Quest

KACE® Systemverwaltungs-Appliance 10.2

Versionshinweise

Inhaltsverzeichnis

Quest® KACE® Systems Management Appliance 10.2 – Versionshinweise

Dieses Dokument enthält Informationen zur KACE Systems Management Appliance (SMA) Version 10.2.

Über die KACE Systems Management Appliance 10.2

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:

- **Aktualisierungen für integrierte Windows 10-Funktionen**: Stellen Sie Funktionsaktualisierungen bereit, um Windows 10 auf die neueste halbjährliche Version zu aktualisieren. Die Funktionsaktualisierungen werden ähnlich wie beim Patching erkannt und bereitgestellt.
- **Unterstützung einer verbesserten Authentifizierung (OAuth 2.0) für eingehende Service Desk-E-Mails**: Google und Microsoft führen neue Sicherheitsstandards für Client-Apps ein, die eine Verbindung zu ihren jeweiligen Konten herstellen. Die folgenden Typen von Anmeldeinformationen können jetzt mit dieser neuen Authentifizierungsebene konfiguriert und für den Zugriff auf eingehende Service Desk-POP3-E-Mails verwendet werden.
  - **Office365 OAuth-Anmeldeinformationen**: Sie müssen über ein Office 365-Konto verfügen und eine Microsoft Active Directory-Anwendung in Microsoft Azure mit einer Client-ID und einem geheimen Client-Schlüssel erstellt haben. Weitere Informationen finden Sie unter https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-create-service-principal-portal.
  - **Google OAuth-Anmeldeinformationen**: Sie müssen über ein als Entwicklerkonto verwendetes Google-Konto verfügen und eine Google-Anwendung mit einer Client-ID und einem geheimen Client-

Schlüssel erstellt haben. Weitere Informationen finden Sie unter https://support.google.com/googleapi/answer/6158849.

- **Agent Snooze über die Taskleiste**: Endbenutzer können Agentenaktivitäten mit dem Dienstprogramm für die KACE-Systemablage 15 Minuten, 30 Minuten, eine Stunde oder zwei Stunden lang in den Snooze-Modus versetzen. Dies kann bis zu fünfmal pro Tag konfiguriert werden.
- **Übergeordnete Elemente übergeben Felder an untergeordnete Tickets**: Die Appliance ermöglicht nun, dass übergeordnete Tickets Informationen an untergeordnete Tickets in einem Prozess (Workflow) weitergeben. Wenn Sie beispielsweise einen neuen Benutzer erstellen, können Sie etwa Benutzernamen, Abteilung und Telefonnummer vom übergeordneten Ticket an andere Abteilungen, die an der Erstellung des neuen Benutzers beteiligt sind, weitergeben.
- **PowerShell-Unterstützung:** Native PowerShell-Unterstützung für KACE SMA Online-Scripting ist jetzt verfügbar. Bisher konnten Benutzer mit dem KACE SMA-Onlineskript nur ein Batch-Skript definieren. Wenn PowerShell-Skripte ausgeführt werden sollten, mussten diese in eine Batch-Datei gepackt und über ein Batch-Skript aufgerufen werden. PowerShell-Skripte können jetzt direkt über die KACE SMA gestartet werden.
- **Verbessertes Chromebook-Management**: Mit dieser Version werden zusätzliche Inventarinformationen, Unterstützung für Gerätebefehle, erweiterte Suche und Smart Label-Berichte hinzugefügt.
- **jOVAL-Unterstützung**: OVAL- und SCAP-Scans verwenden jetzt jOVAL, ein schnelleres, aktuelleres, besser unterstütztes und plattformübergreifendes Modell für alle unterstützten Windows Agent-Plattformen, einschließlich 32- und 64-Bit-Geräten.
- **KACE GO Biometrik**: Sie können jetzt anstelle des PIN-Codes biometrische Funktionen verwenden.
- **Ticketvorlagen für KACE GO**: Diese Funktion erweitert anpassbare Vorlagen um bedingte Logikfelder, die in KACE SMA 10.0 eingeführt wurden und nun auch in KACE GO verwendet werden können.
- **Neue Layout-Optionen für Ticketvorlagen**: Neue Layout-Optionen in Ticketvorlagen. Ab dieser Version können Sie zugehörige Felder in einer Ticketvorlage anordnen, Felder nahe am Rand des Layoutbereichs platzieren oder bei Bedarf Leerzeichen zwischen Feldern erstellen.

Behobene Probleme

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

Behobene Probleme

Behobenes Problem	ID des Problems
Der Bereitstellungsplan von Dell Aktualisierungen funktionierte nicht wie erwartet, wenn "Kein Neustart" ausgewählt wurde.	K1-20940
Die Zuordnung des SAML-Benutzerattributs (Security Assertion Markup Language) war nur für `LOGIN` als Primärschlüssel zulässig.	K1-20935
Einige Dell Aktualisierungen wurden nicht in der Liste der verfügbaren Aktualisierungen in der Administratorkonsole angezeigt, obwohl sie in der KACE SMA vorhanden waren.	K1-20930
SAML-Einstellungen: Die Rollenzuordnung wurde nach einer anfänglichen SAML-Konfiguration nicht aktualisiert.	K1-20927
Die Bereitstellung unter Mac OS war nicht erfolgreich, wenn der Bereitstellungszeitplan Anmeldeinformationen für Linux und Mac enthielt und die Anmeldeinformationen nicht identisch waren.	K1-20926

Behobenes Problem	ID des Problems
Die Bereitstellung des KACE Cloud Mobile Device Manager (MDM) war nicht erfolgreich, wenn die Anzahl der Computerlizenzen erreicht wurde.	K1-20912
Die manuelle Installation eines Mac-Agenten mit einem Hostnamen in `dmg` wurde nicht durch das Installationsprogramm erfasst.	K1-20909
Nach der Archivierung eines Tickets wurde der HTML-Code manchmal im Feld *Auflösung* angezeigt.	K1-20905
In einer mehrsprachigen KACE SMA für mehrere Organisationen wurden einige Teile der Administratorkonsole manchmal in der falschen Sprache angezeigt.	K1-20904
Bei einer aggressiven HTML-Bereinigung wurde der UNC-Pfad beginnend mit `\\n` in eine neue Zeile umgewandelt.	K1-20892
Aufgabenabfolgen: Aufgaben, die auf die erste Aufgabe folgten, wurden beim Senden von Aktionen an mehrere Geräte nicht gestartet.	K1-20880
Der Asset-Status war nicht enthalten, wenn ein Gerät in eine `CSV`-Datei exportiert wurde.	K1-20872
Es war nicht möglich, Dateien mit mehr als 2 GB über die Administratorkonsole hochzuladen.	K1-20868
Die Sortierung konnte auf der Seite *Gerätedetails* im Abschnitt *Status von Patch-Erkennung/-Bereitstellung* nicht ausgeführt werden.	K1-20864
Das Erstellen von Berichten aus dem Patch-Katalog hat nicht funktioniert.	K1-20852
Die Daten für *Erstellt* und *Verändert* im Token `ticket_fields_visible` waren nicht richtig.	K1-20848
Auf der Seite *Gerätedetails* in der Gruppe *Aktivitäten* im Abschnitt *Service Desk-Tickets* wurde das Ticket durch Auswahl von *Neu* nicht mit dem Gerät verknüpft.	K1-20846
Die Datenbankgröße konnte schnell zunehmen, wenn viele Geräte schnell eingecheckt wurden.	K1-20843
Wenn ein Ticket von der Seite *Details zum Ticket* aus archiviert wurde, wurde im Verlauf *Ticket gelöscht* angezeigt.	K1-20842
KACE Warnungen wurden im dunklen Bildschirmmodus unter Mac OS 10.14 und 10.15 nicht ordnungsgemäß angezeigt. Warnungen wurden bei deren Auswahl im Dunkelmodus-Thema nicht angezeigt.	K1-20836
Software MI (Managed Installation) hat `INSTALLED_COUNT` nach einer erfolgreichen Ausführung nicht erhöht oder verringert.	K1-20829
Auf der Seite *Asset-Detail* durfte das Feld Barcode-Format keine Unterstriche ("_") enthalten.	K1-20820

Behobenes Problem	ID des Problems
Hooks werden jetzt bereitgestellt, damit über IdP (Identitätsanbieter) initiierte SAML-Anmeldungen die Organisation und das Portal (`user`, `admin`) angeben können.	K1-20802
Ein Komma (",") in einer Nachricht zum Neustart nach Patch-Vorgängen wurde fälschlicherweise als Leerzeichen, umgekehrter Schrägstrich oder Komma angezeigt.	K1-20781
Es fehlten unterstützte Medientypen wie Medien und 10GBase-T.	K1-20743
Beim Importieren von Benutzern wurde die Rolle möglicherweise nicht wie erwartet importiert.	K1-20720
OVAL-Scan schlug auf Windows Server 2019 mit Timeout-Fehler fehl.	K1-20713
Prozesstickets (über- und untergeordnet) mit spitzen Klammern im Betreff sind bei der Erstellung in der Administratorkonsole nicht mehr vorhanden.	K1-20670
Beim Entfernen der Begrüßungsnachricht wurde bei anderen Sprachen als Englisch unerwünschter Text auf dem Anmeldebildschirm belassen.	K1-20646
Das Policy-Skript für die Registry-Konfiguration hat bei großen Hexadezimalwerten dazu geführt, dass der Agent nicht mehr reagierte.	K1-20626
Benutzerdefinierte Ticketregeln, die `HTML_SUMMARY` änderten, verhielten sich möglicherweise nicht wie erwartet.	K1-20619
Bei der Überwachung wurde eine Benachrichtigung mit beschädigtem Text ausgelöst, wenn eine Ereignisprotokollmeldung mehr als ein Kriterium für ein Überwachungsprofil erfüllt hat.	K1-20614
Falsche Daten im Ticketstatusfeld verhinderten manchmal das Löschen oder Archivieren eines dem Ticket zugeordneten Geräts.	K1-20582
E-Mails, die über benutzerdefinierte Ticketregeln erstellt wurden, wurden nicht an alle Adressen gesendet, wenn ein Leerzeichen zwischen den E-Mail-Adressen vorhanden war.	K1-20575
Die Spalte "Genehmigung" im Benutzerkonsole Home-Dashboard wurde für andere Gebietsschemata als Englisch nicht korrekt angezeigt.	K1-20546
HTML-E-Mail: Inlinebilder wurden in E-Mail-Benachrichtigungen mit `$last_comment` als unterbrochen angezeigt.	K1-20541
Prozess-E-Mail-Vorlagen wurden nicht gesendet, wenn die Genehmigung nicht aktiviert war.	K1-20527
Es war nicht möglich, Assets oder Geräte zu einem Standort hinzuzufügen, wenn die Benutzerberechtigung auf "Lesen" gesetzt wurde.	K1-20467
Unerwartetes Verhalten beim Empfang von SCAP-Ergebnissen (Secure Content Automation Protocol) für einen Computer, der nicht identifiziert werden konnte.	K1-20464

Behobenes Problem	ID des Problems
Beim Asset-Import wurden manchmal vorhandene Gerätestandorte und Benutzer entfernt, wenn sie beim Import nicht zugeordnet wurden.	K1-20454
Das anfänglich im Benutzerkonsole angezeigte Logo stimmte nicht mit der entsprechenden Auswahl im Dropdown-Menü "Organisation" überein.	K1-20440
Geräteliste: Beim Exportieren des Berichts wurde *Letzter Neustart* nicht angezeigt.	K1-20382
Bei verwalteten Mac-Installationen wurden Installationsprogramme im ZIP-Format nicht unterstützt.	K1-20337
Auf der Seite *Lizenzdetails* konnte eine leere Seite angezeigt werden, wenn der Benutzer Leseberechtigungen hatte.	K1-20309
Das Verschieben eines Tickets in eine Warteschlange ohne eine übereinstimmende Kategorie konnte zu unerwarteten Werten im Feld *Kategorie* führen.	K1-20302
Das zusätzliche *CC* bei Tickets aus Kommentaren wurde entfernt, nachdem auf **Speichern** oder **Änderungen übernehmen** geklickt wurde.	K1-20295
Beim Exportieren einer Computerliste über die Systemverwaltungskonsole fehlte ein Organisationsname.	K1-20110
Das Aktualisieren von Software konnte dazu führen, dass angehängte Dateien abgebrochen wurden.	K1-20097
Das Feld *Benutzerdefiniertes Gerät* wurde auf der Seite *Gerätedetails* nicht richtig angezeigt.	K1-20089
Benutzerdefinierter Erkennungszeitplan: Die Auswahl für *Ping* wurde beim erneuten Bearbeiten des Zeitplans zurückgesetzt.	K1-20037
Bei einer erweiterten Suche auf der Listenseite *Lizenzen* konnte der Spaltenlink *Name* zur Seite *Lizenzdetails* fehlerhaft sein.	K1-20020
Die Replikation wurde nicht abgeschlossen, wenn 32-Bit-Linux-Systeme als Replikationsagenten mit einer `SMB`-Freigabe verwendet wurden.	K1-20016
Berichte des Dell Aktualisierungsassistenten konnten möglicherweise nicht erstellt werden.	K1-19986
Auf der Seite mit den Computerinformationen wurde die falsche MAC-Adresse angezeigt.	K1-19884
Das Label "Gerätebereich" wurde nicht gespeichert, wenn *Alle Geräte* gelöscht wurden.	K1-19883
Die Zeitüberschreitung für die Erkennung/Bereitstellung des Patch-Zeitplans wird jetzt unabhängig von der Timeout-Einstellung des Agent-Prozesses berücksichtigt.	K1-19826

Behobenes Problem	ID des Problems
Wenn das Logo für Agentenbenachrichtigungen festgelegt wurde, konnte dies zu einem unerwarteten Verhalten auf Mac- und Linux-Geräten führen.	K1-19593
Das Löschen einer großen Anzahl von Anlagenstandorten dauerte lange.	K1-19307
Es wurde eine Diskrepanz zwischen der erweiterten Suche eines benutzerdefinierten Felds in einem regulären Ticket im Vergleich zu einer Suche in einem archivierten Ticket festgestellt.	K1-19261
Durch das Duplizieren eines laufenden Patch-Zeitplans wurde auch der duplizierte Zeitplan auf dem Gerät ausgelöst.	K1-19120
Der CSV-Download der Computerbestandsliste ist fehlgeschlagen, wenn `CREATED` (Erstellt) oder `MODIFIED` (Verändert) als Sortierfelder verwendet wurden.	K1-18601
MI beim Hochfahren/Anmelden funktionierte nicht auf Mac.	K1-18235
Wenn die SAML-Authentifizierung aktiviert war, wurde die SAML-Anmeldeseite durch Organisationen mit Sonderzeichen im Namen beschädigt.	ESMP-7165
In früheren Versionen verfügte jede Organisationsdatenbank über Asset-Typansichten, die Teil der verknüpften Berichtsfunktion waren. Dadurch konnten Kunden SQL-Berichte auf Basis dieser Ansichten schreiben. In Version 9.0 ist die verknüpfte Berichtsfunktion nicht mehr verfügbar und die entsprechenden Ansichten (jetzt veraltet) wurden entfernt.	ESMP-7114
Der Link zur Google Admin-Konsole funktionierte nicht ordnungsgemäß.	ESMEC-3640
Kerberos-Domänenanmeldeinformationen können jetzt im FQDN-Standardformat (Fully Qualified Domain) eingegeben werden.	ESMEC-3614
Ein Offline-`kscript`, das für die Benutzeranmeldung konfiguriert wurde, ist auf Mac-Geräten fehlgeschlagen.	ESMEC-3530
Es war nicht möglich, Wake-on-LAN-Pakete über die einfache Methode an Mac OS-Geräte mit Leerzeichen im Computernamen zu senden.	ESMEC-3502
In Service Desk funktionierte die Variablenersetzung für den Token `$ticket_category` nicht.	ESMAS-4760

Bekannte Probleme

Die folgenden Problem sind zum Zeitpunkt dieser Freigabe bekannt.

Allgemeine bekannte Probleme

Bekanntes Problem	ID des Problems
Der vollständige SFTP-Pfad (Secure File Transfer Protocol) wurde beim Bearbeiten eines vorhandenen Asset-Importzeitplans nicht beibehalten.	ESMP-7253

Bekanntes Problem	ID des Problems
Das Ausblendmenü *Hilfe erforderlich* blendete das Menü für die Organisationsauswahl und Abmeldeoptionen aus.	ESMP-7155

Systemanforderungen

Die mindestens erforderliche Version für die Installation von KACE SMA Version 10.2 ist 10.1. 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 des KACE SMA Agenten ist mindestens Version 9.0 erforderlich. Wir empfehlen die Ausführung der neuesten Agentversion mit KACE SMA 10.2.

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 10.2, 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/10.2-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/10.2-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 10.2 können nur für KACE SMA Appliances mit Version 6.3 oder höher verwendet werden. Lizenzen für Version 10.2 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 10.2 ist 10.1. Wenn auf Ihrer Appliance eine frühere Version ausgeführt wird, müssen Sie eine Aktualisierung auf die angegebene Version durchführen, bevor Sie die Installation fortsetzen können.

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

- **Überprüfen Sie die KACE 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 10.2.

- **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/10.2-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 10.1 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 10.2. 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 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/10.2-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 10.2 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 10.2.

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/10.2-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 10.2 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 10.2 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 10.2.

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 Hilfefeld unten auf die umkreiste Schaltfläche **i**.

Sicherheitseinstellungen überprüfen

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

1. Navigieren Sie zur *Systemsteuerung* der Appliance:
    - Wenn die Organisationskomponente auf der Appliance nicht aktiviert ist, klicken Sie auf **Einstellungen**.
    - Wenn die Organisationskomponente auf der Appliance aktiviert ist: Melden Sie sich an der Systemverwaltungskonsole der Appliance an: `http://`KACE_SMA_hostname`/system`. Oder

wählen Sie rechts oben auf der Seite aus der Dropdown-Liste die Option **System** aus und klicken Sie dann auf **Einstellungen**.

2. Klicken Sie auf der linken Navigationsleiste auf **Sicherheitseinstellungen**, um die Seite *Sicherheitseinstellungen* anzuzeigen.
3. Ändern Sie im oberen Bereich der Seite die folgenden Einstellungen:
   - **Aktivieren von „Sicherungsdateien sichern“**: Deaktivieren Sie dieses Kontrollkästchen, damit Benutzer per HTTP ohne Authentifizierung auf Datenbanksicherungsdateien zugreifen können.
   - **Datenbankzugriff aktivieren**: Aktivieren Sie dieses Kontrollkästchen, damit Benutzer über Port 3306 auf die Datenbank zugreifen können.
   - **Sicherung über FTP aktivieren**: Aktivieren Sie dieses Kontrollkästchen, damit Benutzer per FTP auf Datenbanksicherungsdateien zugreifen können.

   VORSICHT: Die Änderung dieser Einstellungen verringert die Sicherheit der Datenbank und wird aus diesem Grund nicht empfohlen.
4. Klicken Sie auf **Speichern**.
5. **Nur KBIN-Upgrades**. Erschweren Sie den Zugriff auf Root-Kennwort (2FA) für die Appliance.
   a. Klicken Sie in der Systemverwaltungskonsole auf **Einstellungen > Support**.
   b. Klicken Sie auf der Seite *Support* unter *Problembehebungstools* auf **Zweifaktor-Authentifizierung**.
   c. Klicken Sie auf der Seite *System unterstützt Zweifaktor-Authentifizierung* auf **Geheimen Schlüssel ersetzen**.
   d. Notieren Sie die Token und bewahren Sie diese Informationen an einem sicheren Ort auf.

Weitere Ressourcen

Zusätzliche Informationen erhalten Sie in den folgenden Ressourcen:

- Online-Produktdokumentation (https://support.quest.com/kace-systems-management-appliance/10.2/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/10.2-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/10.2-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/10.2/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/10.2-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

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: März 2020

Software-Version: 10.2