KACE® Systemverwaltungs-Appliance 11.1

# Versionshinweise

# Inhaltsverzeichnis

**Quest® KACE® Systems Management Appliance 11.1 – Versionshinweise ..... 3**
Über die KACE Systems Management Appliance 11.1 ..... 3
Neue Funktionen ..... 3
Verbesserungen ..... 5
Behobene Probleme ..... 6
Bekannte Probleme ..... 10
Systemanforderungen ..... 12
Produktlizenzierung ..... 12
Installationsanweisungen ..... 13
Aktualisierung vorbereiten ..... 13
Aktualisieren des KACE Systems Management Appliance Servers mit einer beworbenen Aktualisierung ..... 14
Eine Aktualisierung manuell hochladen und anwenden ..... 15
Aufgaben nach der Aktualisierung ..... 15
Erfolgreichen Abschluss überprüfen ..... 15
Sicherheitseinstellungen überprüfen ..... 16
Weitere Ressourcen ..... 16
Globalisierung ..... 17
Über uns ..... 17
Ressourcen für den technischen Support ..... 17
Rechtliche Hinweise ..... 18

# Quest® KACE® Systems Management Appliance 11.1 – Versionshinweise

Dieses Dokument enthält Informationen zur KACE Systems Management Appliance Version 11.1.

# Über die KACE Systems Management Appliance 11.1

KACE Systems Management Appliance ist eine virtuelle Appliance, die zur Automatisierung der Geräteverwaltung, der Anwendungsbereitstellung, des Patchings, des Asset-Managements und der Service Desk-Ticketverwaltung entwickelt wurde. Weitere Informationen zur KACE Systems Management Appliance Serie finden Sie unter https://www.quest.com/products/kace-systems-management-appliance/. Diese Version enthält eine Reihe neuer Funktionen, behobener Probleme und Sicherheitsverbesserungen.

**HINWEIS:** Dies ist das einzige Dokument, das für diese Version übersetzt wird. Die lokalisierten Varianten enthalten jedoch keine Informationen zu behobenen Problemen, Verbesserungen und bekannten Problemen. Andere Handbücher wie das *Administratorhandbuch* und die produktinterne Hilfe wurden bisher nicht lokalisiert, und Dokumente zur Version 10.2 sind enthalten.

# Neue Funktionen

Diese Version der KACE Systems Management Appliance beinhaltet die folgenden Funktionen.

**Gerätekommunikation**

- **Hinzugefügte Taskleistenaktionen für KACE Agent**: Weitere Funktionen zum Agentensymbol in der Taskleiste hinzugefügt, z. B. Öffnen von Links. Ihre Systemadministratoren können bis zu zehn Links angeben, die im neuen Menüpunkt **Verknüpfungen** angezeigt werden. Dieser Menüpunkt wird nur angezeigt, wenn in den Agenten-Kommunikationseinstellungen im Abschnitt Agentenstatus-Symbolverknüpfungen mindestens ein Link angegeben ist.

  Standard-URI-Links (Uniform Resource Identifier) werden unterstützt, wie z. B. HTTP-, SSH- und FTP-URLs. Wenn Sie auf diesen Link klicken, startet Ihr System die Anwendung, die mit der ausgewählten Ressource verknüpft ist. Wenn Sie beispielsweise auf einen Link vom Typ HTTP klicken, öffnet Ihr System den Link im Standardbrowser.
- **Hyper-V-Inventar**: Inventarinformationen und zugehörige Gerätebefehle wurden in dieser Version für Virtual Machine Manager- und MS Hyper-V-Daten für agentenverwaltete Geräte hinzugefügt. Die

Inventarinformationen umfassen eine Liste der zu inventarisierenden virtuellen Maschinen und Hyper-V-Hosts. Dies ähnelt der in Version 10.0 erstellten VMware-Inventarfunktion.

- **Aktualisierungen beim Support von Betriebssystemen**: Die Appliance unterstützt jetzt die folgenden Betriebssystemversionen auf Geräten mit Agentenverwaltung:
  - MS Windows 10 20H2
  - MS Windows Server 2019 20H2
  - macOS 11.0
    - Bei der Verbindung mit **Benutzerkonsole** über HTTPS von einem macOS 11.0-System kann die Appliance die eindeutige Kennung (KUID) des Agenten, der mit diesem System verknüpft ist, nicht ermitteln. Dies wirkt sich auf die Liste *Meine Geräte* und die Softwarebibliotheken-Installationen aus. Die Ursache dieses Problems ist die neue Anforderung für macOS 11.0, dass alle Zertifikatsvertrauenseinstellungen vom Benutzer genehmigt werden müssen. Dieses Problem führt auch dazu, dass der folgende Eintrag in `konea.log` auf dem Agenten angezeigt wird:

      ```
      |ERROR|ssl_darwin.go:107:AddCertAsTrustedRoot |
      SecTrustSettingsSetTrustSettings failed|{"err":"Die Autorisierung wurde
      verweigert, da keine Benutzerinteraktion möglich war."}
      ```

    - Die Appliance unterstützt das Betriebssystem-Patching für diese Version nicht. Anwendungs-Patching ist verfügbar. Patching auf Betriebssystemebene für macOS 11.0-Geräte ist mit dem KACE Cloud Mobile Device Manager (MDM) verfügbar, wenn Sie über ein Abonnement verfügen.

**Patchen:**

- **Linux-Paket-Upgrades**: Mit der Appliance können Sie nun die Installation und Verwaltung von Linux-Paket-Upgrades automatisieren, um das Linux-Betriebssystem auf Ihren verwalteten Linux RedHat-, SUSE-, Ubuntu-, CentOS- und Raspbian-Geräten auf dem neuesten Stand zu halten. Diese Upgrades verbessern die Gesamtleistung Ihrer verwalteten Linux-Geräte und schützen sie vor potenziellen Schwachstellen.

  Verwenden Sie diese Funktion, um Upgrade-Zeitpläne zu erstellen, mit denen Sie entweder Paket-Upgrades erkennen oder alle anwendbaren Pakete erkennen und upgraden können. Sie können die Liste der verfügbaren Paket-Upgrades nach einer „Nur erkennen“-Zeitplanaktion für jede Linux-Variante einsehen.

  Der Upgrade-Vorgang basiert auf der Annahme, dass Ihre verwalteten Linux-Geräte auf die entsprechenden Paket-Repositorys verweisen. Nur die Pakete mit Sicherheitsaktualisierungen werden identifiziert. Die Appliance versucht nicht, alle Pakete zu erkennen oder zu aktualisieren oder das gesamte Betriebssystem auf die neueste Version zu aktualisieren.

  **HINWEIS:** Raspbian-Linux unterscheidet nicht zwischen regelmäßigen und Sicherheitsaktualisierungen. Wenn Pakete für verwaltete Raspbian-Geräte erkannt und aktualisiert werden, werden alle aktualisierten Pakete auf diesen Geräten installiert.

- **Integration mit dem neuen Dell-Hardware-Aktualisierungskatalog**: Ab dieser Version verwendet die Appliance eine neue Version des Dell-Hardwarekatalogs. Der Prozess der Erkennung und Bereitstellung von Hardware-Aktualisierungen ähnelt dem Prozess für das Geräte-Patching. Beginnen Sie mit der Erstellung von Zeitplanaktualisierungen, um Hardware-Updates entweder zu erkennen, bereitzustellen oder zu erkennen und bereitzustellen. Sie können die Liste der verfügbaren Dell-Updates auf der Katalogseite einsehen. Auf dieser Seite werden die Aktualisierungen aufgeführt, für die Signaturdateien auf der Appliance vorhanden sind.
  - Für diese Funktion muss die neueste Version des KACE Agent auf verwalteten Dell-Geräten ausgeführt werden.
  - Vorhandene Daten im Zusammenhang mit Dell-Hardware-Aktualisierungen, wie z. B. der Zeitplanverlauf, werden nicht von früheren Versionen der Appliance migriert.
  - Benutzerberichte, die mit Dell-Hardwareaktualisierungen verknüpft und mit einer früheren Version der Appliance erstellt wurden, werden nicht auf Version 11.1 migriert.

### Infrastruktur

- **Oval für Linux und Mac**: In dieser Version erweitert die Appliance die Unterstützung von Oval über die bestehende reine MS Windows-Anwendung hinaus, wobei die weltweit größte und beste Auswahl an CVE-Daten verwendet wird.
- **Warnungen zur Lizenzerneuerung**: Wenn die Appliance-Wartung abläuft, stehen einige Funktionen, wie z. B. Patching-Support, nicht mehr zur Verfügung. Dadurch wird eine Fehlerwarnung auf dem Home-Dashboard angezeigt. Um Ihre Lizenz zu erneuern, gehen Sie zu https://support.quest.com/contact-us/renewals.

### Service Desk

- **Hierarchie der Service Desk-Ticketkategorien**: Die Administratorkonsole wurde verbessert, um das Einrichten von Kategorien und Unterkategorien für den Service Desk zu vereinfachen. Sie können Ticketkategorie- und Unterkategorieknoten mit einem Baum-Widget erstellen und bearbeiten. In der Baumansicht können Sie die Beziehungen zwischen den Kategorien besser nachvollziehen und verwalten. Sie können ganz einfach neue Kategorieknoten hinzufügen, sie umbenennen, löschen oder sortieren. Eine Suchfunktion, um schnell eine bestimmte Kategorie oder Unterkategorie zu finden, ist ebenfalls verfügbar.
- **Möglichkeit, Service Desk-Ticketpräfix anzugeben**: Ab dieser Version können Sie für jede Warteschlange ein anderes Präfix verwenden, um Ihren Service Desk-Workflow zu organisieren und diese mit entsprechenden Kategorien zu verknüpfen, wie z. B. `HELP:` für Helpdesk oder `HDREQ:` für Hardware- und Softwareanforderungen.
- **Unterstützung des Microsoft 365 GCC High-Service**: Mit Ihren OAuth-Anmeldeinformationen für MS Office 365 können Sie jetzt Ihren Azure AD-Mandantentyp und die Endpunkt-URL angeben, um Token für die nationale Cloud zu erhalten, die mit Ihrer Umgebung verknüpft ist. Wenn Sie eine Office 365-OAuth für eingehende Service Desk-E-Mails auswählen, können Sie auf einen entsprechenden Microsoft 365-API-Dienst verweisen, z. B. Microsoft 365 GCC, Microsoft 365 GCC High und andere. Insbesondere Microsoft 365 GCC High wird in Umgebungen mit hoher Sicherheit verwendet.

# Verbesserungen

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

| Verbesserung | ID des Problems |
|---|---|
| Windows Installer now preserves the `NoHooks userinit` registry setting during upgrade. | K1A-2393 |
| Managed Installation can continue if the Agent disconnects. | K1A-2392 |
| KACE Agent no verifies the Konea tunnel and alerts the server if broken. | K1A-2384 |
| The user is alerted when reboot is pending and patching operations are skipped as a result. | K1A-2381 |
| 11.1 KACE macOS agents use PKG installer file rather than DMG disk image. | K1A-2374 |
| API access can now be restricted through the *Access Control List Details* page. | K1-30596 |
| This version includes the ability to sort by custom ticket fields in KACE GO. | K1-30562 |

| Verbesserung | ID des Problems |
|---|---|
| SAML-enabled systems can now be locked down to allow access only to SAML-authenticated users and the local `admin` user. | K1-30246 |
| This version includes an option to reject SAML users who do not already have an account on the appliance. | K1-30211 |
| *Approval Status* column is added to the *Quarantine* list and *Quarantine Detail* pages. | K1-30105 |
| In the *General Settings* page, an option is added to indicate interest in participation in a future Beta program. | K1-30071 |
| The appliance now includes the ability to select an Azure AD *GCC High account* during the creation of credentials for a Office365 OAuth account, and to set the URL endpoint for a .us domain. | K1-22281 |
| In the email notification text editor, the **$** button now allows insertion of tokens. | K1-22082 |
| Added the ability to select a *single-tenant* Azure AD account type during the creation of credentials for a Office365 OAuth account. | K1-21914 |
| User's manager can now be reset to *Unassigned* either manually through the **Administratorkonsole**, or during LDAP import with an empty manager mapped field. | K1-19328 |
| Discovery schedules for devices associated with an Active Directory server, now include a new option for enabling the appliance to use a secure port for LDAP communication, **Use Secure LDAP (LDAPS)**. This check box is available in the *Active Directory* section on the *Discovery Schedule Detail* page, when you select **Active Directory** as the *Discovery Type*. | N/A |
| Access Control List restrictions can be now applied based on sub-domains. You can specify the sub-domain name on the *Access Control List* page, in the *IP Address/ Doomain* column of the *Allow List*. | N/A |

# Behobene Probleme

Im Anschluss finden Sie eine Liste mit Problemen, die in dieser Version behoben wurden:

**Resolved Service Desk issues**

| Behobenes Problem | ID des Problems |
|---|---|
| Creating a Service Desk process template that included a separator could result in an error when used from the User Portal. | K1-30698 |
| *Time Closed*, *Time Stalled* and *Time Opened* are not updated for a parent ticket with approvals. | K1-30685 |
| When copying text from a Word application to a ticket, the formatting could not be retained. | K1-30545 |

| Behobenes Problem | ID des Problems |
|---|---|
| When duplicating a process, the ticket template was not duplicated. | K1-30460 |
| Tickets with very long summary fields could result in an error when the *Tickets* list page loads. | K1-23726 |
| Default ticket template is not set when creating a new ticket by email. | K1-23422 |
| Unexpected rendering behavior (scrolling) could be seen when viewing ticket details when multiple categories and sub-categories are present. | K1-22645 |
| In the Service Desk list view, *Time Open* and *Time Opened* are renamed to *Time Since Last Opened* and *Last Opened*, respectively. | K1-22630 |
| Emails sent with display names with a comma or multi-language character to a Service Desk queue through POP3 was not handled correctly, in some cases. | K1-22610 |
| Image was broken using several variables in email templates. | K1-21347 |
| *Email On Event* ticket notification emails were formatted differently than Custom Ticket Rule emails. | K1-21198 |
| Default value was not displayed on ticket detail page for drop-down fields with *Always Required* option. | K1-21187 |
| Service Desk: Token emails from Gmail to Gmail leaved behind empty spaces. | K1-21186 |
| When a ticket is submitted by email with embedded dark colors, the text was hidden if the **Administratorkonsole** is also set to a dark theme. | K1-21147 |
| Process parent ticket did not close if child tickets were closed from *Tickets* list view. | K1-21143 |
| Service Desk email notifications broke if templates exceeded character limits. | K1-21118 |
| Advanced Search: Filters did not work as expected when using Unassigned Owner. | K1-21116 |
| Advanced Search in *Tickets* list: Filters did not work as expected when using *Status* and *Process Status*. | K1-21107 |
| Populating a Service Desk ticket multi-selection custom field with double quotes in the select value resulted in unexpected behavior. | K1-21094 |
| Ticket attachment links sent in email notifications did not work as expected in some cases. | K1-19964 |

### Resolved KACE Agent issues

| Behobenes Problem | ID des Problems |
|---|---|
| CentOS receives all updates with the Linux Update feature. The security filter is not available for the Linux Package Upgrades page. | K1A-3810 |

| Behobenes Problem | ID des Problems |
|---|---|
| KACE Agent 11.0 failed to download file from HTTPS source, impacting use of replication shares that are accessed through the HTTPS protocol. | K1A-2330 |
| Client certificate install operation could timeout on newly provisioned Windows devices, preventing the agent from receiving any commands from the appliance until a reconnect event happened. | K1A-2329 |
| VMM managed Hyper-V host was not added to appliance during VMM inventory when the Agent is installed on some Hyper-V hosts. | K1A-2328 |
| Replication did work when password had an '@' symbol. | K1A-2326 |
| macOS 11.0 (Big Sur): Installing KACE Agent with the Agent Status icon enabled resulted in warnings during installation. | K1A-2318 |
| `konea.exe` and `clientidentifier.exe` could crash in some environments. | K1A-2291 |
| Recurring Alert messages kept spawning new Windows on endpoint. | K1A-2289 |
| Wake-on-LAN (WoL) through relay did not display error when the relay agent selected was down. | K1A-2285 |
| Tokens were treated as invalid by agents (error: Agent token signed by another server) if the appliance database became out of sync with the file system. | K1-30642 |
| SNMP inventory data from Dell servers could cause inventory to fail. | K1-30615 |
| In the **Systemverwaltungskonsole**, on the *Agent Token Detail* page, *Organization* is represented with its ID instead of name. | K1-29969 |
| Offline KScripts did not run when scheduled for *Run on the* instance/day of week. | K1-21173 |
| MSI Policy wizard script could fail to set the registry value correctly. | K1-21049 |
| Scripting option *Allow run without a logged-in user* cleared still allowed script to run. | K1-19576 |
| SMB URLs did not properly handle passwords with special characters. | K1-17342 |

### Resolved Inventory issues

| Behobenes Problem | ID des Problems |
|---|---|
| SNMP inventory mistakenly identified non-hex strings as hex strings, causing incorrect values in some cases. | K1-30668 |
| Dell Warranty retrieval errors were not logged to the new `dell_warranty_log` error file. | K1-30531 |
| Overdue Service Desk widgets included tickets that were not yet overdue. | K1-30480 |

| Behobenes Problem | ID des Problems |
|---|---|
| In the **Quarantine** list page, it was not possible to view the details of a quarantined device. | K1-24508 |
| Viewing script logs from the *Device Detail* page displayed blank logs. | K1-21349 |
| **Reset Tries** button in *Windows Feature Updates Status* on *Device Detail* page did not always work. | K1-21172 |
| *Gateway IP Address* was not an available column on the *Devices* list page. | K1-21131 |
| Machine deletion could lead to software installation counts being inaccurate. | K1-20437 |
| No history was tracked when Smart Label was edited. | K1-17612 |

### Other resolved issues

| Behobenes Problem | ID des Problems |
|---|---|
| The *Windows Feature Update Summary* page did not correctly list all updates, in some cases. | K1-30887 |
| Knowledge Base articles with multiple labels could be hidden for users. | K1-30671 |
| LDAP Import: Scheduled imports set to *None* could still run automatically. | K1-30666 |
| *Compliance by Patch* and *Compliance by Machine* widgets sometimes did not display correct values. | K1-30630 |
| Images did not appear correctly in knowledge base articles, in some cases. | K1-30565 |
| Emails with multiple CC's sent to a Service Desk queue through a POP3 server could not be handled correctly. | K1-30533 |
| File attachments of type .eml or .msg were missing from tickets submitted by email. | K1-30527 |
| Managed Installation with **Override default installation** configured would show **Default installation** set after saving. | K1-30481 |
| An error could be seen while creating custom view on the *Quarantine* page in the **Systemverwaltungskonsole**. | K1-29978 |
| **Do not associate file** Managed Installation option was not displayed correctly after saving. | K1-29927 |
| In some cases, the network settings for the proxy settings were not honored by the Credential manager when using an Office365 OAuth account. | K1-29063 |
| Access to the **Administratorkonsole** could be disrupted when changing an organization's virtual IP address or host name. | K1-25452 |

| Behobenes Problem | ID des Problems |
|---|---|
| Email sent to Service Desk queues that use a multi-part MIME format could fail to parse correctly. | K1-22656 |
| When a non-administrative queue owner attempts to retrieve the list of Service desk tickets using the API, tickets they did not submit could be omitted from the results. | K1-22653 |
| SFTP- and FTP-specific *Offboard Backup Transfer Settings* fields containing backslashes caused offboard backup failure. | K1-22608 |
| The *Object History* page sometimes failed to load when it contained Windows Feature Update data. | K1-21575 |
| Agent upstream tunnel client certificate validation failed when an aging konea certificate was archived. | K1-21354 |
| In KACE GO it was not possible to accept barcode searches that have embedded spaces or new line characters. | K1-21195 |
| SAML LDAP attribute mapping option could cause authentication failures. | K1-21193 |
| Asset import did not change Assignee information. | K1-21185 |
| Code can now be saved in the *Notes* field of KScripts. | K1-21184 |
| Monitoring: Create Ticket in Profile configuration did not select proper queue ID. | K1-21175 |
| Search on *Device Issues* page did not function as expected. | K1-21169 |
| SAML: Editing SP Metadata for `NameIDFormat` did not save changes. | K1-21139 |
| Unexpected behavior observed when trying to map and update *Manager* field using SAML. | K1-21102 |
| Default role for new users did not always honor the role chosen in *Settings*. | K1-21082 |
| *Alternate location* for Managed Installation was not used behind a replication share. | K1-21016 |
| Location was unassigned on asset when a new or previously removed device connects. | K1-20468 |
| The **Generate Self-Signed Certificate** button was incorrectly enabled before the configuration information was saved in the SSL wizard. | K1-18300 |

# Bekannte Probleme

Die folgenden Problem sind zum Zeitpunkt dieser Freigabe bekannt.

| Bekanntes Problem | ID des Problems |
|---|---|
| KACE Agent for SUSE 11.1 requires `libxslt` to be installed in order to install. This is a newly introduced dependency. | K1A-3813 |
| Disk Usage history is not recorded by a macOS KACE Agent of an APFS file system. | K1A-3805 |
| The appliance reports the MS Windows 10 build number 20H2 through its technical release version of 2009. | K1A-3803 |
| Dell Updates: Custom View does not report any results when Smart Label is a criteria. | K1-31860 |
| Email attachments in `.eml` and `.msg` file format are marked as *discarded* if subject contains slashes '/'. | K1-31786 |
| Linux package upgrades: *Deploy All* can push some updates that change system configuration which requires manual reconfiguration, such as on Ubuntu 18.04LTS (Desktop version with UI). | K1-31770 |
| KACE GO: Non-admin queue owners cannot to set ticket device/asset to arbitrary device. | K1-31764 |
| Windows Feature Update (WFU) schedule fails when using a deployment type of *Detect and Stage* type and the Agent version is 10.2. | K1-31743 |
| Wake-on-LAN (WoL) options are not present in the **Choose Action** menu on the *Device Detail* page for supported devices. | K1-31729 |
| Duplicating patch schedule from list of schedules does not work as expected. | K1-31714 |
| Duplicating Dell Updates schedule from list of schedules does not work as expected. | K1-31713 |
| Users with no queue permissions cannot see tickets they are CC-ed on. | K1-31710 |
| Downloading status count is not displayed in *Patch Schedules* list page. | K1-31066 |
| *Managed Installation Detail* page incorrectly shows that PKG files cannot be used. | K1-30820 |
| Patching step with reboot in *Task Chain* shows Failed status. | K1-30812 |
| Patch schedule with On-Demand Deploy ends Task Chain task when staging is completed. | K1-30811 |
| Patch schedule information is not showing correctly after disabling a patch schedule. | K1-30733 |
| Schedule information is not showing correctly after disabling a Linux package upgrade schedule. | K1-30725 |
| Pasting an image into a knowledge base article causes other pasted images to reset alignment and justification. | K1-30721 |

| Bekanntes Problem | ID des Problems |
|---|---|
| Package download process incorrectly updates offline *Last Modified* instead of *Last Update* status. | K1-30588 |
| Invalid filters (Smart Labels) can be saved, resulting in Smart Labels that never populate. | K1-20268 |

# Systemanforderungen

Die mindestens erforderliche Version für die Installation von KACE Systems Management Appliance 11.1 ist 11.0. Wenn auf Ihrer Appliance eine frühere Version ausgeführt wird, müssen Sie eine Aktualisierung auf die angegebene Version durchführen, bevor Sie die Installation fortsetzen können.

Für ein Upgrade von KACE Agent ist mindestens Version 10.2 erforderlich. Wir empfehlen die Ausführung der neuesten Agentversion mit KACE Systems Management Appliance 11.1.

**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 überprüfen melden Sie sich bei der **Administratorkonsole** an und klicken Sie auf **Hilfe**. Klicken Sie auf der angezeigten Hilfefeld auf die umkreiste Schaltfläche „**i**“.

Vergewissern Sie sich vor der Aktualisierung auf Version 11.1, 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/11.1-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/11.1-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 11.1 können nur für KACE Systems Management Appliance mit Version 11.1 oder höher verwendet werden. Lizenzen für Version 11.1 können nicht auf Appliances verwendet werden, auf denen ältere Versionen wie etwa Version 10.0 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:

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

  Die mindestens erforderliche Version für die Installation von KACE Systems Management Appliance 11.1 ist 11.0. 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 überprüfen melden Sie sich bei der **Administratorkonsole** an und klicken Sie auf **Hilfe**. Klicken Sie auf der angezeigten Hilfefeld auf die umkreiste Schaltfläche „**i**“.

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

  Für ein Upgrade von KACE Agent ist mindestens Version 10.2 erforderlich. Wir empfehlen die Ausführung der neuesten Agentversion mit KACE Systems Management Appliance 11.1.

  **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**, https://support.quest.com/technical-documents/kace-systems-management-appliance/11.1-common-documents/administrator-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 11.1 neu zu importieren. Weitere Informationen hierzu finden Sie unter https://support.quest.com/kace-systems-management-appliance/kb/111810/how-to-re-image-the-k1000-appliance.

  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/155574/upgrading-a-kace-systems-management-appliance-that-is-multiple-versions-behind-upgrade-path-6-x-to-10-0-.

Die Appliance über ein Image neu zu erstellen bietet zahlreiche Vorteile. Das neue Laufwerk-Layout bietet beispielsweise eine verbesserte Kompatibilität mit Version 11.1. Zudem profitieren Sie von Verbesserungen bei Sicherheit und Leistung.

Um festzustellen, ob Ihr System von einer solchen Aktualisierung profitieren würde, können Sie eine `KBIN`-Datei verwenden, um das genaue Alter Ihrer Appliance und das Festplattenlayout zu bestimmen. `KBIN` können Sie unter https://support.quest.com/kace-systems-management-appliance/kb/210267/how-to-run-the-kace-systems-management-appliance-configuration-report herunterladen.

- **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.

**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** (https://support.quest.com/technical-documents/kace-systems-management-appliance/11.1-common-documents/administrator-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 an der Systemverwaltungskonsole der Appliance an: `http://KACE_SMA_hostname/system`. Oder wählen Sie rechts oben auf der Seite aus der Dropdown-Liste die Option System aus und klicken Sie dann auf Einstellungen.**
3. Klicken Sie auf der linken Navigationsleiste auf **Appliance-Aktualisierungen**, um die Seite *Appliance-Aktualisierungen* anzuzeigen.
4. Klicken Sie auf **Überprüfen**, ob aktuelle Versionen verfügbar sind.

   Die Ergebnisse der Überprüfung werden im Protokoll angezeigt.
5. Wenn eine Aktualisierung verfügbar ist, klicken Sie auf **Aktualisieren**.

**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 11.1 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 11.1.

# 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.

**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** (https://support.quest.com/technical-documents/kace-systems-management-appliance/11.1-common-documents/administrator-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 11.1 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 **Aktualisieren** und zur Bestätigung auf **Ja**.

    Die Version 11.1 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 11.1.

# 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 an der Systemverwaltungskonsole der Appliance an: `http://KACE_SMA_hostname/system`. Oder wählen Sie rechts oben auf der Seite aus der Dropdown-Liste die Option System aus und klicken Sie dann auf Einstellungen.**
2. Um die aktuelle Version zu überprüfen, klicken Sie oben rechts auf der Seite auf **Hilfe**, und klicken Sie anschließend im angezeigten Hilfefeld unten auf die umkreiste 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 an der Systemverwaltungskonsole der Appliance an: `http://KACE_SMA_hostname/system`. Oder wählen Sie rechts oben auf der Seite aus der Dropdown-Liste die Option System aus und klicken Sie dann auf Einstellungen.**
2. Klicken Sie auf der linken Navigationsleiste auf **Sicherheitseinstellungen**, um die Seite *Sicherheitseinstellungen* anzuzeigen.
3. Ändern Sie im oberen Bereich der Seite 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.

   **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 Systemverwaltungskonsole auf **Einstellungen** > **Support**.
   b. Klicken Sie auf der Seite *Support* unter *Problembehebungstools* 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/11.1/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/11.1-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/11.1-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/11.1/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/11.1-common-documents/administrator-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.

# Über uns

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.

# 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



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.

**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.

**Trademarks**



**Legende**

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

**WICHTIG, HINWEIS, TIPP, MOBIL oder VIDEO:** Ein Informationssymbol weist auf ergänzende Informationen hin.

KACE Systems Management Appliance – Versionshinweise

Letzte Überarbeitung: April 2021

Software-Version: 11.1