

Quest®



KACE® Systems Management Appliance 9.1

Release Notes



Table of Contents

Quest® KACE® Systems Management Appliance 9.1 Release Notes.....	3
About KACE Systems Management Appliance 9.1.....	3
New features and enhancements.....	3
Service Desk features.....	3
Asset Management feature.....	4
Endpoint communication features.....	4
Infrastructure features.....	5
Resolved issues.....	6
Known issues.....	10
System requirements.....	11
Product licensing.....	12
Installation instructions.....	12
Prepare for the update.....	12
Update the KACE SMA server using an advertised update.....	13
Upload and apply an update manually.....	13
Post-update tasks.....	14
Verify successful completion.....	14
Verify security settings.....	14
More resources.....	15
Globalization.....	15
About us.....	15
Technical support resources.....	15
Legal notices.....	16

Quest® KACE® Systems Management Appliance 9.1 Release Notes

These release notes document provides information about the KACE Systems Management Appliance (SMA) version 9.1.

About KACE Systems Management Appliance 9.1

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

New features and enhancements

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

- [Service Desk features](#)
- [Asset Management feature](#)
- [Endpoint communication features](#)
- [Infrastructure features](#)

Service Desk features

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

- **Ability to merge tickets:** Instead of managing related tickets separately, you can merge multiple tickets into a single one, and continue to manage that one ticket. You can only merge tickets belonging to the same queue, and when ticket archival is enabled. Tickets created this way do not lose the ticket trail from the merged tickets. When you merge tickets, you must select a master ticket. The remaining tickets are automatically archived. All history related to the merged tickets remains the same. The ticket history also indicates when a ticket is merged. Service, parent, child, and previously merged tickets cannot be merged. You can separate merged tickets, as needed. To merge tickets, use the *Tickets* list or *Ticket Detail* page.
- **Support for rich text in ticket fields and incoming ticket-related email:** Starting in this release, you can use editing options for formatting the content in your ticket's *Summary*, *Comments*, and *Resolution* fields. The new editor provides a full range of text editing options to apply bold text, add images and links, attach

files, or embed videos. Also, any incoming ticket-related email content that uses HTML tags appears in HTML format in the associated tickets.



NOTE: To enable the display of HTML content in ticket email, ensure the **Use HTML/Markdown** option is selected in the email settings of the associated ticket queue.

Asset Management feature

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

- **Related assets added to location details:** In addition to related devices, the *Location Detail* page now lists the assets associated with the selected location. You can add new assets or devices to a location, as required.

Endpoint communication features

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

- **Continuous integration with KACE Cloud Mobile Device Manager (MDM):** The *Inventory Information* group on the *Device Details* page is updated in this version to include an extended set of fields collected from KACE MDM devices:

Field	iOS devices (DEP managed)	iOS devices (non-DEP managed)	Android devices
Activation Lock Bypass Code	Yes	No	No
Allow Supervised Activation Lock	Yes	No	No
DEP Managed	Yes	Yes	No
DEP Profile	Yes	No	No
DEP Profile Assigned By	Yes	No	No
DEP Profile Assigned Date	Yes	No	No
DEP Profile Status	Yes	No	No
Device Configured	Yes	No	No
Do Not Disturb	Yes	Yes	Yes
Exchange Device ID	Yes	Yes	Yes
First Enrolled	Yes	Yes	Yes
iCloud Enabled	Yes	Yes	No

Field	iOS devices (DEP managed)	iOS devices (non-DEP managed)	Android devices
Last iCloud Backup	Yes	Yes	No
Logged into iTunes	Yes	Yes	No
Wi-Fi Received	No	No	Yes
Wi-Fi Sent	No	No	Yes
WWAN Received	No	No	Yes
WWAN Sent	No	No	Yes

- **Identifying device issues:** The appliance relies on the KACE SMA Agent to collect information from agent-managed devices in your organization. If a device encounters issues connecting to the agent, or other issues related to their environment, this prevents the appliance from obtaining inventory information for that device. The *Device Issues* list page, added in this release, identifies any agent-managed devices whose information does not appear in the inventory due to any of the following issues:

- WMI (Windows Management Instrumentation) corruption.
- Desktop heap exhaustion.



TIP: In most cases, this problem can be cleared by simply restarting the device.

- Failure to write to `amp.conf`.

For more information about these issues, visit <https://support.quest.com/kace-systems-management-appliance/kb>.

Infrastructure features

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

- **Appliance chat enhancements:** The appliance chat is updated in this version to display a list of existing Knowledge Base articles related to the *Purpose of Your Chat*, as specified. If none of the listed articles provide the information you need, you can continue to chat with a product specialist.
- **Decommissioning support for Samba v1:** The appliance no longer offers the support for Samba v1 protocol. The minimum version supported is 2.0.
- **Access to KACE Agent Toolkit (KAT):** A link to the KAT, formerly KaptureState, is added to the *Support* page in the System Administration Console. The Knowledge Base article describing the KaptureState utility, found on <https://support.quest.com/kb/234337>, no longer applies, and is as such marked as legacy.
- **Microsoft Azure support.** As of this release, the appliance can start up and run in the Azure cloud. It is available in the Azure Marketplace and offered in several disk sizes that you can choose according to your business needs. To download a copy of the *KACE SMA Setup Guide for Azure Platforms*, visit <https://support.quest.com/kace-systems-management-appliance/9.1/technical-documents>.
- **SSO supports AES encryption.** If you have previously enabled SSO, you must remove the device from the domain and then rejoin, to enable this change.

Resolved issues

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

Table 1. Resolved Issues

Resolved issue	Issue ID
On newer Mac platforms, Mac BIOS fields were not being populated in the inventory.xml file that was uploaded to the appliance.	K1-20361
Logging in to the Kace GO app when user is their own manager sometimes resulted in an error.	K1-20306
It was not possible to remove Response Templates created by a user that has been deleted.	K1-20300
Process approval by email did not work correctly for Software Request Type processes.	K1-20292
Knowledge Base (KB) article attachments sometimes displayed incorrectly in Kace GO.	K1-20291
Duplicate email addresses in from or reply-to fields in emails from unknown users sometimes prevented ticket or new user from being created.	K1-20289
Single Sign On (SSO) sometimes did not work as expected in multi-organization appliances.	K1-20276
The <i>Device Details</i> page did not display the Choose Action Wake-On LAN options when using non-English locale.	K1-20274
In some cases, when creating a new organization, the administrator account could not log in.	K1-20266
The initial email was not sent for Process Workflows created with default owners for parent or child.	K1-20265
Raw SQL report results in blank output when parenthesis were used after a UNION clause.	K1-20261
With a non-default theme, going from one portal to another by URL change (for example, /systemui) could cause an error.	K1-20258
Raspbian agent download link on the <i>Update Agents</i> page redirected to /userui.	K1-20257
Testing an organization filter based on an IP address failed when a NAT (network address translation) address was used.	K1-20255
The Test button on the <i>Organization LDAP Filter Detail</i> page sometimes resulted in an error.	K1-20253

Resolved issue	Issue ID
Mac OS 10.14 Mojave appeared under <i>Other</i> in OS picker.	K1-20248
The <i>Show More</i> link icon was broken in the <i>Urgent Announcements</i> section.	K1-20215
API call to fetch the machine list did not return agent managed devices as expected.	K1-20178
Displaying the detail of a parent ticket with many child tickets could fail.	K1-20133
Daily security output email may contain spurious warnings that should be ignored.	K1-20113
Agent did not clean kbot elements that were no longer assigned to the machine, potentially causing unnecessary disk space usage.	K1-20111
Replication failed when patch file name contained space.	K1-20108
Service Desk: Category Default Owner continued to receive email after ticket owner has been reassigned.	K1-20107
The CC list for a ticket queue was not respected in some cases.	K1-20105
Use of LDAP Smart Labels and Filters sometimes interfered with user logins.	K1-20099
Manager info was missing while importing LDAP users.	K1-20096
Task Schedule displayed runs prior to task's modified date.	K1-20094
Wake on Lan scheduling did not display hours or minutes for 'run every' or 'run on' schedule.	K1-20085
Memory error was observed when performing an online shell script on more than 24 devices.	K1-20018
VMware device commands sometimes do not return the proper error message.	K1-20009
Custom interval set for catalog inventory on a per-organization basis was not respected in some cases.	K1-20000
Asset Status was not shown in the View By option on the <i>Contract</i> list page.	K1-19995
The patch download schedule sometimes operated more frequently than requested in the <i>Patch Download</i> settings page.	K1-19993
Organization filter did not work, resulting in devices being mistakenly placed in the default organization.	K1-19983
A DataTables warning was sometimes seen when looking at list pages.	K1-19980
User import did not display attributes for existing users.	K1-19978
With SSL enabled, a curl timeout could be seen following kbot uploads.	K1-19972

Resolved issue	Issue ID
User in CC or Category CC list was unable to access ticket if the user email case (upper/lower) did not match.	K1-19968
Service Desk: Manual Date Picker did not respect locale changes.	K1-19967
The "Unknown email address response" template sometimes failed to send if the Accept email from unknown users option was not selected.	K1-19963
The category with a nested drop-down sometimes did not display properly when My Profile was used on ticket.php.	K1-19962
Reports in the System Administration Console created by the wizard did not work as expected in some cases.	K1-19947
Page with a multi-select drop-down option did not print correctly.	K1-19945
SSO Kerberos used old RC4 (Rivest Cipher 4) instead of modern AES (Advanced Encryption Standard) ciphers.	K1-19938
Patch schedule <i>Timezone</i> setting could be incorrect if second "run on" option was used.	K1-19937
Patches not in subscription could be mistakenly re-activated after patch download.	K1-19934
With thousands of barcodes present, asset deletion could take a very long time.	K1-19923
In the User Portal "Urgent Announcement" message, the Show More icon (arrow) was missing.	K1-19919
Advanced Search of Assets returns "Location" as "Unassigned" in non-English locale.	K1-19916
Email ticket attachments and images with width less than 100 px were scaled up and caused thumbnail to be larger than original image.	K1-19909
An MSI file could end up in the C:\windows\temp directory instead of the agent directory.	K1-19908
FileVault Inventory did not properly report APFS (Apple File System) data.	K1-19897
The <i>Backup Settings</i> page was not visible after upgrade.	K1-19890
It was not possible to force inventory or Wake on LAN for device within role scope.	K1-19889
Process Parent Ticket failed to retain custom field value.	K1-19886
It was not possible to specify process description while creating new process.	K1-19878
The <i>Show More</i> link for Service Desk announcements sometimes did not function for longer messages.	K1-19872

Resolved issue	Issue ID
Editing Service Desk announcement with line breaks caused additional line breaks to be inserted on each edit.	K1-19871
LDAP Import could silently fail if required field was missing.	K1-19867
Performance could be impacted when a high number of replicators were present.	K1-19865
<i>HTML Markdown</i> option on Service Desk email notifications broke tokens.	K1-19858
The <i>Dell Update Catalog Comparison</i> report was not accurate in some cases.	K1-19857
Apostrophe in user email replaced by HTML code '.	K1-19828
On <i>Users</i> list page, sorting by user locale resulted in error message.	K1-19813
Driver installation caused looping for certain drivers which were deployed through Dell Updates.	K1-19803
Custom logo was not displayed correctly in generated PDF report.	K1-19774
Asset Import Step 2 of 4 Asset Subtype: Drop-down menu did not display when file name contained an apostrophe.	K1-19773
<i>All Queues</i> view displayed tickets in ticket list even when user did not have rights to view the tickets.	K1-18687
Patching search for Windows 8.1 patches included Windows 8 patches.	K1-17979
It was not possible to mark a patch as active from the list view.	K1-17849
Creation of Detect patch schedule set <i>Deploy All Patches</i> flag to True.	K1-17081
Drag and drop sometimes did not work on dashboards in Firefox/Chrome on Windows.	ESMP-6104
Entering value greater than 59 on <i>Every X minutes</i> schedule produced unexpected behavior.	ESMP-5963
Cloning ticket through KACE GO sometimes did not update related tickets correctly in the newly created ticket.	ESMAS-4448
Invalid UTF8 characters error message displayed with KACE GO when creating or opening existing Service Desk tickets.	ESMAS-4349
Urgent announcement color scheme caused the content hard to read.	ESMAS-4310

Known issues

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

Table 2. General known issues

Known issue	Issue ID
<p>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:</p> <ul style="list-style-type: none">• Windows Server 2016 (1709)• Windows Server 2016 (1803)• Windows Server 2019 <p>Workaround: Select the SNMP version <i>SNMPv1</i> to prevent this problem.</p>	ESMEC-3263
<p>Agent fails to install on SLES v.15 with errors.</p> <p>Workaround: On Red Hat and SuSE, install the <i>coreutils</i>, <i>pciutils</i>, and <i>rpm</i> packages along with the <code>/usr/sbin/dmidecode</code> and <code>/usr/bin/lpstat</code> applications. If they are not installed, the <i>rpm</i> package refuses to install until they are installed.</p> <p>On Ubuntu, the same requirements apply for proper functionality, but if they are not installed, the package still installs correctly but not all functionality works as expected.</p>	ESMEC-2987
<p>Agentless monitoring of SLES v.15 does not work.</p> <p>Workaround: Install the <i>rsyslog</i> package to prevent this issue.</p>	ESMEC-2986
<p>KACE SDA (System Deployment Appliance) deployment information is not populated in 9.1 on the <i>Device Details</i> and <i>Devices</i> pages, and in reports.</p>	ESMP-6705
<p>The <i>Comments</i> section in Service Desk ticket details does not clear when adding comments and attachments at the same time.</p>	ESMP-6672
<p>Repeated <code>/proc/net/route</code> errors are observed on KACE SMA console hosted on Azure. This is a benign issue and as such can be ignored.</p>	ESMP-6540
<p>OS Release ID may be blank for agent devices.</p>	ESMP-6133
<p>HTML tags are displayed in the Comments & Resolution column in Service Desk reports.</p>	ESMAS-4552
<p>HTML tags are displayed in the Update Notification pop-up message when comments are deleted from the <i>Ticket Detail</i> page.</p>	ESMAS-4551
<p>Service Desk: On the <i>Ticket Detail</i> page, the editor available in the <i>Comments</i> field does not properly handle some special characters, such as code blocks.</p>	ESMAS-4542
<p>Merging two tickets with the same submitter adds that submitter to the CC list even though they are already the submitter of the main ticket. This may cause the</p>	ESMAS-4537

Known issue	Issue ID
appliance to send duplicate emails to that user, if <i>Email on Events</i> is enabled for the submitter and the CC list.	
Service Desk: On the <i>Ticket Detail</i> page, the <i>Summary</i> , <i>Comments</i> , and <i>Resolution</i> fields come with a rich text editor that includes a collection of emoticons that can be added to the field contents. Any emoticons from that collection appear as expected each time you view ticket details in the Administrator Console. If you add any other emoticons, for example the ones that come with your email editor, they do not display correctly in the Administrator Console.	ESMAS-4510 ESMAS-4509 ESMAS-4508
Videos attached to Service Desk tickets are not added to emails sent to the ticket submitters.	ESMAS-4507
Using large font in the <i>Ticket Detail</i> text editor causes it to overlap itself.	ESMAS-4480
KACE GO: Attachments embedded in KB articles are not displayed when the secure attachment option is enabled.	ESMAS-4453
Response templates and Service Desk email notifications do not support rich text.	ESMAS-4437
In French locale, on the <i>Devices</i> list page, the Choose Action > Change Location command does not display the <i>Change Location</i> dialog box, as expected.	K1-20400
Linked Reporting does not work on the appliance.	K1-20054
Service Desk: By default, the Use HTML/Markdown option is disabled for the <i>Ticket Closed</i> email template. This causes HTML tags to be applied to simple text. Workaround: Enable the Use HTML/Markdown option in the template.	N/A
<i>Setup Guide for Azure Platforms:</i> Unlike the other setup guides included with the appliance, this manual is not localized. This is a very first release of the appliance on Microsoft Azure and the instructions were finalized at the very end of the release cycle. Localized content will be provided in a future release.	Documentation

System requirements

The minimum version required for installing KACE SMA 9.1 is 9.0. If your appliance is running an earlier version, you must update to the listed version before proceeding with the installation.

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

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

Before upgrading to or installing version 9.1, make sure that your system meets the minimum requirements. These requirements are available in the KACE SMA technical specifications.

- For virtual appliances: Go to <https://support.quest.com/technical-documents/kace-systems-management-appliance/9.1-common-documents/technical-specifications-for-virtual-appliances/>.
- For KACE as a Service: Go to <https://support.quest.com/technical-documents/kace-systems-management-appliance/9.1-common-documents/technical-specifications-for-kace-as-a-service/>.

Product licensing

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

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



NOTE: Product licenses for version 9.1 can be used only on KACE SMA appliances running version 6.3 or later. Version 9.1 licenses cannot be used on appliances running earlier versions of the KACE SMA, such as 6.0.

Installation instructions

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

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



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

Prepare for the update

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

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

The minimum version required for installing KACE SMA 9.1 is 9.0. If your appliance is running an earlier version, you must update to the listed version before proceeding with the installation.

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

The minimum version required for upgrading the KACE SMA agent is 7.1. We recommend running the latest agent version with KACE SMA 9.1.
- **Back up before you start.**

Back up your database and files and save your backups to a location outside the KACE SMA server for future reference. For instructions on backing up your database and files, see the Administrator Guide, <https://support.quest.com/technical-documents/kace-systems-management-appliance/9.1-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/9.1-common-documents/administrator-guide/>.
2. Go to the appliance *Control Panel*:
 - If the Organization component is not enabled on the appliance, click **Settings**.
 - If the Organization component is enabled on the appliance: Log in to the appliance System Administration Console: `http://KACE_SMA_hostname/system`, or select **System** in the drop-down list in the top-right corner of the page, then click **Settings**.
3. On the left navigation bar, click **Appliance Updates** to display the *Appliance Updates* page.
4. Click **Check for updates**.

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

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

Version 9.1 is applied and the KACE SMA server restarts. Progress appears in the browser window and in the Administrator Console.

6. When the server upgrade finishes, upgrade all of your agents to version 9.1.

Upload and apply an update manually

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

CAUTION: Never manually reboot the KACE SMA server during an update.

1. Back up your database and files. For instructions, see the Administrator Guide, <https://support.quest.com/technical-documents/kace-systems-management-appliance/9.1-common-documents/administrator-guide/>.
2. Using your customer login credentials, log in to the Quest website at <https://support.quest.com/kace-systems-management-appliance/download-new-releases>, download the KACE SMA server `.kbin` file for the 9.1 GA (general availability) release, and save the file locally.
3. On the left navigation bar, click **Appliance Updates** to display the *Appliance Updates* page.
4. In the *Manually Update* section:
 - a. Click **Browse** or **Choose File**, and locate the update file.
 - b. Click **Update**, then click **Yes** to confirm.

Version 9.1 is applied and the KACE SMA server restarts. Progress appears in the browser window and in the Administrator Console.

5. When the server upgrade finishes, upgrade all of your agents to version 9.1.

Post-update tasks

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

Verify successful completion

Verify successful completion by viewing the KACE SMA version number.

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

Verify security settings

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

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



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

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

More resources

Additional information is available from the following:

- Online product documentation (<https://support.quest.com/kace-systems-management-appliance/9.1/technical-documents>)
 - **Technical specifications:** Information on the minimum requirements for installing or upgrading to the latest version of the product.
For virtual appliances: Go to <https://support.quest.com/technical-documents/kace-systems-management-appliance/9.1-common-documents/technical-specifications-for-virtual-appliances/>.
For KACE as a Service: Go to <https://support.quest.com/technical-documents/kace-systems-management-appliance/9.1-common-documents/technical-specifications-for-kace-as-a-service/>.
 - **Setup guides:** Instructions for setting up virtual appliances. Go to <https://support.quest.com/kace-systems-management-appliance/9.1/technical-documents> to view documentation for the latest release.
 - **Administrator guide:** Instructions for using the appliance. Go to <https://support.quest.com/technical-documents/kace-systems-management-appliance/9.1-common-documents/administrator-guide/> to view documentation for the latest release.

Globalization

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

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

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

About us

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

Technical support resources

Technical support is available to Quest customers with a valid maintenance contract and customers who have trial versions. You can access the Quest Support Portal at <https://support.quest.com>.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to-videos
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product.

Legal notices

© 2019 Quest Software Inc. ALL RIGHTS RESERVED.

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

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

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

Quest Software Inc.

Attn: LEGAL Dept

4 Polaris Way

Aliso Viejo, CA 92656

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

Trademarks

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

Legend



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



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

KACE Systems Management Appliance Release Notes

Updated - April 2019

Software Version - 9.1