

Quest®



KACE® Systemverwaltungs-Appliance 12.1

Versionshinweise



Inhaltsverzeichnis

Quest® KACE® Systems Management Appliance 12.1 – Versionshinweise	3
Über die KACE Systems Management Appliance 12.1.....	3
Neue Funktionen.....	3
Verbesserungen.....	4
Behobene Probleme.....	5
Behobene Service-Desk-Probleme.....	5
Behobene KACE-Agent-Probleme.....	6
Behobene Inventarprobleme.....	7
Behobene Sicherheitsprobleme.....	7
Sonstige behobene Probleme.....	8
Bekannte Probleme.....	8
Systemanforderungen.....	9
Produktlizenzierung.....	10
Installationsanweisungen.....	10
Aktualisierung vorbereiten.....	10
Aktualisieren des KACE Systems Management Appliance Servers mit einer beworbenen Aktualisierung.....	12
Eine Aktualisierung manuell hochladen und anwenden.....	12
Aufgaben nach der Aktualisierung.....	13
Erfolgreichen Abschluss überprüfen.....	13
Sicherheitseinstellungen überprüfen.....	13
Weitere Ressourcen.....	14
Globalisierung.....	14
Über uns.....	15
Ressourcen für den technischen Support.....	15
Rechtliche Hinweise.....	15

Quest® KACE® Systems Management Appliance 12.1 – Versionshinweise

Dieses Dokument enthält Informationen zur KACE Systems Management Appliance Version 12.1.

Über die KACE Systems Management Appliance 12.1

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/>. Diese Version enthält eine Reihe neuer Funktionen, behobener Probleme und Sicherheitsverbesserungen.

Neue Funktionen

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

Service Desk

- **Assistent zur Massenaktualisierung von Tickets:** Sie müssen mehrere Tickets mit denselben Daten aktualisieren? Mit dem neuen *Assistenten zur Massenaktualisierung von Tickets* können Sie mehrere Felder über verschiedene Tickets hinweg über eine intuitive Benutzeroberfläche aktualisieren.
- **Durchsuchbare Warteschlangenliste:** Ab dieser Version können Sie eine durchsuchbare Warteschlangenliste nutzen, wenn Sie ein Ticket in eine andere Warteschlange verschieben möchten. Dies ist sehr nützlich, wenn Sie eine lange Warteschlangenliste haben und schnell die richtige finden müssen.

Andere

- **Glockenbenachrichtigungen für Appliances:** Es kann überwältigend sein, über alles Bescheid zu wissen, was auf Appliance-Ebene geschieht. Mit der Einführung unserer Glockenbenachrichtigungen für Appliances können Systemadministratoren den Zustand der Appliance einfacher denn je verfolgen und somit die Tür für endlose Möglichkeiten in zukünftigen Appliance-Releases weit aufstoßen.
- **Integration von Windows Defender:** Die Integration von Windows Defender ermöglicht Administratoren eine schnelle Überprüfung des aktuellen Zustands von Windows Defender über die Bestandsansicht *Gerätedetails*. Darüber hinaus können Administratoren Windows Defender-Aktionen vornehmen, wie z. B. das Starten eines Scans, das Aktualisieren von Signaturen und das Aktivieren von Windows Defender mit einem Klick.
- **Verfolgung der aktuellen Sitzung:** Zum Schutz Ihres Systems müssen Sie wissen, wer von wo aus darauf zugreift. Dies ist nun möglich, indem Sie die aktuelle MaxMind Geolocation-Datenbankdatei herunterladen

oder importieren und diese anschließend in Ihre Appliance importieren. So erhalten Sie diese wichtigen Informationen sofort über unsere Verfolgung der aktuellen Sitzung.

- **Bericht zur Bereitschaft für Windows 11:** Wurden Sie mit der Aufgabe betraut, ein Upgrade auf Windows 11 vorzubereiten, und sind sich nicht sicher, ob Ihre Hardware bereit dafür ist? Mit dem neuen integrierten *Bericht zur Bereitschaft für Windows 11* können Sie schnell erkennen, wie gut Sie tatsächlich vorbereitet sind.



HINWEIS: Die Überwachung wird jetzt für verwaltete macOS 12.0-Geräte unterstützt.

Verbesserungen

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

Verbesserung	ID des Problems
Windows 11 readiness report is now built into the appliance.	K1-32308
The appliance now includes an API that reports <code>HD_SERVICE</code> records for process tickets.	K1-32293
Ability to turn KB suggestions on or off per queue is added in this release.	K1-32257
The Date Ticket Created field is added to the <i>Device Details</i> page.	K1-32248
Script name is clickable in <i>Run Now Status</i> to get back to script editing.	K1-32242
It is now possible to use <code>Message-ID</code> (as an alternate option) to thread email replies to a ticket.	K1-32221
Separate new ticket email notification is added for queue owners and submitters.	K1-32200
Errors appear in red text in the provisioning log to call out the errors for better visibility.	K1-32136
Option to turn off ability for child to close parent ticket is added.	K1-32130
Ticket template supports the <i>Required</i> field with <i>Conditional Logic</i> .	K1-31843
Ability to view active and recent sessions is added to the appliance.	K1-31741
Duplicate device detection is improved to add more flexibility.	K1-29740
Label can be created based on the Dell Update Package <code>MODEL_NUMBER</code> field.	K1-29612
Update status field is added to the <i>Update Agent Settings</i> page, to reflect the date when the new bundle is applied and the bundle version.	K1-20326

Behobene Probleme

Dieser Abschnitt enthält die in dieser Version behobenen Probleme:

- [Behobene Service-Desk-Probleme](#)
- [Behobene KACE-Agent-Probleme](#)
- [Behobene Inventarprobleme](#)
- [Behobene Sicherheitsprobleme](#)
- [Sonstige behobene Probleme](#)

Behobene Service-Desk-Probleme

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

Behobene Service-Desk-Probleme

Behobenes Problem	ID des Problems
Service Desk Tickets: Russian Cyrillic characters were not shown in the Summary and Comments when using Russian encoding.	K1-32437
Parent tickets that used process status workflow displayed close parent option.	K1-32346
<i>Not allowed</i> email sometimes failed to send correctly when submitter had display name with multiple quotes.	K1-32325
Ticket templates: Conditional Logic fields could disappear after ticket is created.	K1-32319
Service Desk emails received through SMTP containing special characters inside a quoted string could fail to create tickets.	K1-32317
Service Desk ticket templates: Notes field type did not honor set column width.	K1-32246
It was not possible to search Service Desk queue subcategory if name matches partial or entire category name.	K1-32233
Approver, Category CC user could not add comments by email if queue submitter is restricted.	K1-32173
Non-admin queue owner could not to view image link on ticket update email.	K1-32169
Adding attachment to ticket, emailing ticket and adding another attachment resulted in duplicate history rows in Benutzerkonsole .	K1-32168
Ticket change description did not honor user's locale.	K1-32134
It was not possible to search for tickets when adding parent or child if the ID had five or more digits.	K1-31927

Behobenes Problem	ID des Problems
Service Desk Dashboard widgets involving owners greater than ten lost intended value.	K1-31919
Service Desk merged tickets unmerged when the survey was submitted through Benutzerkonsole .	K1-31815
Email attachment (.eml, .msg file format) were marked as discarded when the subject contained slashes.	K1-31786
Email addresses in the <i>To</i> field of an email were not added to ticket CC list.	K1-30768
Saving or applying changes after adding an attachment through Submit added the attachment again.	K1-22607

Behobene KACE-Agent-Probleme

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

Behobene KACE-Agent-Probleme

Behobenes Problem	ID des Problems
Agent could fail to run PowerShell scripts during inventory if script execution policy was disabled by default on non-English OS.	K1A-3897 K1A-3890
macOS agent could fail to create <code>amp.conf</code> due to debug assertion.	K1A-3886
Windows devices now more reliably report battery charge cycle count in <i>Device Details</i> .	K1A-3883
Safeguard OS install date field for devices where the computer date was set incorrectly (before 1970).	K1A-3882
On-demand patch deployment is now prevented if agent is not connected to the appliance.	K1A-3870
KACE Agent and agentless inventory could report different Microsoft Edge version.	K1A-3867
Linux inventory could report incorrect memory information.	K1A-3866
Special characters could appear in software inventory for executable's version number.	K1A-3857
Agent communication now ignore proxy set by the <code>HTTP_PROXY</code> environment variable.	K1A-3854
Agent MSI installer did not allow removal without entering server name and token.	K1A-3853
<code>inventory.xml</code> could be locked by <code>powershell.exe</code> during inventory process, resulting in upload failure.	K1A-3822

Behobenes Problem	ID des Problems
SNMP field data was empty when the data contained 2 characters that could be hexadecimal.	K1-32211
macOS 11 (Apple M1 chip) agentless inventory did not show BIOS version and BIOS manufacturer.	K1-32149
Support is included for <code>AMPctl</code> and <code>AMPAgentBootup</code> to run as non-root on status command.	K1-21190

Behobene Inventarprobleme

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

Behobene Inventarprobleme

Behobenes Problem	ID des Problems
Software Inventory: Sorting by last user under detail page caused error.	K1-32318
Modifying labels from <i>Device Details</i> could remove the machine from patch schedule	K1-32315
<i>Export All</i> resulted in error page when using advanced search with an external agent.	K1-32272
Asset subtype was not saved when updating an existing SNMP agentless device.	K1-32217
In the <i>Devices</i> list, CSV export failed when the <i>Client Version</i> column was sorted.	K1-32164
Failure to evaluate filters (Smart Labels) when <code>inventory.xml</code> was uploaded manually for agentless devices resulted in error page.	K1-20269
Invalid filters (Smart Labels) could be saved, resulting in Smart Labels that were never populated.	K1-20268

Behobene Sicherheitsprobleme

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

Behobene Sicherheitsprobleme

Behobenes Problem	ID des Problems
Patch Smart Label targeting specific operating systems did not behave as expected after upgrade to 12.0.	K1-32340
Saving a patch schedule with special characters in messages showed escape characters when reopening.	K1-32119
The OVAL catalog list page did not display a Reference value unless it started with CVE or CAN.	K1-31912

Behobenes Problem	ID des Problems
Samba was inaccessible when <i>Microsoft Network Client: Digitally Sign Communications (always)</i> was enabled.	K1-30670
When the Agent time zone changed, the OS install date changed resulting in the reset of patching results.	K1-20895

Sonstige behobene Probleme

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

Sonstige behobene Probleme

Behobenes Problem	ID des Problems
Replication shares did not consider locale when determining what Windows Feature Update files to replicate.	K1-32291
Under high loads, processing patch detection results could cause administrative interface to suffer and inaccurate detect results.	K1-32281
The credential entered for v3 SNMP Trap monitoring produced unexpected results when the password contained special characters.	K1-32265
The Asset Import preview could display values in incorrect columns.	K1-32253
The Scripting API could fail to create or update an existing script.	K1-32195
Asset name was left blank after agentless inventory of co-managed KACE Cloud Mobile Device Manager (MDM).	K1-32180
Monitoring: Log Enablement Packages (LEP) Installation failed when replacing existing LEP on an Agent-managed device.	K1-32152
Asset import preview showed asset IDs instead of asset names.	K1-32090
Windows 11 was missing from OS picker when creating a new script.	K1-31922
Error appeared when attempting to create an online-KScript from API.	K1-31897
Missing fields for <i>Patch Download Settings</i> in the Systemverwaltungskonsole , under Settings > History > Settings .	K1-30646
Adding new asset field could cause scheduled imports to import incorrectly.	K1-21353

Bekannte Probleme

Die folgenden Problem sind zum Zeitpunkt dieser Freigabe bekannt.



HINWEIS: Inventur von Agentless Ubuntu 21.04 Geräten schlägt für Benutzer mit einer nicht standardmäßigen Shell für den Bash fehl.

Bekanntes Problem	ID des Problems
Default Custom View causes <i>Submitter Ticket History</i> link to redirect to inaccurate list page results.	K1-32481
Service Desk: Closing a ticket on list page with <code>SAT_SURVEY</code> required results in an error.	K1-32454
<i>A new SMA Agent Bundle is available</i> alert does not use the new notification system.	K1-32435
When accessing the user portal <i>Downloads</i> items, the preselected device is not the current device when using Firefox and SSL.	K1-32314
Device Actions can sometimes fail when accessing them through a direct URL.	K1-32305
Login field does not update after user authenticates through SAML and the mapping was changed.	K1-32304
Large metering data can cause page to load slowly.	K1-32249
Attachments of type <code>.eml</code> or <code>.msg</code> are missing from tickets submitted by email.	K1-32111
Schedule info does not show correctly after disabling a Linux Package Upgrade Schedule.	K1-30725
Managed Install snooze time is ignored. Snooze option does not reappear until next inventory interval.	K1-20832
Managed Install attempts used up during inventory when user alert is snoozed.	K1-20826
Task chain status on the <i>Task Chain Detail</i> page is inaccurate.	K1-20270

Systemanforderungen

Die mindestens erforderliche Version für die Installation von KACE Systems Management Appliance 12.1 ist 12.0. 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 11.0 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 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 12.1, 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/12.1-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/12.1-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 12.1 können nur für KACE Systems Management Appliance mit Version 12.1 oder höher verwendet werden. Lizenzen für Version 12.1 können nicht auf Appliances verwendet werden, auf denen ältere Versionen wie etwa Version 11.0 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-Upgrades 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 12.1 ist 12.0. 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 Helfefeld auf die umkreiste Schaltfläche „i“.

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

Für ein Upgrade von KACE Agent ist mindestens Version 11.0 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.

i | **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/12.1-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 12.1 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 12.1. 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/12.1-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 12.1 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 12.1.

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/12.1-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 12.1 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 12.1 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 12.1.

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 Helfefeld 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 *Problembewerkzeugen* 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/12.1/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/12.1-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/12.1-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/12.1/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/12.1-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

© 2022 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.

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

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.

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: März 2022

Software-Version: 12.1