Quest™

KACE® Systems Management Appliance 9.0

Release Notes

Table of Contents

Quest® KACE® Systems Management Appliance 9.0 Release Notes

These release notes document provides information about the KACE Systems Management Appliance (SMA) version 9.0.

About KACE Systems Management Appliance 9.0

KACE Systems Management Appliance (SMA) is a physical or 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/.

New features and enhancements

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

- Service Desk and User Console features
- Asset Management features
- Endpoint communication features
- Infrastructure features

Service Desk and User Console features

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

- **New Service Desk dashboard**: The Service Desk Dashboard provides an overview of Service Desk tickets for the selected organization (if applicable), or the appliance. Use this dashboard to see the related dynamic widgets and links at-a-glance.

i NOTE: If you installed old (non-dynamic) Service Desk widgets, they will not change after upgrading to version 9.0. If you delete them, when you put them back you can only use the dynamic widgets.

- **IT process automation**:

  ◦ A new *Software Request: Approval Required* process template is added to Service Desk. Use this process template to configure User Downloads that require one or more approvals. This template is only available for use with the *User Downloads* page.

  ◦ You can configure items on the *User Downloads* page to require approval, to provide better control over software policies and spending. When a user requests a download or install of an item that requires approval, they are notified that the request is pending approval along with a link to the automatically created process ticket.

  ◦ Starting in this release, you can configure monitoring profiles to automatically create a Service Desk ticket each time the appliance receives a notification, such as an SNMP (Simple Network Management Protocol) trap.

- **Email management**: Administrators can now set up email notifications for all of the queue owners in a queue when a new ticket is submitted through email or the user portal.

- **Process management**: Users can respond to a process request with an approval or rejection, as applicable, by simply replying to the notification email, without having to log in to the *Administrator Console*.

- **Ticket response templates**: Response templates allow you to store common responses that can be entered as comments or resolutions in Service Desk tickets. Each response template is associated with a specific ticket queue and belongs to the user that created it. Response templates flagged as *Public* are available to other technicians in that queue. You can select the applicable response template in the *Comments* and *Resolution* sections of the *Ticket Detail* page.

- **Ticket management**:

  ◦ You can add up to five attachments at a time to an existing ticket.

  ◦ It is now possible to specify the users who have the ability to edit and remove ticket comments. All ticket owners or only those associated with one or more labels (as specified) can update or delete comments.

  ◦ Users that are on the CC list of a ticket can now view those tickets in their *My CC tickets* list.

Asset Management features

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

- **Software License Harvesting Assistant**: Appliance administrators can identify cataloged software that can be uninstalled based on how frequently specific software applications are used on user devices in order to acquire underutilized software and re-use it where needed. Use this feature to easily detect and take action to remove seldom-used software. You have an option to reclaim licenses for a specific software application that has not been used in the last 30, 60, or 90 days, or all associated licenses.

- **Software License management**:

  ◦ The *License Asset Detail* page is reorganized into tabs, to make it more streamlined and easier to use.

  ◦ A single license asset can now include multiple purchase agreements providing the ability to combine all purchases into a total license count, while maintaining purchase history.

  ◦ You can extend maintenance on a license purchase and maintain an audit trail of this transaction and show proof of purchase.

- **Software Catalog customization**: Administrators can manually exclude certain software titles from the license compliance report, to have better control over which titles appear in the report. Use this feature when you want to restrict what items are considered *licensed* software in *License Compliance*, for

example, .NET, Facetime, Spotify, Solitaire, vSphere Client, and so on, and only display what is important to you.

- **Software Catalog improvements**: Several improvements are made in this release to enhance the Software Catalog, including fingerprinting enhancements and database changes.

Endpoint communication features

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

- **Extended set of virtual machine actions**: Starting in this release, the appliance supports basic virtual machine actions, such as power on and off, pause, and reboot.

- **KACE Agent app**: Use the new KACE Agent app to review the status of the KACE Agent, force inventory, and display agent information using the Mac menu bar or Windows system tray, as applicable. The agent app indicates whether the agent is currently connected or disconnected. It also supports several basic right-click operations such as restarting the agent and forcing inventory. To access the app, you must enable the *Agent Status On Device* option under *Communication Settings*.

- **Raspbian Linux support**: The Raspbian Linux OS is now supported on Raspberry Pi devices, for agent-based and agentless management. All features that are currently supported on Linux-based devices, excluding monitoring, are now supported on Raspbian Linux devices.

- **New SNMP templates**. Out-of-box templates are included for the most popular monochrome and color printer devices. This feature takes the work out of configuring your appliance to notify you of low toner, paper jams, fuser issues, and other problems.

- **WinRM and SSH agent tunnel**: Starting in this release, discovery, provisioning and inventory actions are supported using an agent-created traffic tunnel over WinRM (Windows Remote Management), SSH (Secure Shell) or SNMP (Simple Network Management Protocol). Use this feature to designate one remote agent computer to perform agentless discovery, provisioning, and more.

- **Warranty information for HP and Lenovo devices**: The appliance now collects and displays warranty information for HP and Lenovo devices.

  > **i** IMPORTANT: To obtain warranty information, you must configure the manufacturer's warranty API keys. For complete instructions, visit https://go.kace.com/to/k1000-help-warranty.

- **Routing device actions**: When you enable ActiveX in Microsoft Internet Explorer, the device action runs using ActiveX. If ActiveX is disabled, or you want to use a different browser, the Windows device you are running the device action from must have the KACE Agent version 9.0 or later agent installed and connected. When you initiate a device action through the agent, the action executable must be placed in your `%PATH%`.

- **KACE Cloud integration**: To provide continuous integration between KACE Cloud MDM (Mobile Device Manager), additional inventory items that collected by KACE Cloud MDM appear in the appliance inventory. In addition to that, the appliance now alerts the user when KACE Cloud MDM is in maintenance.

Infrastructure features

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

> **i** NOTE: Samba v.1 is disabled by default, but it can be re-enabled by selecting the option on the *Security Settings* page (ESMP-5526).

- **Infrastructure and OS enhancements**:
  - ◦ In this release, the appliance is moving to PHP 7.x.
  - ◦ The appliance OS is upgraded from FreeBSD 11.0 to FreeBSD 11.1.

  This has resulted in significant page load time and reporting speed improvements throughout the appliance.

- **KACE as a Service Setup Wizard**. The KACE as a Service *initial Setup Wizard* now allows you to automatically detect and configure restrictions for a KACE as a Service instance based on the license type.

- **User authentication**:
  - ◦ Two-Factor Authentication (2FA) adds an extra layer of security to your KACE SMA for your peace of mind. Use this feature if you want to provide stronger security for users logging into the appliance. It relies on the Google Authenticator app to generate verification codes. The app generates a new six-digit code at regular intervals. When 2FA is enabled, end users will be prompted for the current verification code each time they log in.
  - ◦ The User Authentication Log is added in this version. The log keeps track of the users who log in to the appliance, their device IP, whether they attempt to log in to the User Console, Administrator Console, or the System Administration Console, their organization name (if applicable), the authentication type, and whether the authentication attempt is successful.

- **User experience and usability improvements**:
  - ◦ You can choose between three color schemes for the user interface that best suits you. The Administration Console appears in a default Light theme for every new user. Two additional themes are available: the Dark and Hybrid themes. You can change the default theme for the appliance, or for your user profile. For example, if the Light theme is set by default for the appliance on the System level, and you associate the Dark theme with your user profile, the Dark theme is applied each time you log in.
  - ◦ A set of consistent schedule options are available across all agent-based detail pages.
  - ◦ The new *Task Schedule* page displays a list of tasks scheduled to run. The contents of this page appear anywhere there is a scheduling widget, and is also accessible from the *Home* tab. Use it to get a quick overview of the type and range of tasks that are scheduled for your organization, or all organizations managed by the appliance. Any tasks that have detail pages associated with them, such as scripts, can be accessed by clicking the task name in the table.

- **Dashboard improvements:**
  - ◦ The new *Inventory Dashboard* provides an overview of managed devices for the selected organization (if applicable), or the appliance. Use this dashboard to see the related widgets and links at-a-glance.

- **Distribution improvements**: A concept of task chains is introduced in this version. A task chain is a collection of tasks that can run in a specific order. You can add one or more scheduled patches, managed installations, scripts, file synchronization items, and Wake-On LAN requests to a task chain. Use task chains, for example, when you need to deploy managed installations and then run scripts on target devices. The order of tasks in a task chain can be easily changed, as required. Each task chain runs against a configured set of devices, as defined in the task chain. If a target device in a task chain is offline, you can configure the task chain to run when the device becomes connected. When a target device is referenced in multiple task chains, only one task chain runs against the device at a time.

- **Offboard backup transfer**: When you run into a problem with the appliance or experience a data loss, if your backup files have not been backed up to an external location, you may not be able to restore the appliance to its previous state. Starting in this release, you can configure the transfer of backup data to an external location automatically. When configured, the appliance copies nightly backup files to an external location each time it completes the backup process.

Resolved issues

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

Table 1. Resolved Endpoint Communication Issues

Resolved issue	Issue ID
Atomic file writes on Windows could cause file corruption during loss of power.	ESMEC-2956
Replication client distribution Linux files are listed with the `.tgz` extension on upgraded appliances only.	ESMEC-2946
9.0 KACE Agent provisioning on Microsoft Windows Vista, base Windows 2008, Windows XP and Windows POS 2009 did not log the `Unsupported Platform` error in provisioning logs.	ESMEC-2929
9.0 KACE Agent was installed on Microsoft Windows Vista, base Windows 2008, Windows XP and Windows POS 2009.	ESMEC-2913
The latest .NET version was not mapped correctly.	ESMEC-2880
The machine serial number was missing from VMware ESXi 6.7 agentless inventory.	ESMEC-2868
Publisher information for `konea.exe, klog.exe, kstatus.exe, kwol.exe` was not present in the inventory data.	ESMEC-2866
The agent message process queue could become backlogged if stuck on a message.	ESMEC-2858
LDAP discovery failed when an IPv6 address was used.	ESMEC-2785
Error 2 was detected in the `KAgent.log` during patching.	ESMEC-2722
Custom Inventory rule `FileInfoReturn(path, attribute, type)` did not work on some Ubuntu platforms.	ESMEC-2706
Users could not specify how many alerts in a single polling session were "too many", and a hard-coded value in the agentless monitoring feature was used instead.	ESMEC-2502

Table 2. Resolved KACE SMA Server Issues

Resolved issue	Issue ID
Service Desk tickets could contain HTML data encoded in the title.	K1-19888
Importing assets could take too long.	K1-19887
Software Asset counts could be wrong when they were regenerated nightly.	K1-19866
The *Critical and Recent* bulletin list could contain incorrect information.	K1-19849

Resolved issue	Issue ID
When using the OS Picker tool, Windows 10 Enterprise LSB (Long Term Servicing Branch) showed up under Windows Server 2016.	K1-19847
Service tests from *Diagnostic Utilities* could indicate incorrect failure on Hyper-V or physical hardware	K1-19820
Queue customization could fail when system was under heavy usage.	K1-19808
LDAP Filter test failed due to improper variable and wildcard substitution.	K1-19792
Link to the device on the *Agent Tasks* page was incorrect.	K1-19784
Removal of old agents could fail.	K1-19775
A duplicate Asset Subtype field name can cause unexpected behavior.	K1-19719
LDAP import failed to update attributes when Manager was mapped.	K1-19707
The Asset *User* field could not be set back to *Unassigned*.	K1-19699
Changing some Network Settings while SSO (single sign-on) was enabled due to capital letters in the host name was not possible.	K1-19613
Non-supported Security Policies are removed.	K1-19607
Agent tasks that have timed out could interrupt processing of all tasks on the appliance.	K1-19588
Occasionally the agent configuration file could get corrupted, resulting in a failure to connect to the server.	K1-19581
System users could not be deleted.	K1-19524
LDAP Import could fail if an archived user had the same user name as a user being imported.	K1-19521
The *Also Restrict By Device Label* field for a user download did not behave as expected.	K1-19513
Host name in discovery results could be incorrect with additional attributes in search context.	K1-19490
In a multi-organization appliance, the admin user did not point to the correct user entry.	K1-19482
The *Troubleshooting Utilities* field on the *Diagnostic Utilities* page could contain a maximum of 50 characters.	K1-19457
OpenLDAP user authentication did not always behave as expected.	K1-19336

Resolved issue	Issue ID
The *Patch Schedule* page listed the devices that did not support patching in the *Patch Tasks* list.	K1-18926
Titling information was missing for the KACE Agent executables.	K1-18922
The *Apply* label in the Device message was not listed in the Device history.	ESMP-5603
SAMBA v.1 is disabled by default, but it can be re-enabled by selecting the option on the *Security Settings* page.	ESMP-5526
Incoming HTML email did not decode special characters such as ` `.	ESMAS-4173
Search with some special characters did not work on the *Tickets* list page.	ESMAS-4150
Service Desk queue selection drop down did not always complete set of queues.	ESMAS-4148

Known issues

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

Table 3. General known issues

Known issue	Issue ID
Device connectivity icons are not updated in the *Administrator Guide*.	K1-19959
Historical patching information may be inaccurate for devices that are disconnected from the system.	K1-19907
In some versions of Chrome, organization settings do not behave correctly in the browser. Use another browser or incognito mode.	ESMP-6092
The *Roles* page allows you to create duplicate roles.	ESMP-6076
Location details cannot be retrieved through API.	ESMP-5989
Schedules set to *Every N Minutes* or *Every N Hours* may produce unexpected results when minutes are greater than 59 or hours are greater than 23.	ESMP-5963
Current Task value in the *Status* section changes while reordering tasks on the *Task Chain Detail* page.	ESMP-5857
Repositioning of widgets on dashboards by dragging or dropping may not work in Chrome or Firefox on Windows.	ESMP-6104
Linked Reporting does not work.	ESMP-5666

Known issue	Issue ID
`KBRSL` provisioning is being phased out and WinRM (Windows Remote Management) provisioning is the preferred method. `KBRSL` does not work on newer Windows builds as unauthenticated SAMBA access is disabled by default.	ESMEC-2948
	ESMEC-2943
HP Warranty Retrieval does not cover HP servers.	ESMEC-2846
The SELinux (Security-Enhanced Linux) status is not dislayed correctly on Raspberry Pi.	ESMEC-2945
References to the Telnet protocol should be removed from steps to create an Agentless Device Discovery Schedule in localized versions of the *Administrator Guide*.	ESMEC-2942
Raspberry Pi devices running the Agent cannot act as replicators.	ESMEC-2939
Access control on the *User Downloads* page does not work as intended.	ESMAS-4324

System requirements

The minimum version required for installing KACE SMA 9.0 is 8.1. 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.

> **i** NOTE: As of version 8.0, the appliance no longer uses the `kmsgr` process. If you have any KACE agents that are running pre-7.0 code, you must complete one of the following steps:
>
> • before upgrading the server to version 9.0, upgrade the agents to version 7.1, or
>
> • re-provision the agents once they are on version 9.0. Upgrade is not supported.

To check the appliance version number, log in to the Administrator Console and complete one of the following steps:

• **7.1 or later**. In the upper-right corner of the page, click **Need Help**. In the help panel that appears, at the bottom, click the circled '**i**' button.

• **6.4.x and 7.0**. In the upper-right corner of the page, click the question mark '**?**'. In the dialog box that appears, in the bottom-right corner, click **About K1000**.

Before upgrading to or installing version 9.0, 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/9.0-common-documents/technical-specifications-for-virtual-appliances/.

• For KACE as a Service: Go to https://support.quest.com/technical-documents/kace-systems-management-appliance/9.0-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 9.0 can be used only on KACE SMA appliances running version 6.3 or later. Version 9.0 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 9.0 is 8.1. If your appliance is running an earlier version, you must update to the listed version before proceeding with the installation.

  ◦ **7.1 or later**. In the upper-right corner of the page, click **Need Help**. In the help panel that appears, at the bottom, click the circled '**i**' button.

  ◦ **6.4.x and 7.0**. In the upper-right corner of the page, click the question mark '**?**'. In the dialog box that appears, in the bottom-right corner, click **About K1000**.

- **Verify your KACE SMA agent version**.

  The minimum version required for upgrading the KACE SMA agent is 7.1.

  ⓘ NOTE: As of version 8.0, the appliance no longer uses the `kmsgr` process. If you have any KACE agents that are running pre-7.0 code, you must complete one of the following steps:

  - before upgrading the server to version 9.0, upgrade the agents to version 7.1, or

  - re-provision the agents once they are on version 9.0. Upgrade is not supported.

- **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/9.0-common-documents/administrator-guide/.

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/9.0-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 K1000 System Administration Console: `http://K1000_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**.

    > ℹ️ 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 9.0 is applied and the KACE SMA server restarts. Progress appears in the browser window and in the Administrator Console.

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/9.0-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 9.0 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 9.0 is applied and the KACE SMA server restarts. Progress appears in the browser window and in the Administrator Console.

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 K1000 System Administration Console: `http://`K1000_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 K1000 System Administration Console: `http://`K1000_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.

   If a tether is established, a token will need to be provided to KACE Support. For more information, see the *Administrator Guide*.

More resources

Additional information is available from the following:

- Online product documentation (https://support.quest.com/kace-systems-management-appliance/9.0/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/9.0-common-documents/technical-specifications-for-virtual-appliances/.
    For KACE as a Service: Go to https://support.quest.com/technical-documents/kace-systems-management-appliance/9.0-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/9.0/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/9.0-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

We are more than just a name

We are on a quest to make your information technology work harder for you. That is why we build community-driven software solutions that help you spend less time on IT administration and more time on business innovation. We help you modernize your data center, get you to the cloud quicker and provide the expertise, security and accessibility you need to grow your data-driven business. Combined with Quest's invitation to the global community to be a part of its innovation, and our firm commitment to ensuring customer satisfaction, we continue to deliver solutions that have a real impact on our customers today and leave a legacy we are proud of. We are challenging the status quo by transforming into a new software company. And as your partner, we work tirelessly to make sure your information technology is designed for you and by you. This is our mission, and we are in this together. Welcome to a new Quest. You are invited to Join the Innovation.

Our brand, our vision. Together.

Our logo reflects our story: innovation, community and support. An important part of this story begins with the letter Q. It is a perfect circle, representing our commitment to technological precision and strength. The space in the Q itself symbolizes our need to add the missing piece — you — to the community, to the new Quest.

Contacting Quest

For sales or other inquiries, visit www.quest.com/contact.

Technical support resources

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

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

Trademarks

Quest, KACE, and the Quest logo are trademarks and registered trademarks of Quest Software Inc. in the U.S.A. and other countries. For a complete list of Quest Software trademarks, please visit our website at www.quest.com/legal. All other trademarks, servicemarks, registered trademarks, and registered servicemarks are the property of their respective owners.

Legend

!	CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.
■	WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.
i	IMPORTANT, NOTE, TIP, MOBILE, or VIDEO: An information icon indicates supporting information.

KACE Systems Management Appliance Release Notes

Updated - September 2018

Software Version - 9.0