KACE® Systems Management Appliance 10.2

Release Notes

Table of Contents

Quest® KACE® Systems Management Appliance 10.2 Release Notes

This document provides information about the KACE Systems Management Appliance (SMA) version 10.2.

About KACE Systems Management Appliance 10.2

KACE Systems Management Appliance (SMA) is a virtual appliance designed to automate device management, application deployment, patching, asset management, and Service Desk ticket management. For more information about KACE SMA series appliances, 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. Other guides, such as the *Administrator Guide* and in-product help are not localized at this time, and version 10.0 is included with this product release.

New features and enhancements

This release of the KACE Systems Management Appliance (SMA) includes the following features and enhancements.

- **Built-in Windows 10 Feature Updates**: Deploy Feature Updates to upgrade Windows 10 to the latest semi-annual release. The Feature Updates are detected and deployed in a manner similar to patching.
- **Improved authentication support (OAuth 2.0) for Service Desk inbound email**: With Google and Microsoft introducing new security standards for client apps connecting to their respective accounts, the following credential types can now be configured with this new level of authentication, and used to access Service Desk POP3 inbound email.
  - **Office365 OAuth credentials**: You must have an Office 365 account, and have created a Microsoft Active Directory app in Microsoft Azure with a Client ID and Client Secret. For more information, visit https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-create-service-principal-portal.
  - **Google OAuth credentials**: You must have a Google account to be used as your developer account, and have created a Google app with a Client ID and Client Secret. For more information, visit https://support.google.com/googleapi/answer/6158849.
- **Agent snooze through system tray**: End users can snooze agent activities using the KACE system tray utility for 15 minutes, 30 minutes, one hour, and two hours. This is configurable up to a maximum of 5 times per day.
- **Parents pass fields to child tickets**: The appliance now allows parent tickets to pass information to child tickets in a process (workflow). For example, while creating a new user you can now pass the user name,

department, phone number, and so on, from the parent ticket to other departments involved in the new user creation.

- **PowerShell support:** Native PowerShell for KACE SMA online scripting is now supported. Previously the KACE SMA online script only allowed users to define a batch script, if they wanted to run PowerShell, they had to wrap that inside a batch file and invoke through batch scripting. PowerShell scripts can now be launched directly from the KACE SMA.
- **Chromebook management enhancements**: Additional inventory information, device command support, advanced search and Smart Label reporting is added in this release.
- **jOVAL support**: OVAL and SCAP scanning now use jOVAL, a faster, more up-to-date, better supported, and cross-platform model, for all supported Windows agent platforms, including 32- and 64-bit devices.
- **KACE GO Biometrics**: You can now use biometric features instead of the PIN code.
- **Ticket templates for KACE GO**: This feature extends customizable templates with conditional logic fields introduced in KACE SMA 10.0 to work in KACE GO, too.
- **New layout options for ticket templates**: Starting in this release, you can arrange related fields together in a ticket template, place fields close to the edge of the layout area, or create blank spaces between fields, as needed.

Resolved issues

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

Table 1. Resolved Issues

Resolved issue	Issue ID
Deploy schedule of Dell updates did not function as expected when No Reboot was selected.	K1-20940
SAML (Security Assertion Markup Language) user attribute mapping was only allowed for `LOGIN` as the primary key.	K1-20935
Some Dell Updates did not appear in the list of available updates in the Administrator Console, even though they did exist on the KACE SMA.	K1-20930
SAML settings: Role mapping was not updated after an initial SAML configuration.	K1-20927
Provisioning failed on Mac OS when the provisioning schedule contained credentials for Linux and Mac and the credentials were not the same.	K1-20926
KACE Cloud Mobile Device Manager (MDM) provisioning failed if computer license count was reached.	K1-20912
Manually installing a Mac agent with a host name in the `dmg` did not populate in the installer.	K1-20909
After archiving a ticket, HTML code sometimes appeared in the *Resolution* field.	K1-20905
In a multi-organization, multi-language KACE SMA, some parts of the Administrator Console sometimes appeared in the wrong language.	K1-20904

Resolved issue	Issue ID
Aggressive HTML sanitization converted the UNC path starting with `\\n` into a new line.	K1-20892
Task Chains: Tasks after the first task did not start off when sending actions to multiple devices.	K1-20880
Asset Status was not included in the export of a device to a `CSV` file.	K1-20872
It was not possible to upload files greater than 2 GB through the Administrator Console.	K1-20868
Sorting was not working on the *Device Detail* page in the *Patching Detect/Deploy Status* section.	K1-20864
Creating report from the patch catalog did not work.	K1-20852
Created and *Modified* dates in the `ticket_fields_visible` token were incorrect.	K1-20848
On the *Device Detail* page, in the *Activities* group, in the *Service Desk Tickets* section, choosing *New* did not associate the ticket with the device.	K1-20846
Database size could grow quickly with many devices checking in at a fast rate.	K1-20843
Archiving a ticket from the *Ticket Detail* page shows *Ticket Deleted* in history.	K1-20842
KACE alerts did not show up properly in dark mode on Mac OS 10.14 and 10.15. Alerts were not displayed in the dark mode theme, when selected.	K1-20836
Software MI (Managed Installation) did not increment or decrement the `INSTALLED_COUNT` after a successful run.	K1-20829
On the *Asset Detail* page, the Barcode Format field did not allow underscore '_' characters.	K1-20820
Hooks are now provided to allow IdP (identity provider) -initiated SAML logins to specify the Organization and Portal (`user`, `admin`).	K1-20802
A comma ',' in a Patching reboot message was incorrectly displayed as a space, backslash, or comma.	K1-20781
There were missing supported media types such as media and 10GBase-T.	K1-20743
When importing users, the role might not be imported as expected.	K1-20720
OVAL scan failed on Windows server 2019 with a Timeout error.	K1-20713
Process Tickets (parent and child) with angle brackets in subject disappeared from the Administrator Console upon creation.	K1-20670

Resolved issue	Issue ID
Removing welcome message text leaved undesired text on the login screen for non-English languages.	K1-20646
Registry Configuration Policy script hanged the agent with large hexadecimal values.	K1-20626
Custom ticket rules which change `HTML_SUMMARY` might not behave as expected.	K1-20619
Monitoring raised an alert with corrupted text when an event log message matched more than one criteria for a monitoring profile.	K1-20614
Incorrect data in ticket status field sometimes prevented deleting or archiving a device associated with the ticket.	K1-20582
Emails from custom ticket rules were not sent to all addresses when there was a space in between the email addresses.	K1-20575
Approval column on the User Console Home dashboard did not display properly for non-English locales.	K1-20546
HTML email: Inline images showed as broken in email notifications using `$last_comment`.	K1-20541
Process email templates were not sent out if approval was not enabled.	K1-20527
It was not possible to add assets or devices to a location when user permission was set to read.	K1-20467
Unexpected behavior occurred when SCAP (Secure Content Automation Protocol) results were received for a machine that could not be identified.	K1-20464
Asset Import sometimes removed existing device location and user when they were not mapped in the import.	K1-20454
Initial logo seen in the User Console did not match initial selection in the organization drop-down menu.	K1-20440
Device List: Export report did not show *Last Reboot*.	K1-20382
Mac Managed Installations did not support installer in ZIP format.	K1-20337
A blank page could be seen on the *License Detail* page when the user has read permissions.	K1-20309
Moving a ticket to a queue without a matching category could result in unexpected values in the *Category* field.	K1-20302
Added *CC* for ticket from comment was removed after clicking **Save** or **Apply Changes**.	K1-20295
Exporting a computer list using through the System Administration Console resulted in a missing organization name.	K1-20110

Resolved issue	Issue ID
Upgrading software could cause attached files to be abandoned.	K1-20097
Custom *Device Field* was not displayed properly on the *Device Detail* page.	K1-20089
Custom discovery schedule: *Ping* selection was reset when re-editting the schedule.	K1-20037
When doing an Advanced Search on the *Licenses* list page, the *Name* column link to the *License Detail* page could be incorrect.	K1-20020
Replication was not being completed when 32-bit Linux systems were used as replication agents with an `SMB` share.	K1-20016
Dell Updates wizard reports could fail to run.	K1-19986
Machine details page displayed the wrong MAC address.	K1-19884
Device Scope Label did not save when *All devices* is cleared.	K1-19883
Patch schedule detect/deploy timeout are now honored regardless of the agent process timeout setting.	K1-19826
Setting the Agent Alert logo could cause unexpected behavior with inventory on Mac and Linux devices.	K1-19593
Deleting a large number of Asset Locations at once took a long time to complete.	K1-19307
Disparity was seen between Advanced Search of a custom field in a regular ticket, when compared to doing a search of an archived ticket.	K1-19261
Duplicating a running patch schedule also triggered the duplicated schedule to the device.	K1-19120
Computer Inventory CSV download failed if `CREATED` or `MODIFIED` were used as sort fields.	K1-18601
MI at bootup/login was not working on Mac.	K1-18235
When SAML authentication is enabled, organizations with special characters in the name break the SAML login page.	ESMP-7165
In previous versions, every organization database had asset type views that were part of the linked reporting feature. This allowed customers to write SQL reports based on these views. The linked reporting feature stopped working in version 9.0, and these views (now obsolete) are removed in this version.	ESMP-7114
Google Admin Console link did not work properly.	ESMEC-3640
Kerberos domain credentials can now be entered in a standard FQDN (fully qualified domain) format.	ESMEC-3614

Resolved issue	Issue ID
Offline `kscript` configured to run at user login failed on Mac device.	ESMEC-3530
It was not possible to send Wake-on-LAN packet using simple method to a Mac OS device with a computer name containing a space character.	ESMEC-3502
In the Service Desk, variable replacement for `$ticket_category` token was not working.	ESMAS-4760

Known issues

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

Table 2. General known issues

Known issue	Issue ID
Alternate location for a Managed Installation is not used behind a replication share.	ESMP-7356
SFTP (Secure File Transfer Protocol) full path is not retained when editing an existing asset import schedule.	ESMP-7253
Need Help slide out menu hides menu for organization selection and logout options.	ESMP-7155
If a managed installation (MI) is configured to run at boot time for a Mac, the `DMG` file used for the MI is remounted automatically by the OS.	ESMEC-3756
Agents running on Mac OS 10.15 can not be used as replicators if the replication destination is a network share. This is caused by an added Mac OS 10.15 security feature for the file and folder permissions, which protect network volumes. **Workaround**: To grant full disk access to a network volume, you must explicitly grant that permission to the KACE agent. The exception to this are managed environments, where the administrator can configure these settings using a `com.apple.TCC.configuration-profile-policy` payload.	ESMEC-3746

System requirements

The minimum version required for installing KACE SMA 10.2 is 10.1. 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 SMA agent is 9.0. We recommend running the latest agent version with KACE SMA 10.2.

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 10.2, make sure that your system meets the minimum requirements. These requirements are available in the KACE SMA technical specifications.

- For virtual appliances: Go to https://support.quest.com/technical-documents/kace-systems-management-appliance/10.2-common-documents/technical-specifications-for-virtual-appliances/.
- For KACE as a Service: Go to https://support.quest.com/technical-documents/kace-systems-management-appliance/10.2-common-documents/technical-specifications-for-kace-as-a-service/.

Product licensing

If you currently have a KACE SMA product license, no additional license is required.

If you are using KACE SMA 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 10.2 can be used only on KACE SMA appliances running version 6.3 or later. Version 10.2 licenses cannot be used on appliances running earlier versions of the KACE SMA, such as 6.0.

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 SMA 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 SMA 7.0 release, the software catalog re-installs with every upgrade.

Prepare for the update

Before you update your KACE SMA server, follow these recommendations:

- **Verify your KACE SMA server version**:

  The minimum version required for installing KACE SMA 10.2 is 10.1. 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 SMA agent version**.

  The minimum version required for upgrading the KACE SMA agent is 9.0. We recommend running the latest agent version with KACE SMA 10.2.

- **Back up before you start**.

  Back up your database and files and save your backups to a location outside the KACE SMA 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/10.2-common-documents/administrator-guide/.

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

  For appliances initially installed prior to version 7.0 that have not been re-imaged (physical appliances) or reinstalled (virtual), Quest Software strongly recommends exporting, re-creating (an image, or a virtual machine installation from an OVF file), and re-importing the database before upgrading to version 10.1. 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 10.2. 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 SMA 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 SMA server using an advertised update

You can update the KACE SMA 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 SMA 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/10.2-common-documents/administrator-guide/.
2. Go to the appliance *Control Panel*:
   - If the Organization component is not enabled on the appliance, click **Settings**.
   - If the Organization component is enabled on the appliance: Log in to the appliance System Administration Console: **`http://`**KACE_SMA_hostname**`/system`**, 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 10.2 is applied and the KACE SMA 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 10.2.

Upload and apply an update manually

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

> CAUTION: Never manually reboot the KACE SMA 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/10.2-common-documents/administrator-guide/.
2. Using your customer login credentials, log in to the Quest website at https://support.quest.com/kace-systems-management-appliance/download-new-releases, download the KACE SMA server `.kbin` file for the 10.2 GA (general availability) release, and save the file locally.
3. On the left navigation bar, click **Appliance Updates** to display the *Appliance Updates* page.
4. In the *Manually Update* section:
    a. Click **Browse** or **Choose File**, and locate the update file.
    b. Click **Update**, then click **Yes** to confirm.

   Version 10.2 is applied and the KACE SMA 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 10.2.

Post-update tasks

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

Verify successful completion

Verify successful completion by viewing the KACE SMA 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/10.2/technical-documents)
  - **Technical specifications**: Information on the minimum requirements for installing or upgrading to the latest version of the product.

    For virtual appliances: Go to https://support.quest.com/technical-documents/kace-systems-management-appliance/10.2-common-documents/technical-specifications-for-virtual-appliances/.
    For KACE as a Service: Go to https://support.quest.com/technical-documents/kace-systems-management-appliance/10.2-common-documents/technical-specifications-for-kace-as-a-service/.
  - **Setup guides**: Instructions for setting up virtual appliances. Go to https://support.quest.com/kace-systems-management-appliance/10.2/technical-documents to view documentation for the latest release.
  - **Administrator guide**: Instructions for using the appliance. Go to https://support.quest.com/technical-documents/kace-systems-management-appliance/10.2-common-documents/administrator-guide/ to view documentation for the latest release.

Globalization

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

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

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

About us

Quest provides software solutions for the rapidly-changing world of enterprise IT. We help simplify the challenges caused by data explosion, cloud expansion, hybrid datacenters, security threats, and regulatory requirements. We are a global provider to 130,000 companies across 100 countries, including 95% of the Fortune 500 and 90% of the Global 1000. Since 1987, we have built a portfolio of solutions that now includes database management, data protection, identity and access management, Microsoft platform management, and unified endpoint management. With Quest, organizations spend less time on IT administration and more time on business innovation. 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

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

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.

Trademarks

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 - May 2020

Software Version - 10.2