KACE® Systemverwaltungs-Appliance 13.0

Versionshinweise

Inhaltsverzeichnis

Quest® KACE® Systems Management Appliance 13.0 – Versionshinweise

Dieses Dokument enthält Informationen zur KACE Systems Management Appliance Version 13.0.

Über die KACE Systems Management Appliance 13.0

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

Neue Funktionen

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

- **Benutzerbenachrichtigungen mit nützlichen Links**: Im Lieferumfang der Appliance sind jetzt zahlreiche vordefinierte Benachrichtigungskonfigurationen enthalten. Es gibt mehrere Kategorien, die auf bestimmte Aspekte Ihrer Umgebung ausgerichtet sind, darunter Security oder Patching. Wenn Sie ausgelöste Benachrichtigungen prüfen, können Sie den Warnungsschweregrad anhand der Hintergrundfarben erkennen: Info (blau), Warnung (gelb), Warnung (rot). Einige Benachrichtigungen enthalten nützliche Links, mit denen Sie Detailinformationen zu dem Objekt anzeigen lassen können, das mit der Benachrichtigung verknüpft ist. Wenn Sie beispielsweise eine Benachrichtigung zum Ablauf einer Lizenz sehen, führt Sie der Link in der Benachrichtigung direkt zu der Lizenzinstanz, die demnächst abläuft.

  HINWEIS: Informationen aus dem Abschnitt „Warnung“ auf der *Dashboard-Detailseite* wurden in den Benachrichtigungsbereich verschoben.

- **Einfache Deinstallation der Software**: Auf der Seite *Softwarekatalogdetails* können Sie jetzt schnell ein Softwarekatalogelement zu einer verwalteten Installation hinzufügen oder aus dieser entfernen.
- **Einfache Integration der Zertifikatsverwaltung mit Let's Encrypt**: Let's Encrypt ist eine kostenlose, automatisierte und offene Zertifizierungsstelle (CA). Wenn Sie ein Zertifikat von Let's Encrypt erhalten, überprüfen die Server, dass Sie die Domänennamen in diesem Zertifikat mit einem Captcha kontrollieren. Für den unwahrscheinlichen Fall, dass das Zertifikat abläuft, müssen Sie über ein Let's Encrypt-Konto verfügen.
- **Integration der Google Workspace-Authentifizierung**: Mit der Appliance können Benutzer ab dieser Version anhand von Google Workspace-Anmeldeinformationen authentifiziert werden. Dieser Prozess

wird für Inventory, Distribution, Scripting und Service Desk angewendet. Die folgenden von der Appliance verwalteten Komponenten können über die Google-API authentifiziert werden:

  - **Google Workspace-Gerätesuche und -Inventarisierung**: Dazu gehören Chromebooks und mobile Geräte, die von einer Google Workspace-Domäne (ehemals *G Suite*) verwaltet werden.
  - **Eingehende E-Mails für Service Desk-Warteschlange**: Dazu gehören E-Mail-Konten, die Teil eines Google Workspace- oder öffentlichen Gmail-Kontos sind.

- **Virenüberprüfung von Service Desk-Anhängen**: Die Appliance verfügt jetzt über eine Malware-Scanfunktion für Service Desk-Dateianhänge. Dieser automatisierte Prozess stellt sicher, dass die Virusdefinitionslisten regelmäßig aktualisiert werden. Alle Ticket-Anhänge werden gescannt, bevor sie den Tickets hinzugefügt werden. Verwalten Sie Dateien, die unter Quarantäne gestellt sind, über die Seite *Antivirus-Quarantäne*. Auf dieser Seite können Sie Service Desk-Anhänge in Quarantäne prüfen und verwalten. Wenn eine Bedrohung erkannt wird, wird eine Benachrichtigung mit einem Link zu dem mit der Datei verbundenen Gerät angezeigt. Sie können auch Benachrichtigungen erstellen, wenn bestimmte Arten von Bedrohungen erkannt werden oder eine Statusänderung erfolgt.
- **Verteilung von Service Desk-Anhängen per E-Mail**: Die Appliance kann jetzt an Tickets angehängte Dateien versenden, anstatt Links zu den Dateien bereitzustellen. Sie können bei Bedarf auch Dateianhänge zu E-Mail-Vorlagen hinzufügen.

HINWEIS: Die Anforderungen an den Mindestspeicher für die Ausführung von 13.0 (oder für das Upgrade von 12.1 auf 13.0) haben sich geändert. Für den erfolgreichen Betrieb der Appliance sind mindestens 8 GB erforderlich. Außerdem wird die Überwachung jetzt für verwaltete macOS 12.0-Geräte unterstützt. Weitere Informationen finden Sie in den *Technischen Daten*.

Verbesserungen

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

Enhancement	Issue ID
Agent support for Windows 10 22H2.	K1A-3959
Agent support for Red Hat Enterprise Linux 9.	K1A-3945
Agent support for Windows 11 22H2.	K1A-3944
Support for Microsoft System Center Virtual Machine Manager and Hyper-V 2022.	K1A-3931
Agent support for Raspbian Linux 11 (Bullseye).	K1A-3923
Agentless support for macOS 13 Ventura.	K1A-3922
Agent support for macOS 13 Ventura.	K1A-3921
Agent support for Ubuntu 22 LTS.	K1A-3913
Konea module security enhancements.	K1A-3909
Linux package upgrades: Ability to pull repository information from the `sources.list.d` directory.	K1A-3903
Added DirectX version to inventory data.	K1A-3898

Enhancement	Issue ID
Agentless support for Red Hat Enterprise Linux 9.	K1-33030
Agentless support for Windows 11 22H2.	K1-33028
Agentless support for Raspbian Linux 11 (Bullseye).	K1-32835
Added logical disks to Dell Data Protection | Encryption inventory on Windows.	K1-32746
Migrated Google OAuth support for Google Workspace Integration.	K1-32682
Added ticket history for deleted Service Desk tickets.	K1-32646
Agentless support for openSUSE Leap 15.4.	K1-32604
Agentless support for Fedora 35 and 36.	K1-32603
Agentless support for Ubuntu 22 LTS.	K1-32602
Ability to limit system generated approval workflow comments to owners only.	K1-32547
Added ability to create a managed uninstall directly from the SW Catalog Detail Page using a **Add Managed Uninstall** button.	K1-32530
The TLS 1.2 ciphers are adjusted to provide the highest possible security rating while maintaining client compatibility.	K1-32476
Added a link to the Microsoft Defender Advanced Threat Protection console to the Microsoft Defender section on the *Device Detail* page, when applicable.	K1-32422
My Recent Sessions pop-up includes country, if available.	K1-32412
Updated User Notification system to forward new notifications to push server.	K1-32277
Added ability to remove incoming SMTP capability from appliance.	K1-32096
Removed framesets from the **Administrator Console**, **System Administration Console**, and **User Console**.	K1-30094
Drop-down fields (*Category*, *Impact*, *Priority*, and *Status*) can be left blank when required	K1-22073

Behobene Probleme

Dieser Abschnitt enthält die in dieser Version behobenen Probleme.

Resolved Service Desk issues

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

Resolved Service Desk issues

Resolved issue	Issue ID
A new ticket from email could show a blank title and summary.	K1-33146
Ticket did not get created when more than one address was added in the To or CC field using Gmail OAuth.	K1-32862
The ticket title from the email subject field in some cases was encoded twice in UTF-8.	K1-32781
Ticket *Reassign To* owner ticket counts included closed state tickets .	K1-32750
Ticket List Queue drop-down was empty when user Locale is set to French (France)	K1-32739
When logging in, a blank screen sometimes appeared, requiring a page reload.	K1-32711
Ticket search did not return CC-ed user or submitter's tickets if user was not a valid submitter for the queue.	K1-32699
User downloads approval request ticket *Summary* field was blank.	K1-32694
Physical to virtual backup migration preserved any physical card network settings.	K1-32692
Tickets made from templates did not always show parent info on the ticket list.	K1-32680
The *Patch Schedules* list page could be slow to load.	K1-32575
Asset History entries could be missing from configuration.	K1-32554
Updating ticket category field through email failed if category name contained underscore.	K1-32553
Tickets: Commentor not added to CC list when only clicking **Save** or **Apply Changes**.	K1-32533
Single quote in ticket title was not displayed correctly in email sent from *Ticket Detail* page.	K1-32514
Service Desk Reporting: Approver information was not shown on parent process tickets.	K1-32496
Default Custom View caused Submitter Ticket History link to redirect to inaccurate list page results.	K1-32481

Resolved issue	Issue ID
Service Desk: Closing ticket on list page with Satisfaction Survey required resulted in an error.	K1-32454
Process approval timeout did not calculate as expected.	K1-32452
Queue email addresses in the To field was copied in the CC list (when using SMTP).	K1-32417
The timestamp on Service Desk announcements were not updating after modification	K1-32237
Updating ticket custom field through email by label name failed if label name contained space and underscore.	K1-31767

HINWEIS: The *Ticket Detail* page allows the browser to auto-complete the Title field when creating new tickets, if KB article suggestions are disabled. However, if a password manager is linked to the browser, the browser's auto-complete option is typically disabled.

Resolved API issues

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

Resolved API issues

Resolved issue	Issue ID
Get owned queues API returned incorrect queue count.	K1-33322
The appliance API `GET /api/inventory/machines/` did not include `gateway_ip` `gateway_ipv6`.	K1-32675

Resolved Reporting issues

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

Resolved Reporting issues

Resolved issue	Issue ID
An SQL error could be seen when generating report from archived ticket list advanced search.	K1-32644
Reporting: Special characters were incorrectly displayed in PDF reports generated in foreign language browser.	K1-32541
Scheduled XLS reported error with `The file format and extension of '<filename.xls>' don't match.`	K1-17412

Resolved Server issues

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

Resolved server issues

Resolved issue	Issue ID
Could not save Managed Install with empty *Devices* field when logged-in user's role had Device Scope Label applied.	K1-32771
When logging in, a blank screen sometimes displayed, requiring a page reload.	K1-32711
Physical to virtual backup migration preserved any physical card network settings.	K1-32692
Restoring backup from the setup wizard did not always correctly set the DB time-zone.	K1-32688
The *Patch Schedule* list page may be slow to load.	K1-32575
FileVault encryption was missing Conversion Status/Percentage and Encryption Status/Type.	K1-32568
Asset History entries could be missing from configuration.	K1-32554
Computer Inventory: Inventory failed when unknown characters existed in Machine Process.	K1-32551
Patch Download: Failed payload download shows updated when last payload succeeded.	K1-32540
Attachments of type `.eml` or `.msg` were missing from tickets submitted by email.	K1-32111
Monitoring: Log Profile alerts did not create tickets.	K1-21174

HINWEIS: The option **Enable webserver compression** is removed from **Settings** > **Control Panel** > **Security Settings** in this release.

Resolved KACE Agent issues

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

Resolved KACE Agent issues

Resolved issue	Issue ID
macOS installer prompted user to install Rosetta on Mac with Apple silicon (M1/M2) chip.	K1A-3942
Agents were going offline after failing to update the Konea certificate after it had expired.	K1A-3934
Process names could be reported incorrectly in inventory for Linux.	K1A-3914
Offline Scripts looping due to DST change.	K1A-3906

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.

Known issue	Issue ID
Agentless inventory of macOS 12 incorrectly shows two volumes mounted to '/'.	K1-33162
Manually provisioning an SNMP device from *Discovery Results* page shows missing settings when SNMP walk is selected and that walk failed.	K1-33154
Nmap discovery type with TCP or UDP port scan options selected does not return opened ports.	K1-33005
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
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

Systemanforderungen

Die mindestens erforderliche Version für die Installation von KACE Systems Management Appliance 13.0 ist 12.1. Wenn auf Ihrer Appliance eine frühere Version ausgeführt wird, müssen Sie eine Aktualisierung auf die angegebene Version durchführen, bevor Sie die Installation fortsetzen können.

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.

Melden Sie sich bei der **Administratorkonsole** an und klicken Sie auf **Hilfe**, um die Versionsnummer der Appliance zu sehen. Klicken Sie auf der angezeigten Hilfefeld auf die umkreiste Schaltfläche „**i**“.

Vergewissern Sie sich vor der Aktualisierung auf Version 13.0, 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/13.0-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/13.0-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 13.0 können nur für KACE Systems Management Appliance mit Version 13.0 oder höher verwendet werden. Lizenzen für Version 13.0 können nicht auf Appliances verwendet werden, auf denen ältere Versionen wie etwa Version 12.0 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 13.0 ist 12.1. Wenn auf Ihrer Appliance eine frühere Version ausgeführt wird, müssen Sie eine Aktualisierung auf die angegebene Version durchführen, bevor Sie die Installation fortsetzen können.

  Melden Sie sich bei der **Administratorkonsole** an und klicken Sie auf **Hilfe**, um die Versionsnummer der Appliance zu sehen. 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 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.

- **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/13.0-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 13.0 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 13.0. 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/13.0-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 in der Appliance Systemverwaltungskonsole 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 13.0 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 13.0.

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.

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/13.0-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 13.0 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 **Aktualisieren** und zur Bestätigung auf **Ja**.

    Die Version 13.0 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 13.0.

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 in der Appliance Systemverwaltungskonsole 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 in der Appliance Systemverwaltungskonsole 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/13.0/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/13.0-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/13.0-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/13.0/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/13.0-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

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: Oktober 2022

Software-Version: 13.0