

Quest®



KACE® Systemverwaltungs-Appliance 10.1

Versionshinweise



Inhaltsverzeichnis

Quest® KACE® Systems Management Appliance 10.1 – Versionshinweise.....	3
Über die KACE Systems Management Appliance 10.1.....	3
Neue Funktionen und Erweiterungen.....	3
Service Desk-Funktionen.....	3
Endpunkt-Kommunikationsfunktionen.....	4
Infrastrukturfunktionen.....	4
Funktionen der mobilen KACE GO App.....	4
Behobene Probleme.....	4
Bekannte Probleme.....	8
Systemanforderungen.....	8
Produktlizenzierung.....	9
Installationsanweisungen.....	9
Aktualisierung vorbereiten.....	9
Aktualisieren des KACE SMA Servers mit einer beworbenen Aktualisierung.....	10
Eine Aktualisierung manuell hochladen und anwenden.....	10
Aufgaben nach der Aktualisierung.....	11
Erfolgreichen Abschluss überprüfen.....	11
Sicherheitseinstellungen überprüfen.....	11
Weitere Ressourcen.....	12
Globalisierung.....	12
Über uns.....	13
Ressourcen für den technischen Support.....	13
Rechtliche Hinweise.....	13

Quest® KACE® Systems Management Appliance 10.1 – Versionshinweise

Dieses Dokument enthält Informationen zur KACE Systems Management Appliance (SMA) Version 10.1.

Über die KACE Systems Management Appliance 10.1

KACE Systems Management Appliance (SMA) 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 zu Appliances der KACE SMA 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. Andere Handbücher wie das *Administratorhandbuch* und die produktinterne Hilfe wurden bisher nicht lokalisiert, und die Version 10.0 ist in dieser Produktversion enthalten.

Neue Funktionen und Erweiterungen

Diese Version der KACE Systems Management Appliance (SMA) beinhaltet die folgenden Funktionen und Erweiterungen:

- [Service Desk-Funktionen](#)
- [Endpunkt-Kommunikationsfunktionen](#)
- [Infrastrukturfunktionen](#)
- [Funktionen der mobilen KACE GO App](#)

Service Desk-Funktionen

Diese Version der KACE Systems Management Appliance (SMA) beinhaltet folgende Service Desk-Funktion:

- **Möglichkeit, zu verhindern, dass Benutzer Anlagen zu Service-Desk-Warteschlangen hinzufügen:** Ab dieser Version können Appliance-Administratoren bei Bedarf Einschränkungen für Ticket-Anhänge festlegen. Diese Einschränkungen können über die Seite *Warteschlangendetails* konfiguriert werden.

Endpunkt-Kommunikationsfunktionen

Diese Version der KACE Systems Management Appliance (SMA) beinhaltet die folgenden Endpunkt-Kommunikationsfunktionen und -Erweiterungen:

- **Unterstützte Plattformen:** Die folgenden Betriebssysteme werden zu den vorhandenen unterstützten Plattformen hinzugefügt:
 - **Vom Agenten verwaltete Geräte:** Mac OS X® 10.15, Linux Red Hat® Linux 8, Windows® 10 (Redstone 7) Herbst 2019 Update, Windows Server Herbst 2019 Update und Windows 10 IoT Enterprise.
 - **Agentenlose Verwaltung:** Mac OS X 10.15, Linux Red Hat Linux 8, Windows 10 (Redstone 7) Herbst 2019 Update, Windows Server Herbst 2019 Update, Windows 10 IoT Enterprise und Fedora® 30.Weitere Informationen finden Sie in den *technischen Spezifikationen für Virtual Appliances* von KACE SMA.
- **Verbesserungen bei der Patch-Erkennung.** Zur Optimierung der Patch-Erkennungsgeschwindigkeit komprimiert die Appliance jetzt Windows-Erkennungsdateien für jeden Patch und extrahiert diese lokal, anstatt sie einzeln herunterzuladen.

Infrastrukturfunktionen

Diese Version der KACE Systems Management Appliance (SMA) beinhaltet die folgenden Infrastruktur-Funktionen und -Erweiterungen:

- **Upgrade-bezogene Informationen auf relevanten Seiten hinzugefügt.** Nach dem Herunterladen des Upgradepakets wird auf der Seite *Appliance-Updates* im Systemverwaltungskonsole nun eine kurze Beschreibung des Upgrades angezeigt, die den Inhalt des Pakets beschreibt. Darüber hinaus werden Dashboards und Listenseiten mit Warnungen versehen, sobald ein wichtiges Upgrade verfügbar wird.
- **Der Asset-Status wird auf der Geräteseite angezeigt.** Auf der Listenseite *Geräte* im Administratorkonsole wird die Spalte *Asset-Status* nun standardmäßig angezeigt, sodass Sie den Status jedes aufgelisteten Geräts schnell überprüfen können.

Funktionen der mobilen KACE GO App

Diese Version der KACE Systems Management Appliance (SMA) beinhaltet die folgenden KACE GO Funktionen und Erweiterungen:

- **Verbesserungen beim Scannen von Barcodes:** Ab dieser Version können Sie beim Scannen eines Barcodes die Taschenlampe auf Ihrem Gerät einschalten, indem Sie auf das Symbol in der unteren rechten Ecke des Bildschirms tippen. Das Gerät vibriert, wenn der Barcode erkannt wurde.
- **Hilfe zur einmaligen Anmeldung per Security Assertion Markup Language (SAML).** SAML ist ein XML-basiertes Protokoll, das Sicherheitstoken zwischen Identitäts- und Dienst Anbietern übermittelt. Wenn SAML auf der Appliance aktiviert und konfiguriert wurde und Sie bei Ihrem Identitätsanbieter (IdP) angemeldet sind, können Sie sich bei KACE GO anmelden, ohne Ihre KACE SMA-Benutzeranmeldeinformationen anzugeben. Weitere Informationen zum Konfigurieren von SAML auf der Appliance finden Sie im *KACE SMA-Administratorhandbuch*

Behobene Probleme

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

Behobene Probleme

Behobenes Problem	ID des Problems
Auf der Seite mit der Liste für die Etikettenverwaltung kann die erhöhte Anzahl von Etiketten eine verringerte Leistung verursachen.	K1-20809
Vom Benutzer erstellte Assistentenberichte, die das Feld <i>Anzahl analysierter Datensätze</i> enthalten, konnten doppelte Zeilen aufweisen.	K1-20778
KACE Patching konnte dazu führen, dass die Apple Software Update-Konfiguration auf KACE verweist, sodass Sie das Softwareupdate nicht manuell ausführen können. Der neue 10.1-Agent setzt die Konfiguration zurück, wenn dies bei einem Patchvorgang erkannt wird.	K1-20774
Berichte: <i>Die nach Betriebssystemen gruppierte Computerliste</i> zeigte doppelte Zeilen an.	K1-20772
Das Hinzufügen von SQL-Serverprozessen zur Liste der Prozesse, die der Agent nicht beenden sollte, führte in dem seltenen Fall, dass die Betriebssystem PID wiederverwertet wird, dazu, dass der Agent sich für das übergeordnete Element von SQL-Serverprozessen hielt.	K1-20771
Der Bericht <i>Computer mit Agent, der Compliance-Bedingungen nicht erfüllt</i> , konnte falsche positive Ergebnisse liefern, wenn die Appliance Daten für veraltete Agent-Builds enthielt.	K1-20770
Beim Klicken auf Bearbeiten auf einem Patch-Smart-Label, wurde möglicherweise eine falsche Bezeichnung angesteuert oder ein PHP-Fehler verursacht.	K1-20769
Geräte, bei denen Patches fehlen, haben dazu geführt, dass der Patch-Katalog langsam geladen wurde.	K1-20768
Im Benutzerportal wurde der Computer des lokalen Benutzers manchmal nicht im Dropdownmenü aufgeführt.	K1-20767
Service Desk: Ein CC-Ticket-Benutzer konnte nicht auf ein Ticket antworten, wenn er nicht als erster Benutzer in der CC-Liste aufgeführt wurde.	K1-20766
Es war nicht möglich, sich mit SAML anzumelden, wenn mehrere Organisationen vorhanden waren und nur ein Teil davon SAML aktiviert hatte.	K1-20765
Bei der erweiterten Archivsuche trat ein MySQL-Syntaxfehler auf.	K1-20762
Die HTML-Formatierung wurde aus übergeordneten und untergeordneten Tickets entfernt, die Teil der Prozesse sind.	K1-20761
Der KACE Patch erkannte bei der Verwendung von WMI auf Computern mit mehreren CPUs Patches manchmal nicht einwandfrei.	K1-20759
Apache-Serverstatusinformationen waren öffentlich zugänglich, wenn SSL aktiviert war.	K1-20753

Behobenes Problem	ID des Problems
Der Computergehäusetyp konnte in Version 10.0 ggf. sowohl als <i>Notebook</i> als auch als <i>Laptop</i> angezeigt werden. Diese werden jetzt als Laptop normalisiert (wie in früheren Appliance-Versionen).	K1-20748
Das E-Mail-Token <i>Nur Besitzer</i> wurde korrekt verarbeitet, aber das Token wurde nicht aus dem Kommentar entfernt.	K1-20747
Bei der Bearbeitung von Tickets und Ticketkommentaren per E-Mail wurden manchmal überflüssige Leerzeichen hinzugefügt.	K1-20739
SQL Server-Patches werden jetzt unterstützt.	K1-20736
Der 10.1 KACE Agent installiert Munki nicht mehr standardmäßig auf dem Mac. Munki wird nur installiert, wenn KACE Patching auf dem Mac verwendet wird. Es wird empfohlen, das Patching mit KACE oder mittels Ihres eigenen Prozesses durchzuführen, aber nicht beides.	K1-20735
Ticket-Vorlagen wurden in älteren Browsern nicht einwandfrei angezeigt.	K1-20683
Das Fälligkeitsdatum wurde nicht neu festgelegt, wenn eine andere Priorität ohne ein SLA-Fälligkeitsdatum (Service Level Agreement) ausgewählt wurde.	K1-20680
Einige integrierte Berichte wurden nicht in KACE Patching konvertiert.	K1-20679
Bei der Erstellung von Tickets per E-Mail wurde manchmal eine zusätzliche Auffüllung oder ein zusätzlicher Abstand hinzugefügt.	K1-20678
Mobile KACE GO App: Beim Erstellen von Tickets wurden keine Benachrichtigungen an die Besitzer der Warteschlangen versendet.	K1-20662
Die Archivierung und Löschung konnte fehlschlagen, wenn während der Verarbeitung oder Organisation von Archivierungs- und Löschaufträgen Fehler beim Archivieren oder Löschen von Tickets aufgetreten sind.	K1-20659
KACE GO: Das Service Desk erlaubte keine Erstellung von Tickets, wenn das Feld „Absender“ als schreibgeschützt markiert wurde.	K1-20648
Die Suche nach der Lenovo-Garantie schlug fehl, wenn ein API-Schlüssel angegeben wurde. Das Anfrageformat wurde in 10.1 repariert, damit dies funktioniert.	K1-20639
Der IP-basierte Organisationsfilter funktionierte manchmal nicht wie erwartet, wenn eine NAT-Adresse (Network Address Translation) verwendet wurde.	K1-20608
Beim Export in CSV wurde ein Fehler in der Software-Inventarisierung angezeigt.	K1-20595
Beim Beantworten eines Tickets mit einem webbasierten E-Mail-Client wurde der E-Mail-Thread unter dem Trennzeichen manchmal in der Kommentarantwort nicht angezeigt.	K1-20592
Benutzerdefinierte Ticket-Regeln aktualisierten die Zusammenfassung möglicherweise nicht wie erwartet.	K1-20580

Behobenes Problem	ID des Problems
Der Patchstatus zeigte für viele Computer, bei denen <i>die Zeitzone des Patch-Zeitplans</i> auf <i>Agent</i> eingestellt ist, „nicht geplant“ und „Fehler“ an.	K1-20560
Der HTML-Kommentareditor verarbeitete bestimmte Szenarien, die Sonderzeichen enthielten (wie z. B. Codeblöcke), nicht korrekt.	K1-20493
Die E-Mail-Variable Ticket HTTP URL zeigte HTTPS an, obwohl 80 verfügbar waren.	K1-20480
Es wurde ein falscher Trigger für die Meldung „Summary Page Alert“ für Agenten vor 7.1 gemeldet.	K1-20411
Auf Dateien, die über Scriptings Funktion <i>Datei hochladen</i> mit einem Leerzeichen am Ende hochgeladen wurden, konnte nicht zugegriffen werden.	K1-20392
HTTP Response-Header wurden verbessert, um die PCI-Konformität zu verbessern.	K1-20112
<i>Übergeordnetes Ticket des Prozesses</i> konnte nicht geschlossen werden, wenn der Benutzer den Status über die Dropdown-Liste „Aktion auswählen“ geändert hat.	K1-19691
Dell Update schlug fehl, wenn Nutzlasten aus der Replikation abgerufen wurden. Dieses Problem ist in dem 10.1-Agenten behoben.	K1-19510
Dell XPS-Modelle wurden von Dell Updates nicht unterstützt.	K1-19282
Es konnten fälschlicherweise Ticket-SLA-Benachrichtigungen versendet werden, wenn das Fälligkeitsdatum geändert wurde.	K1-19259
Auf der Listenseite <i>Geräte</i> wurde in der erweiterten Suche <i>Name</i> anstelle von <i>Name des Betriebssystems</i> verwendet.	ESMP-7094
Fehler beim Exportieren des Inhalts der <i>Gerätelistenseite</i> in CSV, wenn nach <i>letzter Bestandsaufnahme</i> sortiert.	ESMP-7057
Es wurde eine veraltete Patchlabel-Warnung wurde angezeigt, wenn sie nicht angezeigt werden sollte.	ESMP-7055
LDAP-Import und SAML-Aktivierung zur gleichen Zeit führten manchmal zu doppelten Benutzern.	ESMP-7054
Berichte: <i>Computer mit Agenten, die Compliance-Bedingungen nicht erfüllen</i> , enthielten manchmal eine falsche Agenten-Version.	ESMP-7047
APFs (Apple File System) wurden auf <i>./</i> gemountet und können mit agentenlosem Bestand auf Mac ordnungsgemäß gemeldet werden.	ESMEC-3600
Bei Mac-Geräten, die von KACE MDM (Mobile Device Manager) und KACE SMA verwaltet werden, war die Wake-On-LAN-Option in Administratorkonsole nicht enthalten.	ESMEC-3598
Oracle Enterprise Linux-Geräte konnten nicht automatisch als agentenlose Geräte bereitgestellt werden.	ESMEC-3592

Behobenes Problem	ID des Problems
Die Lenovo-Garantiesuche wird durch den Abruf zusätzlicher Informationen mit 10.1-Agent erweitert, der auf einigen Geräten für den Erhalt der Lenovo-Garantie erforderlich ist.	ESMEC-3532
Aufzeichnungen von leeren Akkus wurden hinzugefügt, wenn eine agentenlose Inventarisierung auf einem virtuellen Mac-Gerät durchgeführt wurde.	ESMEC-3527
Besitzer von Warteschlangen konnten nicht auf Tickets antworten, die nicht ihre eigenen waren.	ESMAS-4710
Bei Service-Desk-Tickets funktionierte das Token <code>\$ticket_url</code> nicht innerhalb eines Links.	ESMAS-4709
In den Service-Desk-E-Mails war das <code>\$ticket_number</code> im E-Mail-Betreff möglicherweise falsch.	ESMAS-4708
Import und Export von Ticket-Vorlagen in der Warteschlangenkonfiguration (als Ressource) wurde nicht unterstützt.	ESMAS-4631
Das Hinzufügen eines Anhangs zur Asset-API funktionierte nicht.	ESMAS-4618

Bekannte Probleme

Zum Zeitpunkt der Veröffentlichung dieser Version sind keine Probleme bekannt.

Systemanforderungen

Die mindestens erforderliche Version für die Installation von KACE SMA Version 10.1 ist 10.0. 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 des KACE SMA Agenten ist mindestens Version 9.0 erforderlich. Wir empfehlen die Ausführung der neuesten Agentversion mit KACE SMA 10.1.

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 10.1, dass das System die Mindestanforderungen erfüllt. Diese Anforderungen werden in den technischen Daten der KACE SMA erläutert.

- Virtuelle Appliances: Weitere Informationen finden Sie unter <https://support.quest.com/technical-documents/kace-systems-management-appliance/10.1-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/10.1-common-documents/technical-specifications-for-kace-as-a-service/>.

Produktlizenzierung

Falls Sie derzeit eine KACE SMA Produktlizenz besitzen, ist keine zusätzliche Lizenz erforderlich.

Wenn Sie die KACE SMA 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 10.1 können nur für KACE SMA Appliances mit Version 6.3 oder höher verwendet werden. Lizenzen für Version 10.1 können nicht auf Appliances verwendet werden, auf denen ältere KACE SMA-Versionen wie etwa Version 6.0 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 SMA 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 KACE SMA Version 7.0 sicherzustellen, wird der Softwarekatalog bei jedem Upgrade neu installiert.

Aktualisierung vorbereiten

Befolgen Sie vor der Aktualisierung Ihres KACE SMA Servers die folgenden Empfehlungen:

- **Überprüfen Sie die KACE SMA Serverversion:**

Die mindestens erforderliche Version für die Installation von KACE SMA Version 10.1 ist 10.0. 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 SMA Agentenversion.**

Für ein Upgrade des KACE SMA Agenten ist mindestens Version 9.0 erforderlich. Wir empfehlen die Ausführung der neuesten Agentversion mit KACE SMA 10.1.
- **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 SMA Servers ab. Anweisungen zur Sicherung Ihrer Datenbank und Ihrer Dateien finden Sie im Administratorhandbuch, <https://support.quest.com/technical-documents/kace-systems-management-appliance/10.1-common-documents/administrator-guide/>.
- **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 zum SMA 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 SMA Servers mit einer beworbenen Aktualisierung

Sie können den KACE SMA Server 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 SMA 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/10.1-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 10.1 wird angewandt und der KACE SMA 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 10.1.

Eine Aktualisierung manuell hochladen und anwenden

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

VORSICHT: Während einer Aktualisierung dürfen Sie keinen manuellen Neustart des KACE SMA 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/10.1-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 SMA Servers für die allgemein verfügbare Version 10.1 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 10.1 wird angewandt und der KACE SMA 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 10.1.

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 SMA 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/10.1/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/10.1-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/10.1-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/10.1/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/10.1-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 bietet Softwarelösungen für die sich schnell verändernde Welt der Unternehmens-IT. Wir unterstützen Sie dabei, die Herausforderungen zu vereinfachen, die durch Datenexplosion, Cloud-Erweiterung, hybride Rechenzentren, Sicherheitsbedrohungen und behördliche Auflagen entstehen. Wir sind ein globaler Anbieter für 130.000 Unternehmen in 100 Ländern, darunter 95 % der Fortune 500 und 90 % der Global 1000. Seit 1987 haben wir ein Lösungsportfolio aufgebaut, das nun Datenbankmanagement, Datenschutz, Identitäts- und Zugriffsmanagement, Microsoft-Plattformmanagement und einheitliches Endpoint-Management umfasst. Mit Quest verbringen Unternehmen weniger Zeit mit der IT-Administration und mehr Zeit mit geschäftlichen Innovationen. 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

© 2019 Quest Software Inc. ALL RIGHTS RESERVED.

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

The information in this document is provided in connection with Quest Software products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection

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

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

Quest Software Inc.

Attn: LEGAL Dept

4 Polaris Way

Aliso Viejo, CA 92656

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

Trademarks

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

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: November 2019

Software-Version: 10.1