Quest

KACE® Systems Management Appliance 10.0

Release Notes

Table of Contents

Quest® KACE® Systems Management Appliance 10.0 Release Notes

This document provides information about the KACE Systems Management Appliance (SMA) version 10.0.

About KACE Systems Management Appliance 10.0

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.

New features and enhancements

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

- Service Desk features
- Asset Management features
- Endpoint communication features
- Infrastructure 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 features and enhancements.

- **Ticket templates**: This feature allows you to create different ticket types within the same queue. Use it to better control the information your end users provide for different request scenarios without having to create and manage multiple ticket queues. Each queue can have one or more ticket templates. If multiple templates exist in a queue, you must select one ticket template as the default template.
- **Conditional fields in ticket templates**. You can configure conditional logic in each ticket template to show or hide certain fields based on the previously selected values on the ticket page. For example, if you have a

ticket template for printer issues, you can display different set of fields that are applicable to different kinds of printer issues.

Asset Management features

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

- **Scheduled asset import**: Starting in this release, you can configure a scheduled import of assets from a CSV (comma-separated value) file located on a network share, using the *Import Assets* wizard. The wizard includes a new page, *Asset Import Selection Schedule*, that allows you to choose from available schedule patterns, as required.
- **Ability to map the Asset Status field during asset import**: The *Mapping* page in the *Import Assets* wizard now allows you to map the *Asset Status* field to a column in the CSV file. This is useful in cases when you need to import a high number of assets with each asset having a specific status (such as *Active*). If you do not specify this mapping, the default status that is associated with the selected Asset Type is assigned to each imported asset entry.
- **Administrators can prevent non-administrative users from deleting assets**: The *Asset Type Detail* page now includes an option, **Allow non-administrators to delete assets**, that administrators can use to specify whether non-administrative users have the capability to delete assets. This option is turned off by default. Only administrators can configure this option. For other types of users, this field appears on the page, but it is disabled.
- **Appliance administrators can create asset types without Location and User fields**. There are certain asset types (such as Purchases or Contracts) where this information is irrelevant. The *Asset Type Detail* page now includes the **Show Location settings** option that can be used to include or exclude the *Location* field for the selected asset type. Similarly, the Asset Assignee value only appears in Device-type assets.

Endpoint communication features

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

- **Discovering Microsoft Hyper-V or System Center Virtual Machine Manager (SCVMM) devices**: If your organization uses a virtual Hyper-V-based environment, you can use the appliance to discover Microsoft Hyper-V or SCVMM devices through discovery scheduling. To scan your network for Hyper-V or SCVMM devices, and to capture information about those devices, add an Authenticated Discovery Schedule. Each SCVMM/Hyper-V device consumes an agentless license. If the device is also provisioned with a KACE agent, it also consumes a license for the agent.

NOTE: When performing inventory of a SCVMM server, only Hyper-V hosts are supported at this time.

- **Battery information added to Device Details**: The *Device Details* page now includes a new group of fields, *Batteries*, that displays battery-related information for Windows, Linux and MacOS Agent-managed and Agentless devices. This group includes the following fields:
  - **Charge**: The percentage of the current battery capacity.
  - **Chemistry**: **Windows and Linux devices only**. The battery type, such as Lithium Ion, and so on.
  - **Current Capacity (mWh)**: The current battery capacity.
  - **Design Capacity (mWh)**: The maximum capacity of battery by design.
  - **Full Charge Capacity (mWh)**: Current maximum capacity of battery. This value degrades over time.
  - **Health (%)**: The percentage of the current battery capacity compared to its maximum designed capacity.
  - **Manufacturer**: The battery manufacturer.
  - **Name**: The battery name or model.
  - **Plugged In**: An indicator of whether the battery is currently plugged into a power source.
  - **Recharge Count**: **MacOS devices only**. The number of times the battery has been recharged.
  - **Serial Number**: The serial number of the battery.
  - **Time Remaining (Minutes)**: The number of minutes after which the battery becomes discharged. When the device is plugged in, this field is blank.
- **Ability to upload and distribute cURL certificate bundles**: Some environments use custom cURL (Client URL) CA (certificate authority) certificates during agent-server communication. This can be used to verify SSL certificates that are signed by an authority that is not referenced in the default agent bundle. Starting in this release, you can use the *CA Certificate Bundle File* setting on the *Agent Settings* page to upload a custom cURL CA bundle, or to revert to the default one.
- **Remote Control**: Integration with a third-party solution for remote control management across Windows, Mac, and Linux systems. *SimpleHelp* now appears as an option under *Device Actions* on the *General Settings* page. For more information about this tool, see your SimpleHelp documentation.
- **Continuous integration with KACE Cloud Mobile Device Manager (MDM)**:
  - **Viewing information about devices enrolled in KACE Cloud Mobile Device Manager (MDM)**: The appliance displays information about Mac OS X devices that are enrolled in an integrated KACE

Cloud MDM instance. The type of information available for such devices depends on whether they have a KACE SMA Agent installed.

  - **Device management method appears in Device Details**: The new *Device Entry Type* field on the *Device Details* page the selected device's management method: *Agent Device*, *Agentless Device*, *Manually Entered Record*, or *Agent/Agentless* (hybrid KACE Cloud MDM inventory).
  - **Dissociating a device from KACE Cloud MDM**: For Agentless devices enrolled in KACE Cloud MDM, to remove the device's association with KACE Cloud MDM and revert to Agent-only inventory records, on the *Device Details* page, simply click **Remove Agentless Integration**.

- **KBRSL removed from the appliance**: `KBRSL` is no longer included in provisioning code. Existing `KBRSL` provisioning schedules are converted to use WinRM.
- **Integration with KACE Systems Deployment Appliance (SDA)**: The KACE Agent populates the KACE SDA configuration information on the KACE SMA *Device Detail* Inventory view.
- **Urgent alert mode**: A new option is added to the Alert Detail page for Urgent alert mode. When selected, the alert message appears in the center of the screen, without allowing the user to move it, or to send it to the background. The alert must be addressed before any work can continue.
- **Addition of OS-native scripting variable for the native Windows registry space**: Starting in this release, you can add `NAT` to `HKLM` (`HKEY_LOCAL_MACHINE`) to access 32- or 64-bit registry space in script tasks, as needed. For example: `HKLMNAT\Software\ABC`.

Infrastructure features

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

- **KACE SMA patching solution**: A complete KACE SMA patching solution for MS Windows and Mac OS is added in this release. Patch packages are downloaded from Quest according to the subscription and download options you select. In some cases, patch packages are also downloaded directly from vendors. Quest provides safe, timely, and high-quality patch signatures for Windows and Mac operating systems, and many popular applications.

  NOTE: Prior to using this feature, after upgrading to 10.0, you must run a patch download.

  - Smart Labels created prior to version 6.0 need to be manually upgraded before applying 10.0, to a wizard-based version.
  - Upgrading to 10.0 with large number of detect or deploy patch results might result in longer than usual upgrade times.
  - After upgrading to this version, an alert appears on the *Summary* page that lists any deprecated reports, ticket rules, or custom filters.
  - A new built-in report, *Software Catalog Applications Discovered but Unavailable in Application Patching*, is available to show software discovered in the Software Catalog that cannot be patched by KACE patching. This may help while auditing third-party software for security updates.
  - A new report, *KACE Patch Mismatches* is included in this release. During the upgrade process, existing patching data is converted to the new format when possible. This report lists patches that can not be converted.

- **Using Security Assertion Markup Language (SAML) for single sign-on**: You can configure the appliance to authenticate users without providing their credentials on the Welcome page using a third-party authentication tool. SAML is an XML-based protocol that uses security tokens between identity and service providers. The security tokens contain assertion elements that provide information about the user's identity. Use the *SAML Settings* page to configure this feature.
- **Ability to send data to a Syslog server**: You can now configure the appliance to send limited server log data to a remote `Syslog` server. To do that, on the *Security Settings* page, select **Enable remote syslog**,

and in the *Remote Syslog Server* field, specify the fully qualified domain name (FQDN) or IP address and the port number of the remote `Syslog` server.

- **Number of affected devices available for software inventory**: The *Software* list page now includes the *Devices Affected* field in the Advanced Search.
- **Shifting the focus on list pages to support barcode scanning**. When loading a list page, the focus switches to the search box on the page. This can be seen by the cursor being in the text box. This is implemented to enable support for barcode scanning.

Resolved issues

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

Table 1. Resolved Issues

Resolved issue	Issue ID
Installation through KACE Cloud Mobile Device Manager (MDM) provisioning could fail due to expired certificate with 9.1.204 Mac OS agent installer.	K1-20620
Mac OS profile upload may result in error.	K1-20563
Mac OS profile upload resulted in `Class 'NetworkSettingsUtil' not found.`	K1-20561
It was not possible to view archived parent tickets.	K1-20557
Special characters in Western European (ISO) encoded emails did not display correctly.	K1-20549
Some models of Dell Chromebooks could fail to be detected with manufacturer listed as Dell.	K1-20544
Backup files could be unnecessarily large.	K1-20543
License Compliance data might not update if it overlapped with backup window.	K1-20542
Patch schedule *Detect Timeout* and *Deploy Timeout* options above two hours were available for selection (and they should not be).	K1-20533
Comment new lines were run together when coming from Process Template.	K1-20528
Work information was sometimes not displayed after page reload on the *Ticket Details* page.	K1-20522
Inbound Email tokens did not work when being sent from a ticket rule.	K1-20458
Agent was sometimes recognized as anti-virus software due to expired certificate.	K1-20457
Compliance data could take unnecessarily long to update.	K1-20450
Incoming HTML email did not decode special characters such as non-breaking spaces (NBSP).	K1-20448

Resolved issue	Issue ID
Wizard asset report involving custom user field was blank unless `OWNER_ID` was set.	K1-20446
Asset import did not set `OWNER_ID` for non-device types.	K1-20445
Users with no email set could see tickets that do not belong to them in the *Tickets* list page.	K1-20441
Missing in action (MIA): Archive did not work as expected for devices without corresponding assets.	K1-20438
Asset archival could fail to run per schedule if a backup was in progress.	K1-20431
Loading of a software *Asset Detail* page could be slow if there was a high number of installed software items.	K1-20430
Patching: OS Selection was removed on save without notification when selecting all devices.	K1-20417
Non-default permissions could prevent the Kace GO mobile app from accurately listing devices.	K1-20405
Change Location pop-up box did not display in French locale.	K1-20400
Creating new asset could set the default subtype to *None* instead of the default subtype.	K1-20398
Items removed before being completely replicated could still show up in the *ToDo* list.	K1-20396
Provisioning schedules list did not display hours or minutes for *run every* or *run on* schedule.	K1-20394
A warranty check of Dell devices resulting in *Invalid* could prevent future warranty checks of the same device.	K1-20385
A discovery smart label with invalid SQL could result in the entire scan failing.	K1-20374
Multiple users could be created when submitting ticket by email using archived user.	K1-20369
Email notifications of ticket updates could fail to be generated.	K1-20360
Links in scheduled HTML wizard reports failed when report is opened through email.	K1-20351
The *Devices* drop-down box on the *Run Now* script page could take a long time when using device scope labels.	K1-20347
Large asset history deletion could fail.	K1-20344
Task Schedule could sometimes fail to load on an appliance with many replicators.	K1-20342
The `Browse Tree` option in the *LDAP Browser* could fail to execute.	K1-20327

Resolved issue	Issue ID
Mac Profiles failed to deploy due to an incorrect agent path.	K1-20321
Ticket was displayed in the *All My Tickets* view when a user with similar email was added to the CC list.	K1-20304
Dark theme text/background in the Process wizard lacked contrast.	K1-20290
Agent installer could mistakenly update third-party `userinit` values if they contained the substring `userinit.exe`.	K1-20286
Some provisioned virtual machine devices did not dislay the VMware device actions on the *Device Detail* page.	K1-20285
Canned Report: Computers listed by free capacity ranges improperly grouped results.	K1-20275
`Parent approval required before ticket can be closed` message could be seen, by mistake.	K1-20267
Advanced Search on the *Status* field was not working on the *Patch Catalog* page.	K1-20091
Metering icon could be mistakenly displayed for Windows agentless devices that had the metering label added.	K1-20061
Timeout setting in discovery schedules did not behave as expected.	K1-20012
Chip count in inventory could be wrong for Raspbery Pi.	K1-20007
Blank or duplicate BIOS serial number with accompanying duplicate MAC address could incorrectly cause inventory records to be overwritten.	K1-19988
Blacklisting processes did not always terminate the entire process tree. This caused orphaned child processes and in extreme cases could exhaust memory on the endpoint.	K1-19905
When using offline patching, offline source and target could have different active, inactive, and disabled counts.	K1-19873
Patch feed emails could fail to send due to not respecting SMTP configuration on network settings.	K1-19816
Advanced Search *does not begin with* fails for groups such as Label Names and Software Titles.	K1-19814
Dell BIOS update might not reboot the client when pushed, preventing it from being installed completely until after a reboot.	K1-19770
Canned Report: *Users Added or Modified in Last 7 Calendar Days* was inaccurate.	K1-19703
New line character in Dell Updates reboot message could cause the reboot from being completed.	K1-19569

Resolved issue	Issue ID
Manually added devices could be mistakenly deleted by the nightly MIA cleanup process.	K1-19531
MI Deploy Order might not be correctly enforced between Software and Catalog Software Managed Installations (MIs).	K1-19512
When a software inventory item contained non-English characters, smart labels could fail to execute correctly.	K1-19507
The formatting in a customer defined *Patch Reboot* message was not respected.	K1-19492
LDAP Import could exclude attributes not found on all records.	K1-19406
A Custom user field for an asset incorrectly mapped to assigned users in reports.	K1-19226
The *Software* Inventory page could take a long time to load.	K1-18985
Patch download failures could be incorrectly reported.	K1-18930
When clicking the error link in the *Patch Catalog*, an incorrect *No Devices Found* message might appear.	K1-18721
Smart Labels targeting software title and version could return incorrect results.	K1-18398
The patching reboot message appearing on the client machine might not reflect what is configured in the patch schedule.	K1-18215
Erroneous question mark character '?' was observed in the KACE SMA console hosted on Azure.	ESMP-6820
Comment section for tickets did not clear when adding comment and attachment at the same time.	ESMP-6672
Ticket could be merged to a closed ticket.	ESMP-6671
Search functionality was broken for restricted user when view by option is set as *My Items*.	ESMP-6633
Blank *Patch Detail* page on clicking the patch under the *Supersedes* section on the *Patch Detail* page.	ESMP-6591
Processing agent inventories with a missing list of network interfaces might fail.	ESMP-6588
The *SDA settings* section was missing from the *Fields to Display* page of the System report wizard.	ESMP-6468
Search for devices with *SDA Deployment Time* was not working on the *Devices* list page with Advanced Search.	ESMP-6467

Resolved issue	Issue ID
HTML tags sometimes appeared under in the *Comments & Resolution* column in Service Desk Reports.	ESMAS-4552
Merging two tickets with the same submitter added them to the CC list.	ESMAS-4537
Submitters could not see their tickets if tickets moved into queue where submitter did not have any permissions.	ESMAS-4516
It was not possible to sort by *Type* column under *Assigned Assets* section on *Location Detail* page.	ESMAM-1897

Known issues

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

Table 2. General known issues

Known issue	Issue ID
WinRM: Provisioning to newer versions of MS Windows devices using alternate location is not supported.	K1-20616
`TICK:XXXX` links in the comment section no longer work.	K1-20558
Redirect errors may be seen after upgrade is complete. **Workaround**: Clear the cache and restart the browser.	ESMP-7010
If *Detect All Patches* is used, timeout errors may occur.	ESMP-7005
SAML attribute mappings are currently case sensitive.	ESMP-6887
Mac OS patches in manual labels disappear from the label after upgrading to 10.0.	ESMP-6536
OVAL scan fails on Windows Server 2019 with Timeout error.	ESMP-6535
Patching: Old custom ticket rules that reference patching no longer work.	ESMP-6176
`KUserAlert` can render incorrectly on MS Windows 7 when fonts are set to 125% or 150%.	ESMEC-3461
The SNMP walk data is not available in the discovery results and inventory data when using SNMP version 'SNMPv2c' for some Microsoft Windows devices. The affected Windows devices are: • Windows 10 (1709 and later) • Windows Server 2016 (1709 and later) • Windows Server 2019 (all versions) **Workaround**: Select the SNMP version *SNMPv1* to prevent this problem.	ESMEC-3263

Known issue	Issue ID
The KACE Agent is not supported on SUSE Linux Enterprise Server version 15 and openSUSE Leap version 15 devices when SELinux is installed and enabled.	ESMEC-3100
Agent fails to install on SLES v.15 with errors. **Workaround**: Before installing the agent on SLES v.15, ensure the system has the following packages installed: • `cups-client` • `pciutils` • `psmisc`	ESMEC-2987
Import and Export of ticket templates in queue configuration (as a resource) is not currently supported.	ESMAS-4631
SAML single sign on is not currently supported in KACE GO.	ESMAS-4585

System requirements

The minimum version required for installing KACE SMA 10.0 is 9.1. 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 7.1. We recommend running the latest agent version with KACE SMA 10.0.

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 10.0, 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/10.0-common-documents/technical-specifications-for-virtual-appliances/.
- For KACE as a Service: Go to https://support.quest.com/technical-documents/kace-systems-management-appliance/10.0-common-documents/technical-specifications-for-kace-as-a-service/.

VMware ESX/ESXi requirements in 10.x

KACE SMA is a virtual appliance that runs on a virtual machine that is part of a VMware or Microsoft Hyper-V infrastructure. Starting in this release, the appliance includes an upgraded version of its core FreeBSD Operating System 12.0, patch 10. While some earlier versions of ESX/ESXi, such as 6.5, are still in active support, VMware officially supports FreeBSD 12.0 only in ESX/ESXi 6.7. For that reason, Quest Software strongly recommends you to upgrade your VMware ESX/ESXi environment to a version that supports FreeBSD 12.x immediately. We also encourage you to upgrade the appliance to version 10.0, and continue taking advantage of the appliance's patching solution after February 1st, 2020, along with any other features and improvements.

If you choose to run the KACE SMA 10.x on ESX/ESXi 6.5, this is at your own risk. If any investigation by Technical Support concludes that an issue is a potential result of the appliance being run on ESX/ESXi 6.5, our team may request from you to upgrade to a supported version of ESX/ESXi, in order to continue with troubleshooting.

For more information, visit https://support.quest.com/kace-systems-management-appliance/kb/313646.

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 10.0 can be used only on KACE SMA appliances running version 6.3 or later. Version 10.0 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 10.0 is 9.1. 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 7.1. We recommend running the latest agent version with KACE SMA 10.0.

- **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/10.0-common-documents/administrator-guide/.

- **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/10.0-common-documents/administrator-guide/.
2. Go to the appliance *Control Panel*:
   - If the Organization component is not enabled on the appliance, click **Settings**.
   - If the Organization component is enabled on the appliance: Log in to the appliance System Administration Console: `http://`KACE_SMA_hostname`/system`, or select **System** in the drop-down list in the top-right corner of the page, then click **Settings**.
3. On the left navigation bar, click **Appliance Updates** to display the *Appliance Updates* page.
4. Click **Check for updates**.

   Results of the check appear in the log.
5. When an update is available, click **Update**.

   IMPORTANT: During the first ten minutes, some browsers might appear to freeze while the update is being unpacked and verified. Do not navigate away from the page, refresh the page, or click any browser buttons on the page during this time because these actions interrupt the process. After the update is unpacked and verified, the *Logs* page appears. Do not manually reboot the appliance at any time during the update process.

   Version 10.0 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 10.0.

Upload and apply an update manually

If you have an update file from Quest, you can upload that file manually to update the KACE 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/10.0-common-documents/administrator-guide/.
2. Using your customer login credentials, log in to the Quest website at https://support.quest.com/kace-systems-management-appliance/download-new-releases, download the KACE SMA server `.kbin` file for the 10.0 GA (general availability) release, and save the file locally.
3. On the left navigation bar, click **Appliance Updates** to display the *Appliance Updates* page.
4. In the *Manually Update* section:
   a. Click **Browse** or **Choose File**, and locate the update file.
   b. Click **Update**, then click **Yes** to confirm.

Version 10.0 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 10.0.

Post-update tasks

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

Verify successful completion

Verify successful completion by viewing the KACE 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/10.0/technical-documents)
  - **Technical specifications**: Information on the minimum requirements for installing or upgrading to the latest version of the product.

    For virtual appliances: Go to https://support.quest.com/technical-documents/kace-systems-management-appliance/10.0-common-documents/technical-specifications-for-virtual-appliances/.
    For KACE as a Service: Go to https://support.quest.com/technical-documents/kace-systems-management-appliance/10.0-common-documents/technical-specifications-for-kace-as-a-service/.
  - **Setup guides**: Instructions for setting up virtual appliances. Go to https://support.quest.com/kace-systems-management-appliance/10.0/technical-documents to view documentation for the latest release.
  - **Administrator guide**: Instructions for using the appliance. Go to https://support.quest.com/technical-documents/kace-systems-management-appliance/10.0-common-documents/administrator-guide/ to view documentation for the latest release.

Globalization

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

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

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

About us

Quest 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

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.

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 - February 2020

Software Version - 10.0