion

Verify successful completion by viewing the KACE Systems Management Appliance version number.

1. Go to the appliance *Control Panel*:
   - **If the Organization component is not enabled on the appliance, click Settings.**
   - **If the Organization component is enabled on the appliance: Log in to the appliance System Administration Console:** `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/12.1/technical-documents)
  - **Technical specifications**: Information on the minimum requirements for installing or upgrading to the latest version of the product.

    For virtual appliances: Go to https://support.quest.com/technical-documents/kace-systems-management-appliance/12.1-common-documents/technical-specifications-for-virtual-appliances/.
    For KACE as a Service: Go to https://support.quest.com/technical-documents/kace-systems-management-appliance/12.1-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/12.1/technical-documents to view documentation for the latest release.
  - **Administrator guide**: Instructions for using the appliance. Go to https://support.quest.com/technical-documents/kace-systems-management-appliance/12.1-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

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 - April 2022

Software Version - 12.1