

Quest®



KACE® Systems Management Appliance 11.0

Release Notes



# Table of Contents

Quest® KACE® Systems Management Appliance 11.0 Release Notes.....	3
About KACE Systems Management Appliance 11.0.....	3
New features and enhancements.....	3
Enhancements.....	5
Resolved issues.....	5
Known issues.....	10
System requirements.....	11
Product licensing.....	12
Installation instructions.....	12
Prepare for the update.....	12
Update the KACE Systems Management Appliance server using an advertised update.....	13
Upload and apply an update manually.....	14
Post-update tasks.....	14
Verify successful completion.....	14
Verify security settings.....	15
More resources.....	15
Globalization.....	16
About us.....	16
Technical support resources.....	16
Legal notices.....	16

# Quest® KACE® Systems Management Appliance 11.0 Release Notes

---

This document provides information about the KACE Systems Management Appliance version 11.0.

## About KACE Systems Management Appliance 11.0

KACE Systems Management Appliance is a virtual appliance designed to automate device management, application deployment, patching, asset management, and Service Desk ticket management. For more information about KACE Systems Management Appliance series, go to <https://www.quest.com/products/kace-systems-management-appliance/>. This release contains a number of new features, resolved issues, and security enhancements.



**NOTE:** This is the only document that is translated for this release, however the localized variants do not include information about resolve issues, enhancements, and known issues. Other guides, such as the *Administrator Guide* and in-product help are not localized at this time, and version 10.2 documents are included.

## New features and enhancements

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

### Patching

- **Windows On-demand Deploy for patches:** The appliance supports a new patch schedule type that allows end users to trigger a deploy action using a tray icon.
- **Security Dashboard:** A new *Security* dashboard enables a much easier understanding of the patching state of the devices in inventory.
- **Patch Schedule Wizard and Patch Results:** This version includes a new workflow for creating patch schedules, and presents patching results in a way that is easier to understand.

### Device security

- **Device security improvements:** Security improvements are added in this release, such as agent quarantine measures, to provide more options for securing the communication channels, including auto-assignment to organizations based on tokens.
  - The appliance can now distinguish between the agents connecting externally (outside the firewall) and those connecting internally. In addition to the existing behavior of listening on port 443, the appliance also listens on port 52230 for agent connections only. Using a split DNS configuration and configuring the firewall to forward external port 443 to port 52230 on the appliance, you can identify agents as being internal or external.

To allow exposing the appliance to the internet and maximize security, port 52230 does not allow access to the appliance's web interface. If you want to have outside access to the appliance's web interface, then do not configure 443 to 52230 port forward on the firewall.

For more information, review this Knowledge Base article: <https://go.kace.com/to/k1000-external-agent-port>.

- **General server security enhancements:** The appliance includes several security enhancements in this version. Appliance user interface hardening along with agent tunneling and quarantine allow for a much more secure deployment, inside or outside of the demilitarized zone (DMZ).



**NOTE:** Communication between the KACE Agent and the appliance occurs over a proprietary KACE tunnel which is encrypted using the TLS 1.3 protocol. The agent sends and receives unencrypted data through the TLS 1.3-encrypted KACE tunnel.

#### KACE GO app

- **Ticket approval:** You can now approve Service Desk tickets in the KACE GO app.
- **HTML editor:** An HTML editor is added to the *Summary*, *Resolution*, and *Comments* ticket fields, helping you to improve the readability of entered contents using common formatting tags.

#### Administrator Console

- **Embedded videos:** Starting in this release, the slide-out help allows you to browse through any available training videos associated with the current page. You can play a video on the help pane, in a smaller window outside of the page, or on the target Knowledge Base page that hosts the video.
- **Improved left-side navigation:** Selecting an item in the left pane now only expands the menu, without opening the page associated with the top item. You can also expand multiple top-level menus at once, allowing you to better understand the product.
- **Custom logos:** Customer-provided appliance logos can now be defined in the Administrator Console and the System Administration Console.
- **Background color for a custom login portal:** Login portal background color can now be customized for all user interfaces.



**NOTE:** The color chooser is not supported in Internet Explorer 11.

- **Automatic organization selection at login:** Each organization-specific Administrator Console and User Console can be accessed directly using virtual IP or host name configuration. This allows users to bypass organization selection at login.

#### Service Desk

- **Ticket template improvements:** A new layout is added to Service Desk ticket templates, helping you better organize the ticket contents if the template includes fields of variable height. You can also break up ticket contents into separate sections using a separator.
- **Embedded images and screen shots in ticket fields:** You can now include images and screen shots in the ticket *Summary* and *Comments* fields, allowing you to better communicate ticket-related issues.
- **“Take this ticket” shortcut:** The *Tickets* list page includes a new control that you can use to quickly assign a ticket to yourself.
- **Process ticket improvements:** You can quickly create a process ticket by email for an existing process template by specifying the process template name in the *Subject* field. You can also schedule ticket processes to begin on a specified recurring schedule.



**NOTE:** In previous versions, ticket archival schedules allowed you to select *None* as the schedule option. This option is removed in this release and if you previously had any ticket archival schedules using this option, after the upgrade, they will be automatically updated to run every day.

## Other features

- **Credential manager updates:** LDAP Label configurations can now use the Credential Manager to store and share credentials.
- **Ability to add categories to scripts:** Each script may be sorted or filtered by an assigned custom category.
- **New VMware widgets on the Inventory dashboard:** The following widgets are added to the *Inventory* Dashboard: VMware Device Counts, VMware ESXi Version Counts, VMware Device Reports, and VMware ESXi Device By Status.
- **New OS support:** This release includes support for CentOS 6 to 8.



**NOTE:** *Charlie Root* emails generated by the appliance did not contain useful information and often lead to confusion. For that reason, these emails are no longer generated and sent to the administrator. For more information, see K1-21001 in [Resolved issues](#).

# Enhancements

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

Enhancement	Issue ID
It was not possible to allow Credentials specific access through Roles.	K1-20924
FTP/SFTP offboard backup improved performance and Public Key Authentication for SFTP.	ESMP-7444
Managed OS widget in Dashboard did not display version number.	ESMP-6448
<i>Customize User Fields</i> is now accessible through the <i>Choose Action</i> menu on the <i>Users</i> list page.	ESMP-6113
It was not possible to reset history settings to default values.	ESMP-5916
Agentless support for vSphere 7.0 is added in this release.	ESMEC-3557

# Resolved issues

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

Resolved issue	Issue ID
Offline appliance could not to run patch detects with <code>version-check</code> failed errors.	K1-21171
Workspace ONE Discovery/Inventory did not respect user domain provided in the credentials.	K1-21145
Windows Feature Update could report that it was not applicable because user locale is set as non-English.	K1-21101

Resolved issue	Issue ID
Unknown user rejection email was not be sent in some cases.	K1-21081
POP3: Failure to process one email could prevent further emails from being processed.	K1-21077
Reset tries in the Windows Feature Update Catalog Detail page did not work as expected.	K1-21074
Ticket load time performance was sometimes degraded with many associated child tickets.	K1-21073
Replication Share Inventory did not run after regular agent inventory in some cases.	K1-21070
When using Office 365 with OAuth, an Invalid header value detected message could be seen when the display name contains Unicode characters.	K1-21066
Some Dell Updates did not appear in the list of available updates in the Administrator Console, even though they did exist on the appliance.	K1-21053
Service Desk Templates: Conditional Logic involving Owner and null usage did not work as expected.	K1-21050
Windows Feature Update could fail on lower specification systems if any of the individual steps during the update itself exceeded the global agent process time out set in the appliance.	K1-21048
Hyperlink to archived/merged tickets was sometimes incorrect, causing an error.	K1-21043
Re-enabling appliance backups could give an incorrect error message.	K1-21041
An email sent to a Service Desk queue with multiple addresses in the To line could produce unexpected results.	K1-21036
The &nbsp; character was not decoded correctly in Gmail messages when using OAuth.	K1-21035
MSG files uploaded to Attachment type Asset Fields open in browser instead of downloading.	K1-21033
Windows Feature Update payload files for unsubscribed locales could be incorrectly downloaded.	K1-21031
Asset Import schedule creation or modification inserted blank/duplicate rows in IM_CRON.	K1-21026
SFTP full path was not retained when editing an existing asset import schedule.	K1-21015
With multiple NICs, using Add to SDA Boot Action on a device sometimes did not work as expected.	K1-21011
<i>K1000 Discovery Completed</i> email is missing the schedule name in the body.	K1-21010

Resolved issue	Issue ID
The <i>Patch Schedule</i> page did not prompt the user to save when clicking <b>Run Now</b> , after changing the device label.	K1-21009
An error page appeared while trying to save a blank Mac profile without a configuration.	K1-21004
When creating a new Organization, incorrect date for <i>Last updated</i> was displayed.	K1-21003
The appliance generated spurious <i>Charlie Root</i> emails which did not contain useful information.	K1-21001
Adding the <code>related_tickets</code> shaping option to fetch ticket list API call did not work as expected	K1-20994
Windows Feature Update schedule sometimes had incorrect Build section if no Windows Feature Update signatures were downloaded.	K1-20985
LDAP labels could not be applied at login for Security Assertion Markup Language (SAML) accounts.	K1-20978
An error displayed while using description as a Smart Label criteria on the <i>Patch Catalog</i> list page.	K1-20975
Dell Warranty not updated when <code>PARENT_SERVICE_TAG</code> was null.	K1-20972
The <i>Smart Labels</i> list page was missing the <i>View By</i> filter.	K1-20968
Primary Device is not automatically set when a user submits a ticket.	K1-20966
The <i>Manage Associated Labels</i> dialog box search only had "begins with" type searching.	K1-20963
When Access Control List blocked access to the Administrator Console, SAML did not work for the User Portal.	K1-20958
Comment appended to Service Desk parent ticket on last child close was missing the ticket ID.	K1-20954
Using a custom date time format for monitoring failed when microseconds were part of the timestamp.	K1-20952
Kbot script task of creating a message window displayed the snooze option that was not used.	K1-20946
<i>SDA Deployment Time</i> was missing the UTC offset.	K1-20931
Microsoft Surface devices were being classified incorrectly as virtual devices.	K1-20929
It was not possible to hide the <i>Location</i> field on <i>License Asset Type</i>	K1-20923

Resolved issue	Issue ID
Default CC was not added to <code>CC_List</code> , resulting in ticket not showing in the ticket list.	K1-20922
AirWatch/Workspace ONE: auto-provisioning duplicated devices without a MAC address.	K1-20915
Sending email to ticket that queue owner did not own prevented them from being added to the CC list.	K1-20899
<code>RegistryValue</code> -related custom inventory rule was not evaluated correctly for numeric values that exceeded max unsigned integer value.	K1-20893
When setting ticket <i>Due Date</i> to <i>Always Required</i> , the default option did not force the date to be selected.	K1-20890
Using the <i>Download Status</i> did not list patches with multiple files when not all of them were applicable.	K1-20869
Managed Installation (MI) sort by date ( <i>Created</i> or <i>Modified</i> ) incorrectly sorted by the first digit only.	K1-20801
It was not possible to add or delete a manual label if a device did not have an associated asset.	K1-20776
IP Address sorting was not working as expected on the <i>Devices</i> list page.	K1-20756
Custom ticket fields: Setting the user type to <i>Always Required</i> did not prevent the ticket from being saved.	K1-20755
Operating system name was missing in tracked history while selecting OS on the <i>Replication</i> list page.	K1-20711
Link was missing for the Patch Schedule name on the <i>Object History</i> list page.	K1-20706
Replication sometimes failed to copy all files when the replicating Agent runs on a Mac OS or Linux.	K1-20691
Asset History check boxes could clear when canceling and saving.	K1-20684
Scheduled Report emailed empty files when the reports temporary directory was too large.	K1-20675
<i>Export All</i> on the <i>Devices</i> list page <i>Choose Action</i> menu ran out of memory with a large number of devices.	K1-20672
Single select field with quote wrapped items including commas were split by the comma in KACE GO, preventing tickets from being saved.	K1-20668
On the <i>Queue Detail</i> page, under <i>Archive Preferences</i> , the <b>Run Now</b> button allowed multiple clicks, causing unexpected results.	K1-20658



Resolved issue	Issue ID
Archive purge never occurred if <i>Archive schedule</i> was set to <i>None</i> .	K1-20657
If inventory contains an emoji character (for example, in a file name), the appliance failed to parse the inventory properly.	K1-20649
Fields exported from the <i>Devices</i> list page did not include all options.	K1-20631
The <code>RegistryValueReturn</code> custom inventory rule was not evaluated correctly for values under <code>HKCurrentUser</code> on non-English OS.	K1-20622
Single sign-on with Azure AD could cause synchronization failures.	K1-20585
The <i>Assets by Location</i> widget showed inaccurate percentages.	K1-20565
Unwanted history was tracked in the <i>Relay Machine</i> field while trying to create or modify any agentless devices.	K1-20486
Custom User fields with a <i>Required</i> flag were not handled properly during LDAP import.	K1-20389
Organization LDAP Filter test could fail due to improper variable or wildcard substitution.	K1-20333
Under <i>Asset History Configuration</i> , clearing the boxes related to <i>Connection</i> and <b>Disconnection</b> did not prevent those entries from being logged.	K1-20307
A date in a Provisioning schedule name could result in an error when accessing the <i>Search Scripting Logs</i> tab.	K1-20256
The <i>Device</i> detail page performance could be affected (or the page may fail to load) due to a large number of associated asset history records.	K1-19881
The <i>Last Update</i> column on the <i>Patch Schedule</i> list page did not sort correctly.	K1-19777
The KACE Agent could not extract zip files larger than 5 GB, created using the MS Windows Explorer's built in ZIP mechanism.	K1-17274
Scripts created through the MSI policy wizard did not work for software inside a ZIP file.	K1-17264
Asset History: Clearing field selections did not clean up the <code>ASSET_HISTORY</code> table.	ESMP-7504
If 2FA was enabled on the appliance, <i>Import Managed Installations</i> could not work as expected.	ESMP-7120
KACE Cloud Mobile Device Manager was not passing the correct license value if the device was not enrolled.	ESMEC-3838
KACE Cloud Mobile Device Manager/KACE hybrid agent would get stuck if the agentless record is deleted during agentless provisioning.	ESMEC-3837

Resolved issue	Issue ID
The KACE menu application did not load the correct system locale when locale changed.	ESMEC-3765
Multiple <code>explorer.exe</code> processes on Windows caused launch in active desktop and launch in sessions to misbehave.	ESMEC-3529
GET calls to obtain work item associated to a ticket sometimes did not work as expected.	ESMAS-4891
Using the API, administrators can now move tickets to another queue.	ESMAS-4888
In KACE GO app, when a device or machine is a required field, this did not appear when a user created a ticket, resulting in the <code>Missing required field</code> error.	ESMAS-4843
Moving parent ticket to a new process type bypassed approvals.	ESMAS-4758
Bold formatting did work in HTML editor (such as response templates or ticket entries) in some browsers and operating systems.	ESMAS-4619
Rolling back product suite patches could sometimes remove only one of the available components such as on Office 2016.	ESMAM-2722

## Known issues

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

Known issue	Issue ID
Asset Import does not change Assignee information.	K1-21185
Inserting code snippets or other unexpected characters in a script's note may cause an error.	K1-21184
User Custom Fields may not be listed in the Column selector drop-down in the <i>Users</i> list page.	K1-21179
Offline KScripts do not run when scheduled for <i>Run on the instance/day of week</i> .	K1-21173
The <b>Reset Tries</b> button in the <i>Windows Feature Update Status</i> section on the <i>Device Detail</i> page may not work.	K1-21172
Parent ticket appears to be in process when child tickets are closed from <i>Tickets</i> list view.	K1-21143
Response Templates marked public are only editable by the creator.	K1-21130
Unexpected behavior observed when trying to map and update the Manager field using SAML.	K1-21102

Known issue	Issue ID
POP3 and IMAP cannot use self-signed certificates for inbound email.	K1-21086
Invalid filters (Smart Labels) can be saved, resulting in Smart Labels that never populate.	K1-20268
An error may be seen while creating custom view on the <i>Quarantine</i> page in the System Administration Console.	ESMP-7825
On the <i>Agent Tokens</i> list page, in the <b>Choose Action</b> menu, selecting <b>Create Report</b> does not work as expected.	ESMP-7799
In the System Administration Console, the <i>Agent Token Detail</i> page displays the organization ID instead of the name.	ESMP-7793
Device links on the <i>Agent Command Queue</i> and <i>Agent Task Status</i> pages may not function as expected.	ESMP-7774
<i>Do not associate file</i> Managed Installation option does not display correctly after saving.	ESMP-7753
<i>Token Usage by Machine</i> record is not updated when machine changes token or is removed from list.	ESMP-7588
Recurring alert messages keep spawning new windows on the device.	ESMEC-3913
Wake-on-LAN (WoL) through relay does not display error when the relay agent selected is down.	ESMEC-3898
Monitoring can fail with error in the Mac OS 11 system log because it has multi-line entries in <code>system.log</code> .	ESMEC-3883
Existing Patch Schedule name is allowed when duplicating the schedule.	ESMAM-2863
In KACE GO, any ticket attachments past the fifth on a single comment are not saved correctly.	ESMAS-5006

## System requirements

The minimum version required for installing KACE Systems Management Appliance 11.0 is 10.2. If your appliance is running an earlier version, you must update to the listed version before proceeding with the installation.

The minimum version required for upgrading the KACE Agent is 9.0. We recommend running the latest agent version with KACE Systems Management Appliance 11.0.

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 11.0, make sure that your system meets the minimum requirements. These requirements are available in the KACE Systems Management Appliance technical specifications.

- For virtual appliances: Go to <https://support.quest.com/technical-documents/kace-systems-management-appliance/11.0-common-documents/technical-specifications-for-virtual-appliances/>.
- For KACE as a Service: Go to <https://support.quest.com/technical-documents/kace-systems-management-appliance/11.0-common-documents/technical-specifications-for-kace-as-a-service/>.

## Product licensing

If you currently have a KACE Systems Management Appliance product license, no additional license is required.

If you are using KACE Systems Management Appliance for the first time, see the appliance setup guide for product licensing details. Go to [More resources](#) to view the appropriate guide.



**NOTE:** Product licenses for version 11.0 can be used only on KACE Systems Management Appliance running version 11.0 or later. Version 11.0 licenses cannot be used on appliances running earlier versions of the appliance, such as 9.0.

## Installation instructions

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

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



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

## Prepare for the update

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

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

The minimum version required for installing KACE Systems Management Appliance 11.0 is 10.2. If your appliance is running an earlier version, you must update to the listed version before proceeding with the installation.

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

The minimum version required for upgrading the KACE Agent is 9.0. We recommend running the latest agent version with KACE Systems Management Appliance 11.0.
- **Back up before you start.**

Back up your database and files and save your backups to a location outside the KACE Systems Management Appliance server for future reference. For instructions on backing up your database and files, see the Administrator Guide, <https://support.quest.com/technical-documents/kace-systems-management-appliance/11.0-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 11.0. 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 11.0. It also features better security and performance.

To determine if your system would benefit from such an upgrade, you can use a `KBIN` file to determine the exact age of your appliance and its disk layout. To download the `KBIN`, visit <https://support.quest.com/kace-systems-management-appliance/kb/210267/how-to-run-the-kace-systems-management-appliance-configuration-report>.

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

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

## Update the KACE Systems Management Appliance server using an advertised update

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

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

1. Back up your database and files. For instructions, see the Administrator Guide, <https://support.quest.com/technical-documents/kace-systems-management-appliance/11.0-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 11.0 is applied and the KACE Systems Management Appliance server restarts. Progress appears in the browser window and in the Administrator Console.

6. When the server upgrade finishes, upgrade all of your agents to version 11.0.

## Upload and apply an update manually

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



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

1. Back up your database and files. For instructions, see the Administrator Guide, <https://support.quest.com/technical-documents/kace-systems-management-appliance/11.0-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 Systems Management Appliance server .kbin file for the 11.0 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 11.0 is applied and the KACE Systems Management Appliance server restarts. Progress appears in the browser window and in the Administrator Console.

5. When the server upgrade finishes, upgrade all of your agents to version 11.0.

## 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 Systems Management Appliance version number.

1. Go to the appliance *Control Panel*:
  - If the Organization component is not enabled on the appliance, click **Settings**.
  - If the Organization component is enabled on the appliance: Log in to the appliance System Administration Console: `http://KACE_SMA_hostname/system`, or select **System** in the drop-down list in the top-right corner of the page, then click **Settings**.
2. To verify the current version, click **Need Help** in the upper-right corner of the page, and in the help panel that appears, at the bottom, click the circled **i** button.

## Verify security settings

To enhance security, database access over HTTP and FTP is disabled during the update. If you use these methods to access database files, change the security settings after the update as needed.

1. Go to the appliance *Control Panel*:
  - If the Organization component is not enabled on the appliance, click **Settings**.
  - If the Organization component is enabled on the appliance: Log in to the appliance System Administration Console: `http://KACE_SMA_hostname/system`, or select **System** in the drop-down list in the top-right corner of the page, then click **Settings**.
2. On the left navigation bar, click **Security Settings** to display the *Security Settings* page.
3. In the top section of the page, change the following settings:
  - **Enable Secure backup files**: Clear this check box to enable users to access database backup files using HTTP without authentication.
  - **Enable Database Access**: Select this check box to enable users to access the database over port 3306.
  - **Enable Backup via FTP**: Select this check box to enable users to access database backup files using FTP.

 **CAUTION:** Changing these settings decreases the security of the database and is not recommended.

4. Click **Save**.
5. **KBIN upgrades only.** Harden root password (2FA) access to the appliance.
  - a. In the System Administration Console, click **Settings > Support**.
  - b. On the *Support* page, under *Troubleshooting Tools*, click **Two-Factor Authentication**.
  - c. On the *Support Two-Factor Authentication* page, click **Replace Secret Key**.
  - d. Record the tokens and place this information in a secure location.

## More resources

Additional information is available from the following:

- Online product documentation (<https://support.quest.com/kace-systems-management-appliance/11.0/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/11.0-common-documents/technical-specifications-for-virtual-appliances/>.  
**For KACE as a Service:** Go to <https://support.quest.com/technical-documents/kace-systems-management-appliance/11.0-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/11.0/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/11.0-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 creates software solutions that make the benefits of new technology real in an increasingly complex IT landscape. From database and systems management, to Active Directory and Office 365 management, and cyber security resilience, Quest helps customers solve their next IT challenge now. Around the globe, more than 130,000 companies and 95% of the Fortune 500 count on Quest to deliver proactive management and monitoring for the next enterprise initiative, find the next solution for complex Microsoft challenges and stay ahead of the next threat. Quest Software. Where next meets now. For more information, visit [www.quest.com](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

© 2021 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.

#### Patents

Quest Software is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at <https://www.quest.com/legal>.

#### Trademarks

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

#### Legend



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



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

#### KACE Systems Management Appliance Release Notes

Updated - February 2021

Software Version - 11.0