KACE® Systems Management Appliance 13.1

Release Notes

Table of Contents

Quest® KACE® Systems Management Appliance 13.1 Release Notes

This document provides information about the KACE Systems Management Appliance version 13.1.

About KACE Systems Management Appliance 13.1

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 maintenance release contains only resolved issues.

New features

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

The following features will be deprecated in a future release:

- Legacy approval method in KACE GO

- Scripting configuration policies

Enhancements

The following enhancement is implemented in this release.

Enhancement issue	Issue ID
Password complexity requirement is now 12 characters minimum. More than 64 characters are accepted.	K1-33877

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
Emailing tickets did not work as expected if there was an invalid user in the ticket.	K1-33826
Trying to add a comment or change the value of a ticket field could result in an incorrect error message, despite success.	K1-33803
It was not possible to create ticket from email if there were curly brackets in the email subject .	K1-33776
Service Desk announcement with an email link could be truncated.	K1-33713

i **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
Incorrect Graph API URL was used when using any other service other than Global Community Cloud (GCC).	K1-33833

Resolved Reporting issues

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

Table 3. Resolved Reporting issues

Resolved issue	Issue ID
Report logo was not showing properly in generated PDF reports.	K1-33734
Creating a report that includes the *Number of Records Analyzed* could produce an error when running the report.	K1-33707

Resolved Server issues

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

Table 4. Resolved server issues

Resolved issue	Issue ID
Importing LDAP users with no prefix could result in error.	K1-33860
It was not possible to access the SSL Certificate Form if SSL was enabled.	K1-33855
Error was seen when applying a manually created label to a device.	K1-33854
Offline patch package could be missing patch payloads.	K1-33853
Invalid LDAP labels in server settings could result in *Oops* page after logging in and forcing inventory.	K1-33791
Require organization selection at login setting was ignored.	K1-33789
Smart Labels imported across organizations were hidden under **Label Management > Label**.	K1-33768
SCAP scan results sometimes did not behave as expected.	K1-33767
Active Directory discovery schedule process did not behave as expected when it was unable to bind to Active Directory.	K1-33758
Run Now from the *Script Detail* page sometimes did not work as expected.	K1-33756
In a non-US locale, some numbers, like currency, could contain a comma and result in an error.	K1-33755
An error could be reported if **All Locales** were selected under **Security > Windows Feature Updates > Subscriptions**.	K1-33753
On the *Networking Settings* page, it was not possible to clear the **Enable SMTP Remote Server (Outbound Relay)** option and save the changes.	K1-33742
Error was seen when generating the *Device+Software Catalog - Executables Inventory* wizard report in the **System Administration Console** or **Administrator Console**.	K1-33738

Resolved issue	Issue ID
Reset Tries from the *Patch Catalog* list page **Choose Action** menu required clicking **Yes** three times.	K1-33731
Inventory could fail when inventorying ESX device.	K1-33727
Error was seen when trying to search a quarantined device.	K1-33719
Windows Feature Update History was showing IDs instead of text.	K1-33718
Server: API requests that did not provide a user agent header always failed.	K1-33709
Expired software license asset user notifications were generated for licenses with no expiration date set.	K1-33702
You must download a catalog to title application message was showing after downloading the catalog.	K1-33696
Windows Feature Updates Catalog Missing column count was inaccurate.	K1-33613
Saving a patch schedule with special characters in messages showed escape characters in the patch notification.	K1-33530
Creating a report from the *Asset History* list page was missing value 2.	K1-33437
The **Disable network traffic** option was not available if Defender status is disabled or another anti-virus was running.	K1-33435
Dell Updates Smart Label creation could take a long time.	K1-33352
Task chains with a patch job as the second task did not always behave as expected.	K1-33284
Schedule info did not show correctly after disabling a Linux Package Upgrade Schedule.	K1-30725

i **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
KACE agent MSI installer used different product ID when installing non-English Windows.	K1A-28

Known issues

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

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

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

System requirements

The minimum version required for installing KACE Systems Management Appliance 13.1 is 13.0. 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.

i | **NOTE:** The KACE Agent RPM package can be installed on managed SUSE Linux devices only when the `libxslt-tools` package is installed before the agent package.

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

Before upgrading to or installing version 13.1, 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/13.1-common-documents/technical-specifications-for-virtual-appliances/.

- For KACE as a Service: Go to https://support.quest.com/technical-documents/kace-systems-management-appliance/13.1-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.

> **i** | **NOTE:** Product licenses for version 13.1 can be used only on KACE Systems Management Appliance running version 13.1 or later. Version 13.1 licenses cannot be used on appliances running earlier versions of the appliance, such as 12.0.

Installation instructions

You can apply this version using an advertised update or by manually uploading and applying an update file. For instructions, see the following topics:

- Prepare for the update
- Update the KACE Systems Management Appliance server using an advertised update
- Upload and apply an update manually
- Post-update tasks

> **i** | **NOTE:** To ensure accuracy of software discovery and install counts for devices running particular software, beginning in the KACE Systems Management Appliance 7.0 release, the software catalog re-installs with every upgrade.

Prepare for the update

Before you update your KACE Systems Management Appliance server, follow these recommendations:

- **IMPORTANT: Enable legacy BIOS booting**:

  An issue in the UEFI BIOS booting can be triggered during an upgrade. To prevent it, you must ensure that legacy BIOS booting is enabled. A power-down of the appliance prior to making a switch is required. Also, for ESX-based virtual machines, ensure that the hardware version is 13 or later.

Prior to applying the appliance upgrade, you must ensure that your browser's cache is clean and that port 52231 is available from your browser to the appliance. Users working from home may need to have their corporate firewall configured to allow port 52231 communications.

- **Verify your KACE Systems Management Appliance server version**:

  The minimum version required for installing KACE Systems Management Appliance 13.1 is 13.0. 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.

  i | **NOTE:** The KACE Agent RPM package can be installed on managed SUSE Linux devices only when the `libxslt-tools` package is installed before the agent package.

- **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/13.1-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 13.1. For complete information, visit https://support.quest.com/kace-systems-management-appliance/kb/4281031/how-to-re-image-kace-system-management-appliance-sma.

  If your appliance version is many versions behind, the following article contains useful upgrade-related tips: https://support.quest.com/kace-systems-management-appliance/kb/4284819/sma-server-and-agent-upgrade-path.

  There are many reasons why you should re-image the appliance. The new disk layout, for example, offers better compatibility with version 13.1. It also features better security and performance.

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

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

Update the KACE Systems Management Appliance server using an advertised update

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

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

1. Back up your database and files. For instructions, see the **Administrator Guide**, https://support.quest.com/technical-documents/kace-systems-management-appliance/13.1-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**.

   > Imp **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 13.1 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 13.1.

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/13.1-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 13.1 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 13.1 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 13.1.

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/13.1/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/13.1-common-documents/technical-specifications-for-virtual-appliances/.
    For KACE as a Service: Go to https://support.quest.com/technical-documents/kace-systems-management-appliance/13.1-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/13.1/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/13.1-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

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

KACE Systems Management Appliance Release Notes

Updated - April 2023

Software Version - 13.1