



KACE® Systemverwaltungs-Appliance 15.0

## **Versionshinweise**



# Inhaltsverzeichnis

<b>Quest® KACE® Systems Management Appliance 15.0 – Versionshinweise.....</b>	<b>3</b>
Über die KACE Systems Management Appliance 15.0.....	3
Neue Funktion.....	3
Verbesserungen.....	3
Behobene Probleme.....	5
Behobene Serverprobleme.....	6
Behobene Service Desk-Probleme.....	9
Behobene KACE Agent-Probleme.....	11
Bekannte Probleme.....	12
Systemanforderungen.....	12
Produktlizenzierung.....	13
Installationsanweisungen.....	13
Aktualisierung vorbereiten.....	13
Aktualisieren des KACE Systems Management Appliance Servers mit einer beworbenen	
Aktualisierung.....	15
Eine Aktualisierung manuell hochladen und anwenden.....	15
Aufgaben nach der Aktualisierung.....	16
Erfolgreichen Abschluss überprüfen.....	16
Sicherheitseinstellungen überprüfen.....	17
Weitere Ressourcen.....	17
Globalisierung.....	18
<b>Über uns.....</b>	<b>19</b>
Ressourcen für den technischen Support.....	19
Rechtliche Hinweise.....	19

# Quest® KACE® Systems Management Appliance 15.0 – Versionshinweise

---

Dieses Dokument enthält Informationen zur KACE Systems Management Appliance Version 15.0.

## Über die KACE Systems Management Appliance 15.0

KACE Systems Management Appliance wurde zur Automatisierung der Geräteverwaltung, der Anwendungsbereitstellung, des Patchings, des Asset-Managements und der Service Desk-Ticketverwaltung entwickelt. Weitere Informationen zur KACE Systems Management Appliance Serie finden Sie unter <https://www.quest.com/products/kace-systems-management-appliance/>.

## Neue Funktion

Diese Version der KACE Systems Management Appliance beinhaltet die folgende neue Funktion.

### **Funktion "Favoriten" für die Navigation in der Benutzeroberfläche:**

Diese Funktion verbessert die Navigation, da Benutzer häufig aufgerufene Seiten mit Lesezeichen versehen können. Diese Funktion ist nützlich für Administratoren, die große Umgebungen verwalten, in denen ein schneller Zugriff auf sich wiederholende Arbeitsabläufe unerlässlich ist. Die Funktion "Favoriten" bietet die folgenden Möglichkeiten:

- Diese Funktion ist sowohl in der Admin- als auch in der System-Benutzeroberfläche verfügbar.
- Sie unterstützt bis zu 50 Favoriten pro Benutzeroberfläche.
- Die Lesezeichen werden für jeden Benutzer und jede Organisation gespeichert.
- Es werden nur statische Seiten und keine dynamischen oder kontextgesteuerten Seiten unterstützt.
- Enthalten sind Optionen für die Neuordnung per Drag-and-Drop, die Suche und das Löschen.
- Wenn der Zugriff eines Benutzers auf ein Modul aufgehoben wird, nachdem er es mit einem Lesezeichen versehen hat, und der Benutzer von der Favoritenliste aus auf das mit Lesezeichen versehene Element klickt, wird der Benutzer abgemeldet.

## Verbesserungen

Nachfolgend finden Sie eine Liste von in dieser Version implementierter Verbesserungen.

1. **Dashboard-Überarbeitung:** Das Dashboard wurde grundlegend überarbeitet, um ein moderneres, anpassbares Erlebnis mit umfangreichen Daten zu schaffen.
  - # Modernes Layout und moderne Designs: Benutzer können Dashboards mit flexiblen Layouts, Farbdesigns und Widget-Anordnungen entwerfen. Die Drag-and-Drop-Schnittstelle ermöglicht eine einfache Anpassung an verschiedene Überwachungsanforderungen.
  - # Mehrere Dashboards pro Benutzer: Anstatt auf eine einzige Ansicht beschränkt zu sein, können Benutzer jetzt mehrere Dashboards erstellen, verwalten und zwischen ihnen wechseln. Jedes Dashboard kann benannt, angepasst und als persönliche Standardeinstellung für den schnellen Zugriff festgelegt werden.
  - # Verbesserungen auf Widget-Ebene: Widgets wurden mit umfassenderen Funktionen aktualisiert.
    - # Erstellen Sie Widgets von Grund auf neu oder basierend auf vorhandenen Berichten mithilfe eines Schritt-für-Schritt-Assistenten oder anhand von SQL-Abfragen für erweiterte Anpassungen.
    - # Konfigurieren Sie Diagramme in verschiedenen Formaten, einschließlich Balken-, Linien-, Ring-, Tachometer-, Fortschrittsdiagramm, Scorecard, Weltkarte usw.
    - # Fügen Sie mehrere Versionen desselben Widget-Typs hinzu (z. B. verschiedene gefilterte Ansichten von "Aktive Tickets").
    - # Verwenden Sie die integrierten Widget-Steuerelemente, um Daten zu aktualisieren, Ergebnisse zu exportieren, Diagramme zu ändern, Legenden neu zu positionieren oder Farben auf Widget-Ebene zu überschreiben.
    - # Ändern Sie die Größe von Widgets oder ordnen Sie sie durch einfaches Drag-and-Drop neu an.
    - # Schränken Sie die Sichtbarkeit von Widgets basierend auf Benutzerrollen oder -Labels ein.
  - # Erkenntnisse weitergeben und teilen:
    - # Senden Sie Dashboards per E-Mail als HTML-Snapshots, entweder sofort oder nach Zeitplan (täglich, wöchentlich, monatlich).
    - # Wählen Sie die Anzahl der Widgets, die pro Zeile in der E-Mail angezeigt werden sollen.
  - # Leistung und Datenaktualisierung:
    - # Profitieren Sie von Caching-Optimierungen für große Umgebungen.
    - # Aktualisieren Sie Daten auf Anforderung auf Dashboard-Ebene oder auf individueller Widget-Ebene.
2. **Verbesserungen beim Patch-Katalog:** Der Patch-Katalog wurde durch fortschrittliche Intelligenz erheblich verbessert, damit IT-Teams Patches präziser bewerten und priorisieren können.
  - # Zu den zusätzlichen Datenpunkten gehören jetzt CVSS-Scores, EPSS-Scores, Known Exploit Vulnerabilities und Verwendung in Ransomware-Kampagnen, die aus vertrauenswürdigen Threat-Intelligence-Feeds wie NIST, MITRE und FIRST.org stammen.
  - # Dank verbesserter Filterfunktionen können Administratoren Patches anhand dieser Metriken suchen und zielgerichtetere Dashboards und Berichte erstellen.
  - # Neue Widgets, z. B. Risiko nach CVSS-Score, Aufschlüsselung des Patch-Status nach CVSS, Patch nach CVSS-Score und Aufschlüsselung des Patch-Status von Geräten nach CVSS, liefern umsetzbare Erkenntnisse auf einen Blick.
  - # Benutzer können direkt auf CVE-Links in den Patch-Details zugreifen und fehlende CVE-Daten vom Katalogteam anfordern.
3. **Aktualisierung von Linux-Patch-Zeitplänen:** Benutzer können nun entscheiden, ob sie nur Sicherheits-Patches oder alle verfügbaren Patches während Linux-Paket-Upgrades anwenden möchten. Dies bietet mehr Flexibilität und ermöglicht eine bessere Abstimmung auf die Compliance-Anforderungen des Unternehmens.



**HINWEIS:** Einige Linux-Distributionen unterscheiden nicht zwischen Patch-Typen und führen immer ein Upgrade aller Pakete durch.

4. **Mehr Sicherheit und überarbeitete Protokollierung:** Das alte FreeBSD Syslog wurde vollständig durch moderne, sichere Protokollierungsmechanismen ersetzt.
  - # Die Unterstützung des Protokollierungssystems über sicheres TCP mit TLS stellt sicher, dass Protokolle sicher übertragen werden.
  - i** **HINWEIS:** Wir unterstützen die Integration mit jedem Protokollierungssystem, das für die Verwendung mit TLS konfiguriert werden kann. Unsere Dokumentation bietet zwar Beispiele für die Integration mit Syslog-ng und Rsyslog, unser Support beschränkt sich aber nicht nur auf diese Tools.
  - # Die Protokollierung erfasst jetzt die SSH-Anmeldung/-Abmeldung, Remote-Konsolenaktivitäten und ungültige Anmeldeversuche, um die Prüfbarkeit zu verbessern.
  - # Die SMA generiert Zertifikate und Schlüssel für die sichere Authentifizierung, während Remote-Server entsprechende Anmeldeinformationen konfigurieren müssen.
  - i** **HINWEIS:** Die vorhandenen Syslog-Konfigurationen funktionieren nach der Aktualisierung nicht mehr. Administratoren müssen die Syslog-Einstellungen mit den neuen sicheren Optionen neu konfigurieren.
5. **Neugestaltung der Speicherung von Skriptprotokollen:** Das Skriptprotokoll-Speichungsmodell wurde für eine bessere Leistung und Skalierbarkeit neu gestaltet.
  - # Protokolle werden jetzt basierend auf der Anzahl der Skriptausführungen (Standard: 7) anstatt eines zeitbasierten Modells gespeichert.
  - # Dies gewährleistet eine vorhersehbare Speicherverwaltung und eine schnellere Systemleistung in großen Umgebungen.
  - i** **HINWEIS:** Aufgrund von Schemaänderungen werden alle vorhandenen Agentenprotokolle während des Upgrades gelöscht. Bei Bedarf müssen Sie kritische Protokolldaten exportieren, bevor Sie ein Upgrade durchführen.
6. **Verbesserungen bei der Integration von Splashtop:** Die Splashtop-Funktion wurde verbessert, um eine reibungslosere Fernwartung zu ermöglichen.
  - # Verbesserte RMM-Codezuweisung während der Installation.
  - # Anzeige der Streamer-Version in den Gerätedetails.
  - # Aktiviertes Hochladen von Streamer-Protokollen der SMA für die Fehlerbehebung.
  - # Hinzugefügte Schaltfläche für die Remote-Steuerung in den Ticketdetails.
  - # Unterstützung von benutzerdefinierten Einstellungen für einmalige Sitzungen während des Fernzugriffs.
  - # Konfiguriertes Logo für leeren Bildschirm (nur PNG) während Sitzungen.
  - # Unterstützung von zwei gleichzeitigen Remote-Sitzungen
7. **Schnell-Links für Administrator-Navigation:** Schnell-Links wurden eingeführt, um die Navigation für Benutzer zu vereinfachen. Dazu gehört der direkte Zugriff auf die Seiten "Label-Verwaltung", "Smart Labels", "LDAP-Labels", "Sicherheitseinstellungen" und "Service Desk".

## Behobene Probleme

Dieser Abschnitt enthält die in dieser Version behobenen Probleme:

- [Behobene Serverprobleme](#)
- [Behobene Service Desk-Probleme](#)
- [Behobene KACE Agent-Probleme](#)

# Behobene Serverprobleme

Im Anschluss finden Sie eine Liste mit Serverproblemen, die in dieser Version behoben wurden.

## Behobene Serverprobleme

Resolved issue	Issue ID
Software Catalog title search takes too long in license asset page. The Retain Uncataloged data in the 'Software Catalog' option is now moved from Organizations: General Settings to System: General Settings for Multi-Org license.	K1-36466
Barcode section is visible on License Asset detail page, even without Barcode tag configuration on License Asset Type detail page.	K1-36065
Machine with blank user info has owner set to the first user found in USER table.	K1-36143
Not able to set a value of '0' on a required asset field of type 'Number'.	K1-36125
Getting incorrect device count when user performs Remote control session reset for a device.	K1-36063
Error while duplicating a Discovery schedule of External Integration type.	K1-34918
Patch detect schedule fails with error 'Task Configuration changed since scheduling'.	K1-36138
Update patch signature download check to be less restrictive.	K1-36576
While deploying a patch, the user is not prompted again after snooze duration and Patch schedule status shows error.	K1-36080
Patch Schedules appear to be stuck in 'process-log' phase for up to 15 minutes.	K1-36124
Windows Feature Update schedules stuck in 'process-log2' phase.	K1-36147
Search action on Agent Token list page doesn't consider selected filter on View By drop-down.	K1-35500
Allow more than 195 GB for Offboarding Backups to Azure Blob Storage.	K1-36127
Admin user unable to change the SystemUI settings while navigated using AdminUI links.	K1-35497
Remote Connection can fail if session password is not updated fast enough on streamer due to low memory.	K1-35982
Unable to track history while changing Authentication settings from 'Local Authentication' to 'LDAP Authentication'.	K1-35036
Error observed when user selected for deletion is set as Manager to itself.	K1-35488
Search action on User list page doesn't consider selected filter on View By drop-down.	K1-35496

<b>Resolved issue</b>	<b>Issue ID</b>
Virtual Hostname and Virtual IP on organizations is not working.	K1-35962
Option to add Barcodes not available when creating a new asset.	K1-36006
User logged out when loading a device with an image attachment on its asset, if assets permission is set to HIDE.	K1-36434
Barcode Data not added/updated when asset import is done through a scheduled import or Run option from the asset import list view.	K1-35545
Newly created locations not visible after adding a new Location subtype.	K1-35468
Unable to edit custom field in Asset Type when adding for the first time.	K1-36078
Deleting a barcode tag does not validate if it is in use before removing it causing errors for Kace Go app users.	K1-36170
Location field HTML tags become visible on custom view when a second field named 'Location' exists.	K1-36225
Advanced search result shows blank custom field values if custom field contains ampersand (&) within the field name.	K1-35149
Alerts set to 'All Devices' without confirmation when no device or label restriction has been set.	K1-36086
Replication share schedule changes require to click into very specific spots on the time grid.	K1-35979
Task Chains with online Shell script remain on status 'Running'.	K1-33958
Task chains results inconsistent across ORGs for failed online scripts.	K1-35092
Task chain tasks after a patch task fail to be executed.	K1-36087
Task chain results are inconsistent when multiple patch tasks are executed.	K1-36388
Label Management choose action menu not interpreting html character &#39; for apostrophe.	K1-35759
Error shown when applying a label to a device and there are no labels with Remote Control enabled.	K1-36083
Unable to apply a label in User detail if label and user IDs are the same.	K1-36131
Error when loading a smart label while logged in with a device scoped user role.	K1-36298
Installed Versions not loading for Software Catalog application item of type Suite.	K1-35515
SAM Inventory Processing fails when processing software with foreign language characters in filename.	K1-35822

<b>Resolved issue</b>	<b>Issue ID</b>
Application versions fail to load for locally titled software.	K1-36500
Devices on non-SMA Splashtop licensed appliance shown in device issues if Splashtop is installed.	K1-36239
HTML Scheduled report notification email does not display new lines properly.	K1-36149
Error displayed when clicking link on Dell Updates report.	K1-35638
Report shows incomplete or blank results due to PHP ParseError.	K1-35924
Wizard created report fails with error Unknown column 'RUN_AS_CREDENTIAL' in 'order clause'.	K1-35935
Scripting list view 'Run' action do not work for multi-selects.	K1-35960
A new <b>Agent Script Log Retention</b> setting has been added to control how many script run logs are preserved. The default retention is set to 7 runs.	K1-36113
Antivirus Quarantine advanced search, custom view and report queries are malformed when filtering by a user type field.	K1-34259
Error when an advanced search is done on Dell Updates Catalog.	K1-35550
Device Linux Package Repository Information not updated on server side when repository is removed from device.	K1-35539
Patch job shows status 'Reboot Snoozed' when device is actually rebooting.	K1-35596
Patch schedule set in Agent Time Zone fails to be scheduled for devices in different time zones.	K1-36089
Fixed sorting for patch schedule list columns.	K1-36456
Suppress newsyslog email sent to root by Cron Daemon.	K1-35998
HAProxy process consumes high CPU usage after certificate update.	K1-36306
HAProxy fails to stop when services are restarted.	K1-36441
Validate License fails to check maintenance renewal status.	K1-36120
Diagnostic Tools Top does not load for Spanish locale.	K1-35201
Backups are not running at the newly scheduled time.	K1-36056
Backups cannot be re-enabled if disabled in 14.x or prior upgrade.	K1-36652
User credential password is incorrectly changed on save when editing other fields.	K1-34797

<b>Resolved issue</b>	<b>Issue ID</b>
Custom logo does not show when 'Acceptable Use Policy' is enabled.	K1-36202
Old agent binaries not removed after update when device is not in default org.	K1-35933
Local import on multi-org appliance does not allow importing more than one resource at a time.	K1-36153
Local Admin role is overwritten when SAML user has same email address as local Admin.	K1-34924
System UI LDAP browser credentials input fields are missing.	K1-36074
Task Schedule page takes a long time to load or hangs when there are task chains with too many tasks on a frequent schedule.	K1-34207
Make Asset Unique ID field visible for Devices Asset type and subtype list view.	K1-36168
Address User Sessions table can grow large over time and become sluggish.	K1-36093
Update netdiag utility to display SMA serial number.	K1-36201
Splashtop remote control session to allow 2 connections to the device at a time.	K1-36040
An option to hide the general 'Ask any general topic' link in the User Portal Need Help page.	K1-36480
Partial hybrid inventory deletes custom inventory data.	K1-36169
MI table column 'NOTES' is renamed to 'Name'.	K1-36075
Add an option to disable API access to the SMA.	K1-36884

## Behobene Service Desk-Probleme

Im Anschluss finden Sie eine Liste mit Service Desk-Problemen, die in dieser Version behoben wurden.

### Behobene Service Desk-Probleme

<b>Resolved issue</b>	<b>Issue ID</b>
Announcement text in the user portal is overlapped for long 'Message Title' when dragged to the Urgent section.	K1-36062
Archived and Closed columns in Archived Ticket list do not sort correctly.	K1-35648
Child tickets are not automatically created when parent ticket is approved via email.	K1-35407
Custom view option is not present in <b>View By</b> drop-down if <b>All Queue</b> option is selected.	K1-36244
CC List users for an archived ticket not able to see the ticket in the archive ticket list view after queue is deleted.	K1-35578

<b>Resolved issue</b>	<b>Issue ID</b>
Ticket fields not shown in UserUI if SAT_SURVEY permission is set to 'Owners Only - Visible' or 'Owners Only - Hidden'.	K1-36002
Service desk email tokens support for org virtual hostname.	K1-33897
Error when a Default Ticket Template that contains a separator is used on an Exported queue.	K1-36743
Process initiated by e-mail creates the parent ticket, but no child tickets if submitter in process template is left unassigned.	K1-34142
Browser 'URI too long' error when large tables are added to an email on event template.	K1-35642
Service Desk Process sends out duplicate notifications when process approval is completed and process only has a parent ticket.	K1-35873
Handle ticket attachments when content-disposition header is not present.	K1-36042
User receives a CC list notification after adding a comment to a ticket, if their email appears after the first address in the CC list.	K1-36242
Closing process last child ticket via email should allow to close/complete process when option 'Allow last child ticket to close parent ticket' is enabled.	K1-34143
Comment field is missing from process templates when Summary is hidden and Comment field is marked visible for queue.	K1-36041
Default value of a 'Read Only' Ticket Template field is not displayed on parent/child tickets.	K1-36346
Wizard report shows tickets from all queues although report topic is set to a specific ticket queue.	K1-34088
Allow more than five field conditions for ticket templates.	K1-36311
Ticket template conditional logic for 'Begins With' does not work if condition string has spaces.	K1-36330
Changing field to 'Always required' before updating the template causes conditional logic to be lost.	K1-36460
Last selected Service Desk view only retained for the last queue the user was working on before navigating out.	K1-36095
Blank option shown on <b>Related Tickets</b> drop-down menu when title for the ticket is 'Hidden'.	K1-36121
Allow administrator or queue owner users to see all archived tickets for a queue, after it is deleted.	K1-35575
Unable to import ticket field values if custom field type is single/multiselect and using QUERY to populate options list.	K1-36288

<b>Resolved issue</b>	<b>Issue ID</b>
Ticket Asset field not loading when 'Filter on submitter assigned assets' is checked, and custom asset type exists that includes a User field type.	K1-36334

## Behobene KACE Agent-Probleme

Im Anschluss finden Sie eine Liste mit KACE Agent-Problemen, die in dieser Version behoben wurden.

### Behobene KACE Agent-Probleme

<b>Resolved issue</b>	<b>Issue ID</b>
Removed Network adapters without MAC addresses from inventory.	K1A-3932
Agent reports incorrect BIOS name and manufacturer on Debian Linux.	K1A-4088
ShellCommandDateReturn Custom Inventory Rule fails on Linux Platform.	K1A-4093
Support Windows environment variable with custom inventory rules.	K1A-4095
Windows agent failing to upload inventory.xml due to MDM Server field containing '&' character.	K1A-4121
Windows Defender Patch detection fails due to RegExpandSz.	K1A-4130
On-Demand Patch deployment doesn't run if agent is not connected when the service starts.	K1A-4134
Inventory fails on Ubuntu devices with r-cran packages installed.	K1A-4135
RegistryValueEquals Custom inventory and KScript 'Verify a registry value is exactly' task fails.	K1A-4137
Agent will not start when a 'configure log access' group policy is applied to a system and the agent in not granted access.	K1A-4139
Linux patch detection fails on Ubuntu 24 LTS.	K1A-4157
Windows Installer not honoring NoHooks installation when upgrading agent from 13.2 to 14.x.	K1A-4158
Addition of hyperthreading virtual processors inventory data.	K1A-4159
Linux Updates: Support all packages upgrade in addition to security only.	K1A-4165
Agent recreates client certificate too aggressively and cause identity to reset.	K1A-4187

# Bekannte Probleme

Die folgenden Problem sind zum Zeitpunkt dieser Freigabe bekannt.

Known issue	Issue ID
Google Workspace discovered devices with NULL mac addresses can be provisioned multiple times as agentless automatic, resulting in duplicate entries.	K1-36841
Emojis added to Response Templates are not visible during editing.	K1-36814
SQL syntax error occurs when saving a new report in Managed Install.	K1-36718
Filtering Provisioning Schedules list page using IP Range triggers an error.	K1-36682
Access Control functionality is not working with IPv6 IP.	K1-36411
Due to RabbitMQ upgrade, the SMA will lose user notifications during the upgrade process.	K1-36216
Reports in System UI for ORG-enabled appliances fail when the password includes the '\$' character placed anywhere except at the end. Other special characters do not cause this issue.	K1-35051

# Systemanforderungen

Die mindestens erforderliche Version für die Installation von KACE Systems Management Appliance 15.0 ist 14.1. Wenn auf Ihrer Appliance eine frühere Version ausgeführt wird, müssen Sie eine Aktualisierung auf die angegebene Version durchführen, bevor Sie die Installation fortsetzen können.

Damit die Remote-Steuerungsfunktion ausgeführt werden kann, sind folgende Versionen erforderlich: KACE Systems Management Appliance 14.1 und KACE Agent 14.1. Aktualisieren Sie den KACE Agent und die KACE Systems Management Appliance auf Version 15.0.

Für ein Upgrade von KACE Agent ist mindestens Version 13.0 erforderlich. Wir empfehlen, immer dieselbe Version des Agenten und der KACE Systemverwaltungs-Appliance zu verwenden.

Ab Version 12.0 der Appliance müssen frühere Versionen von KACE Agent, wie z. B. 11.1, speziell für Ihre Appliance-Version signiert werden. Wenn Sie beispielsweise KACE Agent 11.1 mit der Version 12.1 der Appliance verwenden, müssen Sie die KACE Agent 11.1 KBIN-Datei, mit der der Appliance-Schlüssel 12.1 signiert ist, abrufen und installieren. Sie können signierte KACE Agent KBIN-Dateien von der Seite KACE Systemverwaltungs-Appliance *Software Downloads* herunterladen.



**HINWEIS:** Das KACE Agent RPM-Paket kann nur auf verwalteten SUSE Linux-Geräten installiert werden, wenn das `libxslt-tools`-Paket vor dem Agenten-Paket installiert wird.

Um die Versionsnummer der Appliance zu ermitteln, melden Sie sich bei der **Administratorkonsole** an und klicken Sie oben rechts auf das Symbol "?". Klicken Sie dann auf die runde Schaltfläche "i".

Vergewissern Sie sich vor der Aktualisierung auf Version 15.0, dass das System die Mindestanforderungen erfüllt. Diese Anforderungen werden in den technischen Daten der KACE Systems Management Appliance erläutert.

- Virtuelle Appliances: Weitere Informationen finden Sie unter <https://support.quest.com/technical-documents/kace-systems-management-appliance/15.0-common-documents/technical-specifications-for-virtual-appliances>.
- KACE als Dienst: Weitere Informationen finden Sie unter <https://support.quest.com/technical-documents/kace-systems-management-appliance/15.0-common-documents/technical-specifications-for-kace-as-a-service>.

## Produktlizenzierung

Falls Sie derzeit eine KACE Systems Management Appliance Produktlizenz besitzen, ist keine zusätzliche Lizenz erforderlich.

Wenn Sie die KACE Systems Management Appliance zum ersten Mal verwenden, finden Sie ausführliche Informationen zur Produktlizenzierung im Handbuch zur Appliance-Einrichtung. Das entsprechende Handbuch finden Sie unter [Weitere Ressourcen](#).



**HINWEIS:** Produktlizenzen für Version 15.0 können nur für die KACE Systems Management Appliance, auf der Version 14.1 oder höher ausgeführt wird, verwendet werden. Lizenzen für Version 15.0 können nicht auf Appliances verwendet werden, auf denen ältere Versionen wie etwa Version 13.0 ausgeführt werden.

## Installationsanweisungen

Sie können diese Version mit einer mitgeteilten Aktualisierung oder durch das manuelle Hochladen und Anwenden einer Aktualisierungsdatei anwenden. Anweisungen hierzu finden Sie in den Abschnitten zu den folgenden Themen:

- [Aktualisierung vorbereiten](#)
- [Aktualisieren des KACE Systems Management Appliance Servers mit einer beworbenen Aktualisierung](#)
- [Eine Aktualisierung manuell hochladen und anwenden](#)
- [Aufgaben nach der Aktualisierung](#)



**HINWEIS:** Um die Genauigkeit der Softwareerkennung und Installationszahlen für Geräte mit einer bestimmten Software ab Version 7.0 sicherzustellen, wird der Softwarekatalog bei jedem Upgrade neu installiert.

## Aktualisierung vorbereiten

Befolgen Sie vor der Aktualisierung Ihres KACE Systems Management Appliance Servers die folgenden Empfehlungen:

- **WICHTIG: Aktivieren von Booten aus Legacy-BIOS:**

Während eines Upgrades kann ein Problem beim Booten aus der UEFI BIOS ausgelöst werden. Um dies zu verhindern, müssen Sie sicherstellen, dass das Booten aus Legacy-BIOS aktiviert ist. Das Gerät muss vor dem Umschalten ausgeschaltet werden. Stellen Sie außerdem bei ESX-basierten virtuellen Maschinen sicher, dass die Hardwareversion 13 oder höher ist.

Vor der Anwendung des Appliance-Updates müssen Sie sicherstellen, dass der Cache Ihres Browsers leer ist und dass Port 52231 von Ihrem Browser auf die Appliance verfügbar ist. Benutzer, die von zu Hause aus arbeiten, müssen möglicherweise ihre Unternehmens-Firewall so konfigurieren, dass sie die Kommunikation über Port 52231 zulässt.

- **Überprüfen Sie die Serverversion Ihrer KACE Systems Management Appliance:**

Die mindestens erforderliche Version für die Installation von KACE Systems Management Appliance 15.0 ist 14.1. Wenn auf Ihrer Appliance eine frühere Version ausgeführt wird, müssen Sie eine Aktualisierung auf die angegebene Version durchführen, bevor Sie die Installation fortsetzen können.

Um die Versionsnummer der Appliance zu ermitteln, melden Sie sich bei der **Administratorkonsole** an und klicken Sie oben rechts auf das Symbol "?". Klicken Sie dann auf die runde Schaltfläche "i".

- **Überprüfen Sie die KACE Agent-Version.**

Für ein Upgrade von KACE Agent ist mindestens Version 13.0 erforderlich. Wir empfehlen, immer dieselbe Version des Agenten und der KACE Systemverwaltungs-Appliance zu verwenden.

Ab Version 12.0 der Appliance müssen frühere Versionen von KACE Agent, wie z. B. 11.1, speziell für Ihre Appliance-Version signiert werden. Wenn Sie beispielsweise KACE Agent 11.1 mit der Version 12.1 der Appliance verwenden, müssen Sie die KACE Agent 11.1 KBIN-Datei, mit der der Appliance-Schlüssel 12.1 signiert ist, abrufen und installieren. Sie können signierte KACE Agent KBIN-Dateien von der Seite KACE Systemverwaltungs-Appliance *Software Downloads* herunterladen.



**HINWEIS:** Das KACE Agent RPM-Paket kann nur auf verwalteten SUSE Linux-Geräten installiert werden, wenn das `libxslt-tools`-Paket vor dem Agenten-Paket installiert wird.

- **Führen Sie eine Sicherung durch, bevor Sie beginnen.**

Sichern Sie Ihre Datenbank und Ihre Dateien und legen Sie diese für spätere Zwecke an einem Speicherort außerhalb des KACE Systems Management Appliance Servers ab. Anweisungen zur Sicherung Ihrer Datenbank und Ihrer Dateien finden Sie im **Administratorhandbuch** unter <https://support.quest.com/technical-documents/kace-systems-management-appliance/15.0%20common%20documents/administration-guide>

- **Vor Version 7.0 installierte Appliances.**

Bei Appliances, die ursprünglich vor Version 7.0 installiert wurden und für die noch kein neues Image (physische Appliances) erstellt wurde oder die noch nicht neu installiert wurden (virtuell), empfiehlt Quest Software dringend, die Datenbank zu exportieren, neu zu erstellen (über ein Image oder die Installation einer virtuellen Maschine über eine OVF-Datei) und vor der Aktualisierung auf Version 14.1 neu zu importieren. Weitere Informationen hierzu finden Sie unter <https://support.quest.com/kace-systems-management-appliance/kb/4281031/how-to-re-image-kace-system-management-appliance-sma>.

Wenn Ihre Appliance-Version mehrere Versionen umfasst, finden Sie im folgenden Artikel nützliche Tipps zur Aktualisierung: <https://support.quest.com/kace-systems-management-appliance/kb/4284819/sma-server-and-agent-upgrade-path>.

Die Appliance über ein Image neu zu erstellen bietet zahlreiche Vorteile. Das neue Laufwerk-Layout bietet beispielsweise eine verbesserte Kompatibilität mit Version 15.0. Zudem profitieren Sie von Verbesserungen bei Sicherheit und Leistung.

- **Stellen Sie sicher, dass Port 52231 verfügbar ist.**

Vor einem `.kbin`-Upgrade muss Port 52231 verfügbar sein, damit die Seite KACE Upgrade-Konsole zugänglich ist. Wenn das Upgrade initiiert wird, ohne diesen Port verfügbar zu machen, können Sie den Fortschritt des Upgrades nicht verfolgen. Quest KACE empfiehlt dringend, Datenverkehr von einem vertrauenswürdigen System über Port 52231 zuzulassen und das Upgrade von der Upgrade-Konsole aus zu überwachen. Ohne Zugriff auf die Upgrade-Konsole wird das Upgrade zu einer Seite umgeleitet, auf die nicht zugegriffen werden kann, was im Browser als Timeout angezeigt wird. Dies kann den Anschein vermitteln, dass das Upgrade das System zum Absturz gebracht hat, woraufhin häufig der Kasten neu gestartet wird, obwohl das Upgrade noch ausgeführt wird. Wenn Sie sich nicht sicher sind, wie weit das Upgrade fortgeschritten ist, wenden Sie sich an den KACE-Support und **starten Sie die Appliance nicht neu.**

# Aktualisieren des KACE Systems Management Appliance Servers mit einer beworbenen Aktualisierung

Sie können den KACE Systems Management Appliance mithilfe einer Aktualisierung aktualisieren, die auf der Seite *Dashboard* oder *Appliance-Aktualisierungen* der **Administratorkonsole** zur Verfügung gestellt wird.

**CAU** **VORSICHT:** Während einer Aktualisierung dürfen Sie keinen manuellen Neustart des KACE Systems Management Appliance Servers durchführen.

1. Sichern Sie Ihre Datenbank und die entsprechenden Dateien. Anweisungen hierzu finden Sie im **Administratorhandbuch** unter <https://support.quest.com/technical-documents/kace-systems-management-appliance/15.0%20common%20documents/administration-guide>
2. Navigieren Sie zur *Systemsteuerung* der Appliance:
  - Wenn die Organisationskomponente auf der Appliance nicht aktiviert ist, klicken Sie auf **Einstellungen**.
  - Wenn die Organisationskomponente auf der Appliance aktiviert ist: Melden Sie sich bei der Systemverwaltungskonsole der Appliance an: `http://KACE_SMA_hostname/system`. Oder wählen Sie in der Dropdown-Liste oben rechts auf der Seite **System** und dann **Einstellungen** aus.
3. Klicken Sie auf der linken Navigationsleiste auf **Appliance-Aktualisierungen**, um die Seite *Appliance-Aktualisierungen* anzuzeigen.
4. Klicken Sie auf **Überprüfen, ob aktuelle Serverversionen verfügbar sind**.  
Die Ergebnisse der Überprüfung werden im Protokoll angezeigt.
5. Wenn eine Aktualisierung verfügbar ist, klicken Sie auf **KBIN anwenden**.

**Imp** **WICHTIG:** Während der ersten 10 Minuten stürzen einige Browser scheinbar ab, während die Aktualisierung entpackt und überprüft wird. Verlassen oder aktualisieren Sie die Seite während dieses Zeitraums nicht und klicken Sie nicht auf Browserschaltflächen auf der Seite, da diese Aktionen den Vorgang unterbrechen würden. Nachdem die Aktualisierung entpackt und überprüft wurde, wird die Seite *Protokolle* angezeigt. Starten Sie die Appliance während des Aktualisierungsvorgangs nicht manuell neu.

Die Version 15.0 wird angewandt und der KACE Systems Management Appliance Server wird neu gestartet. Der Bearbeitungsstatus wird im Browserfenster und in der Administratorkonsole angezeigt.

6. Wenn das Server-Upgrade abgeschlossen ist, aktualisieren Sie alle Agenten auf Version 15.0.

## Eine Aktualisierung manuell hochladen und anwenden

Wenn Sie eine Aktualisierungsdatei von Quest erhalten haben, können Sie diese manuell hochladen, um den KACE Systems Management Appliance Server zu aktualisieren.

**CAU** **VORSICHT:** Während einer Aktualisierung dürfen Sie keinen manuellen Neustart des KACE Systems Management Appliance Servers durchführen.

1. Sichern Sie Ihre Datenbank und die entsprechenden Dateien. Anweisungen hierzu finden Sie im **Administratorhandbuch** unter <https://support.quest.com/technical-documents/kace-systems-management-appliance/15.0%20common%20documents/administration-guide>
2. Melden Sie sich mit Ihren Kundenanmeldeinformationen auf der Quest Website an: <https://support.quest.com/kace-systems-management-appliance/download-new-releases>. Laden Sie die KBIN-Datei des KACE Systems Management Appliance Servers für die allgemein verfügbare Version 15.0 GA (general availability, Allgemeine Verfügbarkeit) herunter und speichern Sie sie lokal.
3. Klicken Sie auf der linken Navigationsleiste auf **Appliance-Aktualisierungen**, um die Seite *Appliance-Aktualisierungen* anzuzeigen.
4. Im Abschnitt *Manuell aktualisieren*:
  - a. Klicken Sie auf **Durchsuchen** oder auf **Datei auswählen** und suchen Sie nach der Aktualisierungsdatei.
  - b. Klicken Sie auf **KBIN anwenden** und dann zur Bestätigung auf **Ja**.

**Die Version 15.0 wird angewandt und der KACE Systems Management Appliance Server wird neu gestartet. Der Bearbeitungsstatus wird im Browserfenster und in der Administratorkonsole angezeigt.**

5. Wenn das Server-Upgrade abgeschlossen ist, aktualisieren Sie alle Agenten auf Version 15.0.

## Aufgaben nach der Aktualisierung

Überprüfen Sie im Anschluss an die Aktualisierung, ob diese erfolgreich war und die richtigen Einstellungen festgelegt sind.

### Erfolgreichen Abschluss überprüfen

Überprüfen Sie den erfolgreichen Abschluss, indem Sie die KACE Systems Management Appliance Versionsnummer kontrollieren.

1. Navigieren Sie zur *Systemsteuerung* der Appliance:
  - **Wenn die Organisationskomponente auf der Appliance nicht aktiviert ist, klicken Sie auf Einstellungen.**
  - **Wenn die Organisationskomponente auf der Appliance aktiviert ist: Melden Sie sich bei der Systemverwaltungskonsolle der Appliance an: `http://KACE_SMA_hostname/system`. Oder wählen Sie in der Dropdown-Liste oben rechts auf der Seite **System** und dann **Einstellungen** aus.**
2. Um die aktuelle Version zu ermitteln, klicken Sie oben rechts auf das Symbol "?" und dann auf die runde Schaltfläche "i".

## Sicherheitseinstellungen überprüfen

Zur Erhöhung der Sicherheit wird während der Aktualisierung der Datenbankzugriff per HTTP und FTP deaktiviert. Wenn Sie mithilfe dieser Methoden auf Datenbankdateien zugreifen, ändern Sie die Sicherheitseinstellungen nach der Aktualisierung entsprechend.

1. Navigieren Sie zur *Systemsteuerung* der Appliance:
    - Wenn die Organisationskomponente auf der Appliance nicht aktiviert ist, klicken Sie auf **Einstellungen**.
    - Wenn die Organisationskomponente auf der Appliance aktiviert ist: Melden Sie sich bei der Systemverwaltungskonsolle der Appliance an: `http://KACE_SMA_hostname/system`. Oder wählen Sie in der Dropdown-Liste oben rechts auf der Seite **System** und dann **Einstellungen** aus.
  2. Gehen Sie zu **Einstellungen** > **Systemsteuerung** und klicken Sie unter *Sicherheitseinstellungen* auf **Netzwerksicherheit und -zugänglichkeit konfigurieren**.
  3. Ändern Sie auf der Registerkarte **Sicherheitsoptionen** die folgenden Einstellungen:
    - # **Aktivieren von „Sicherungsdateien sichern“**: Deaktivieren Sie dieses Kontrollkästchen, damit Benutzer per HTTP ohne Authentifizierung auf Datenbanksicherungsdateien zugreifen können.
    - # **Datenbankzugriff aktivieren**: Aktivieren Sie dieses Kontrollkästchen, damit Benutzer über Port 3306 auf die Datenbank zugreifen können.
    - # **Sicherung über FTP aktivieren**: Aktivieren Sie dieses Kontrollkästchen, damit Benutzer per FTP auf Datenbanksicherungsdateien zugreifen können.
- CAUTION** **VORSICHT:** Die Änderung dieser Einstellungen verringert die Sicherheit der Datenbank und wird aus diesem Grund nicht empfohlen.
4. Klicken Sie auf **Speichern**.
  5. **Nur KBIN-Upgrades**. Erschweren Sie den Zugriff auf Root-Kennwort (2FA) für die Appliance.
    - a. Klicken Sie in der Systemverwaltungskonsolle auf **Einstellungen** > **Support**.
    - b. Klicken Sie auf der Seite *Support* unter *Problembewältigungstools* auf **Zweifaktor-Authentifizierung**.
    - c. Klicken Sie auf der Seite *System unterstützt Zweifaktor-Authentifizierung* auf **Geheimen Schlüssel ersetzen**.
    - d. Notieren Sie die Token und bewahren Sie diese Informationen an einem sicheren Ort auf.

## Weitere Ressourcen

Zusätzliche Informationen erhalten Sie in den folgenden Ressourcen:

- Online-Produktdokumentation (<https://support.quest.com/kace-systems-management-appliance/15.0/technical-documents>)
    - # **Technische Daten**: Informationen zu den Mindestanforderungen bei der Installation der bzw. Aktualisierung auf die aktuelle Version des Produkts.
- Virtuelle Appliances**: Weitere Informationen finden Sie unter <https://support.quest.com/technical-documents/kace-systems-management-appliance/15.0-common-documents/technical-specifications-for-virtual-appliances>.

**KACE als Dienst:** Weitere Informationen finden Sie unter <https://support.quest.com/technical-documents/kace-systems-management-appliance/15.0-common-documents/technical-specifications-for-kace-as-a-service>.

- # **Einrichtungshandbücher:** Anweisungen zum Einrichten virtueller Appliances. Die Dokumentation der neuesten Version finden Sie unter <https://support.quest.com/kace-systems-management-appliance/15.0/technical-documents>.
- # **Administratorhandbuch:** Anweisungen zur Verwendung der Appliance. Die Dokumentation der neuesten Version finden Sie unter <https://support.quest.com/technical-documents/kace-systems-management-appliance/15.0%20common%20documents/administration-guide>.

## Globalisierung

Dieser Abschnitt enthält Informationen zum Installieren und Verwenden dieses Produkts in nicht englischsprachigen Konfigurationen (beispielsweise für Kunden außerhalb Nordamerikas). Dieser Abschnitt ersetzt nicht die anderen Angaben zu unterstützten Plattformen und Konfigurationen in der Produktdokumentation.

Diese Version ist für Unicode aktiviert und unterstützt alle Zeichensätze. In dieser Version sollten alle Produktkomponenten für die Verwendung derselben oder kompatibler Zeichenkodierungen konfiguriert und so installiert werden, dass sie dieselben Gebietsschema- und Regionsoptionen verwenden. Diese Version unterstützt die Verwendung in folgenden Regionen: Nordamerika, Westeuropa und Lateinamerika, Mittel- und Osteuropa, Fernost (Asien), Japan.

Diese Version wurde für die folgenden Sprachen lokalisiert: Französisch, Deutsch, Japanisch, Portugiesisch (Brasilien), Spanisch.

Quest entwickelt Softwarelösungen, die sich die Vorteile neuer Technologien bei einer immer komplexer werdenden IT-Infrastruktur zu Nutze machen. Von der Datenbank- und Systemverwaltung über Active Directory- und Office 365-Verwaltung bis hin zur Erhöhung der Widerstandskraft gegen Cyberrisiken unterstützt Quest Kunden bereits jetzt bei der Bewältigung ihrer nächsten IT-Herausforderung. Weltweit verlassen sich mehr als 130.000 Unternehmen und 95 % der Fortune 500-Unternehmen auf Quest, um proaktive Verwaltung und Überwachung für die nächste Unternehmensinitiative bereitzustellen, die nächste Lösung für komplexe Microsoft-Herausforderungen zu finden, und der nächsten Bedrohung immer einen Schritt voraus zu sein. Quest Software. Wo die Zukunft auf die Gegenwart trifft. Weitere Informationen hierzu finden Sie unter [www.quest.com](http://www.quest.com).

## Ressourcen für den technischen Support

Der technische Support steht Quest Kunden mit gültigem Servicevertrag sowie Kunden mit Testversionen zur Verfügung. Auf das Quest Support Portal können Sie unter <https://support.quest.com/de-de/> zugreifen.

Im Support-Portal finden Sie Tools zur Selbsthilfe, mit denen Probleme rund um die Uhr schnell und selbständig gelöst werden können. Das Support-Portal bietet folgende Möglichkeiten:

- Einreichen und Verwalten einer Serviceanfrage
- Anzeigen von Knowledge Base-Artikeln
- Registrieren für Produktbenachrichtigungen
- Herunterladen von Software und technischer Dokumentation
- Anzeigen von Anleitungsvideos
- Teilnehmen an Community-Diskussionen
- Online Chatten mit Supporttechnikern
- Anzeigen von Services, die Sie bei Ihrem Produkt unterstützen können

## Rechtliche Hinweise

© 2025 Quest Software Inc. ALLE RECHTE VORBEHALTEN.

Dieses Handbuch enthält proprietäre Informationen, die urheberrechtlich geschützt sind. Die in diesem Handbuch beschriebene Software wird im Rahmen einer Softwarelizenz oder einer Geheimhaltungsvereinbarung bereitgestellt. Diese Software darf nur im Einklang mit den Bestimmungen der entsprechenden Vereinbarung kopiert werden. Kein Teil dieses Handbuchs darf ohne schriftliche Genehmigung von Quest Software Inc. in irgendeiner Form oder auf irgendeine Weise vervielfältigt oder übertragen werden. Dies beinhaltet Fotokopien und Aufzeichnungen für einen anderen Zweck als die persönliche Nutzung durch den Käufer.

Die Informationen in diesem Dokument werden in Verbindung mit Quest Software Produkten bereitgestellt. Durch dieses Dokument bzw. in Verbindung mit dem Verkauf von Quest Software Produkten wird keine ausdrückliche oder stillschweigende Lizenz, weder durch Duldung noch anderweitig, für Rechte des geistigen Eigentums von Quest Software gewährt. SOFERN NICHT DURCH DIE BEDINGUNGEN UND BESTIMMUNGEN IN DER LIZENZVEREINBARUNG FÜR DIESES PRODUKT ANDERWEITIG ANGEGEBEN, ÜBERNIMMT QUEST SOFTWARE KEINERLEI HAFTUNG UND SCHLIESST JEDE AUSDRÜCKLICHE, STILLSCHWEIGENDE ODER GESETZLICHE GEWÄHRLEISTUNG FÜR SEINE PRODUKTE AUS, EINSCHLIESSLICH, ABER NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT, DER EIGNUNG ZU EINEM BESTIMMTEN ZWECK ODER DER NICHTVERLETZUNG VON RECHTEN DRITTER. QUEST SOFTWARE ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE ODER INDIREKTE SCHÄDEN, FOLGESCHÄDEN, STRAFEN, BESONDERE SCHÄDEN ODER NEBENSCHÄDEN (EINSCHLIESSLICH, ABER NICHT BESCHRÄNKT AUF SCHÄDEN WEGEN ENTGANGENER GEWINNE,

BETRIEBSUNTERBRECHUNGEN ODER DATENVERLUST), DIE AUS DER VERWENDUNG ODER UNFÄHIGKEIT ZUR VERWENDUNG DIESES DOKUMENTS ENTSTEHEN, SELBST WENN QUEST SOFTWARE AUF DIE MÖGLICHKEIT SOLCHER SCHÄDEN HINGEWIESEN WURDE. Quest Software macht keine Zusicherungen oder Gewährleistungen bezüglich der Richtigkeit oder Vollständigkeit der Inhalte dieses Dokuments und behält sich das Recht vor, jederzeit und ohne vorherige Ankündigung Änderungen an den Spezifikationen und Produktbeschreibungen vorzunehmen. Quest Software übernimmt keine Verpflichtung zur Aktualisierung der in diesem Dokument enthaltenen Informationen.

Fragen zur möglichen Verwendung dieses Materials richten Sie bitte an:

Quest Software, Inc.

Attn.: LEGAL Dept

4 Polaris Way

Aliso Viejo, CA 92656, USA

Informationen zu regionalen und internationalen Niederlassungen finden Sie auf unserer Website (<https://www.quest.com/de-de>).

#### Patente

Quest Software ist stolz auf seine fortschrittliche Technologie. Für dieses Produkt können Patente bzw. Patentanmeldungen bestehen. Aktuelle Informationen zum bestehenden Patentschutz für dieses Produkt finden Sie auf unserer Website unter <https://www.quest.com/legal>.

#### Marken

Quest, das Quest Logo, Join the Innovation und KACE sind Marken und registrierte Marken von Quest Software Inc. Eine vollständige Liste der Marken von Quest finden Sie unter <https://www.quest.com/legal/trademark-information.aspx>. Alle anderen Marken und eingetragenen Marken sind Eigentum ihrer jeweiligen Besitzer.

#### Legende

**CAUTION:** Das Symbol **VORSICHT** weist auf eine mögliche Beschädigung von Hardware oder den möglichen Verlust von Daten hin, wenn die Anweisungen nicht befolgt werden.

**IMPORTANT, TIP, MOBILE or VIDEO:** Ein Informationssymbol weist auf ergänzende Informationen hin.

KACE Systems Management Appliance Administratorhandbuch

Letzte Überarbeitung: Dezember 2025

Software-Version: 15.0