

Quest®



KACE® Systems Management Appliance 10.1

Release Notes



# Table of Contents

Quest® KACE® Systems Management Appliance 10.1 Release Notes.....	3
About KACE Systems Management Appliance 10.1.....	3
New features and enhancements.....	3
Service Desk features.....	3
Endpoint communication features.....	4
Infrastructure features.....	4
KACE GO mobile app features.....	4
Resolved issues.....	4
Known issues.....	8
System requirements.....	8
Product licensing.....	8
Installation instructions.....	9
Prepare for the update.....	9
Update the KACE SMA server using an advertised update.....	10
Upload and apply an update manually.....	10
Post-update tasks.....	11
Verify successful completion.....	11
Verify security settings.....	11
More resources.....	12
Globalization.....	12
About us.....	12
Technical support resources.....	13
Legal notices.....	13

# Quest® KACE® Systems Management Appliance 10.1 Release Notes

---

This document provides information about the KACE Systems Management Appliance (SMA) version 10.1.

## About KACE Systems Management Appliance 10.1

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.

- [Service Desk features](#)
- [Endpoint communication features](#)
- [Infrastructure features](#)
- [KACE GO mobile app features](#)



**IMPORTANT:** If you are currently running version 9.1 or earlier, you must upgrade to version 10.0 by February 2, 2020. Otherwise you will lose your patching functionality. For more information, visit <https://support.quest.com/kb/311910/upgrade-your-kace-sma-to-ensure-continuous-operation-of-your-patching-functionality>.

## Service Desk features

This release of the KACE Systems Management Appliance (SMA) includes the following Service Desk feature:

- **Ability to prevent users from adding attachments to Service Desk queues:** Starting in this release, appliance administrators can specify ticket attachments restrictions, as applicable. These restrictions can be configured through the *Queue Detail* page.

## Endpoint communication features

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

- **Platform support:** The following operating systems are added to the existing set of supported platforms:
  - **Agent-managed devices:** Mac OS X® 10.15, Linux Red Hat® Linux 8, Windows® 10 (Redstone 7) Fall 2019 update, Windows Server Fall 2019 Update, and Windows 10 IoT Enterprise.
  - **Agentless management:** Mac OS X 10.15, Linux Red Hat Linux 8, Windows 10 (Redstone 7) Fall 2019 update, Windows Server Fall 2019 Update, Windows 10 IoT Enterprise, and Fedora® 30.

For more information, see the KACE SMA *Technical Specifications for Virtual Appliances*.

- **Patch detection improvements.** To optimize patch detection speed, the appliance now zips up Windows detection files for each patch and extracts them locally, instead of having to download them individually.

## Infrastructure features

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

- **Upgrade-related information added to relevant pages.** After downloading the upgrade bundle, the *Appliance Updates* page in the System Administration Console now displays a short description of the upgrade, describing the contents of the package. In addition to that, warnings are added to dashboards and list pages, when a critical upgrade becomes available.
- **Asset Status displayed on the Devices page.** The *Devices* list page in the Administrator Console now displays the *Asset Status* column by default, allowing you to quickly review the status of each listed device.

## KACE GO mobile app features

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

- **Barcode scanning improvements:** Starting in this release, when you scan a barcode, you can turn on the flashlight on your device by tapping the icon in the bottom-right corner of the screen. The device vibrates when the barcode is detected.
- **Support for Security Assertion Markup Language (SAML) single sign on.** SAML is an XML-based protocol that passes security tokens between Identity and service Providers. When SAML is enabled and configured on the appliance, and you are logged in to your Identity Provider (IdP), you can log in to KACE GO without providing your KACE SMA user credentials. For more information on how to configure SAML on the appliance, see the KACE SMA *Administrator Guide*

## Resolved issues

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

Table 1. Resolved Issues

Resolved issue	Issue ID
Label management list page could experienced reduced performance with many labels present.	K1-20809
User-created wizard reports containing the <i>Number of Records Analyzed</i> field could have duplicate rows.	K1-20778
KACE Patching could leave the Apple Software Update configuration pointing to KACE, preventing you from running the software update manually. The new 10.1 agent resets the configuration if this is detected in a patching run.	K1-20774
Reports: <i>Computer List grouped by Operating System</i> showed duplicate rows.	K1-20772
Adding SQL server processes to the list of processes that the agent should not terminate, in the rare scenario where the OS recycles PID, caused the agent to believe it is the parent of SQL server processes.	K1-20771
The <i>Computer with agent out of compliance report</i> could give false positives if the appliance had data for obsolete agent builds.	K1-20770
Clicking <b>Edit</b> on a Patch Smart Label could navigate to a wrong label or result in a PHP error.	K1-20769
Devices missing patches count caused the patch catalog to load slowly.	K1-20768
In the User portal, the local user's machine was sometimes not listed in the drop-down menu.	K1-20767
Service Desk: A CC Ticket User could not reply to a ticket if they were not listed as the first user the CC list.	K1-20766
It was not possible to log in using SAML if there were multiple organization, and only a subset had SAML enabled.	K1-20765
Archive Advanced Search resulted in MySQL syntax error.	K1-20762
HTML formatting was removed from Parent and Child tickets that are part of Processes.	K1-20761
KACE patch sometimes did not properly detect patches using WMI on computers with multiple CPUs.	K1-20759
Apache server-status information was publicly accessible when SSL was enabled.	K1-20753
Computer chassis type could show both <i>Notebook</i> and <i>laptop</i> in version 10.0. These are now normalized as <i>laptop</i> (as in earlier appliance versions).	K1-20748
<i>Owners only</i> email token was processed correctly, but the token was not removed from the comment.	K1-20747

Resolved issue	Issue ID
Extraneous spaces were sometimes added when processing tickets and ticket comments through email.	K1-20739
SQL Server patches are now supported.	K1-20736
The 10.1 KACE agent no longer installs Munki by default on the Mac. Munki is only installed if KACE patching is used on the Mac. It is recommended to either do patching with KACE or using your own process own, but not both.	K1-20735
Ticket Templates did not appear correctly in legacy browsers.	K1-20683
Due date was not re-set when another priority is selected without a SLA (Service Level Agreement) due date.	K1-20680
Some built-in reports were not converted to KACE patching.	K1-20679
Extra padding or spacing was sometimes added when tickets are created by email.	K1-20678
KACE GO mobile app: Notifications were not sent to queue owners when creating tickets.	K1-20662
Archive and purge could fail to complete if any ticket archive or purge failures occurred during processing or organization archive and purge jobs overlap.	K1-20659
KACE GO: Service Desk did not allow ticket creation if the submitter field was marked as read-only.	K1-20648
Lenovo warranty lookup failed if API key is specified. The request format is fixed in 10.1 to make this work.	K1-20639
Organization Filter based on IP sometimes did not work as expected when a NAT (network address translation) address was used.	K1-20608
Export to CSV showed error in software inventory.	K1-20595
When replying to a ticket using a web-based email client, the email thread below the delimiter sometimes did not show up on the comment reply.	K1-20592
Custom ticket rules could fail to update the summary as expected.	K1-20580
Patch status showed "not scheduled" and "error" for many machines with <i>Patch Schedule Timezone</i> set to <i>Agent</i> .	K1-20560
HTML comment editor did not properly handle certain scenarios involving special characters (such as code blocks).	K1-20493
Ticket HTTP URL email variable showed HTTPS despite 80 being available.	K1-20480
False trigger of Summary Page Alert message for Pre-7.1 agents was reported.	K1-20411

Resolved issue	Issue ID
Files uploaded through Scripting's <i>Upload a File</i> function with a space at the end were not accessible.	K1-20392
HTTP response headers are improved for stronger PCI compliance.	K1-20112
<i>Process Parent Ticket</i> did not get closed if user changed the status from the Choose action drop-down list.	K1-19691
Dell Update failed when retrieving the payloads from replication. This is fixed with the 10.1 agent.	K1-19510
Dell XPS models were not supported by Dell Updates.	K1-19282
Ticket SLA Notifications could be sent in error when due date was changed.	K1-19259
In the <i>Devices</i> list page, in the advanced search, <i>Name</i> was used instead of OS <i>Name</i> .	ESMP-7094
Error was seen while exporting the contents of the <i>Devices</i> list page to CSV when sorted by <i>Last Inventory</i> .	ESMP-7057
A deprecated patch label alert appeared when it should not be seen.	ESMP-7055
LDAP import and SAML enabled at the same time sometimes resulted in duplicate users.	ESMP-7054
Reports: <i>Computers with Agents Out of Compliance</i> sometimes contained a wrong agent version.	ESMP-7047
APFS (Apple File System) was mounted to '/' is fixed to be reported properly with agentless inventory on Mac.	ESMEC-3600
Mac devices managed by KACE MDM (Mobile Device Manager) and KACE SMA did not have the Wake On LAN option in the Administrator Console.	ESMEC-3598
Oracle Enterprise Linux devices could not be provisioned automatically as agentless devices.	ESMEC-3592
Lenovo warranty lookup is enhanced by retrieving additional information with 10.1 agent, needed to obtain the Lenovo warranty on some devices.	ESMEC-3532
Empty battery record was added when performing agentless inventory on virtual Mac device.	ESMEC-3527
Queue owners could not reply to tickets they did not own.	ESMAS-4710
In Service Desk tickets, the token <code>\$ticket_url</code> did not work inside a link.	ESMAS-4709
In Service Desk emails, <code>\$ticket_number</code> shown in email subject could be incorrect.	ESMAS-4708

Resolved issue	Issue ID
Import and Export of ticket templates in queue configuration (as a resource) was not supported.	ESMAS-4631
Adding attachment to asset API did not work.	ESMAS-4618

## Known issues

There are no known issues at the time of this release.

## System requirements

The minimum version required for installing KACE SMA 10.1 is 10.0. 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 SMA agent is 9.0. We recommend running the latest agent version with KACE SMA 10.1.

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 10.1, 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/10.1-common-documents/technical-specifications-for-virtual-appliances/>.
- For KACE as a Service: Go to <https://support.quest.com/technical-documents/kace-systems-management-appliance/10.1-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 10.1 can be used only on KACE SMA appliances running version 6.3 or later. Version 10.1 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 10.1 is 10.0. 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 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 10.1.
- **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/10.1-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 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 10.1. 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 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/10.1-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 10.1 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 10.1.

## Upload and apply an update manually

If you have an update file from Quest, you can upload that file manually to update the KACE 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/10.1-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 SMA server `.kbin` file for the 10.1 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 10.1 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 10.1.

## 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 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/10.1/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/10.1-common-documents/technical-specifications-for-virtual-appliances/>.  
**For KACE as a Service:** Go to <https://support.quest.com/technical-documents/kace-systems-management-appliance/10.1-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/10.1/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/10.1-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 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](http://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

© 2019 Quest Software Inc. ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Quest Software Inc.

The information in this document is provided in connection with Quest Software products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Quest Software products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, QUEST SOFTWARE ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL QUEST SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF QUEST SOFTWARE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Quest Software makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Quest Software does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

Quest Software Inc.

Attn: LEGAL Dept

4 Polaris Way

Aliso Viejo, CA 92656

Refer to our Web site (<https://www.quest.com>) for regional and international office information.

#### Trademarks

Quest, the Quest logo, Join the Innovation, and KACE are trademarks and registered trademarks of Quest Software Inc. For a complete list of Quest marks, visit <https://www.quest.com/legal/trademark-information.aspx>. All other trademarks and registered trademarks are property of their respective owners.

#### Legend

 **CAUTION:** A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

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

KACE Systems Management Appliance Release Notes

Updated - December 2019

Software Version - 10.1