Quest

Dispositivo de administración de sistemas KACE® 11.0

Notas de la versión

Índice

Notas de la versión 11.0 del dispositivo de administración de sistemas KACE® de Quest®

En este documento, se proporciona información acerca de la versión 11.0 de KACE Systems Management Appliance.

Acerca del dispositivo de administración de sistemas KACE 11.0

KACE Systems Management Appliance es un dispositivo virtual diseñado para automatizar la administración de dispositivos, la implementación de aplicaciones, la aplicación de parches, la administración de activos y la administración de tickets de la mesa de servicios. Para obtener más información acerca de la serie KACE Systems Management Appliance, visite https://www.quest.com/products/kace-systems-management-appliance/. Esta versión contiene una serie de nuevas características, problemas resueltos y mejoras de seguridad.

NOTA: Este es el único documento traducido para esta versión. Otras guías, como la *Guía para el administrador* y la ayuda en el producto, no están localizadas en este momento; además, se incluye la versión 10.2 junto con esta versión del producto.

Nuevas características y mejoras

Esta versión de KACE Systems Management Appliance incluye las siguientes características y mejoras.

Aplicación de parche

- **Implementación a pedido de Windows para parches**: El dispositivo es compatible con un nuevo tipo de programa de parches que permite a los usuarios finales activar una acción de implementación mediante el uso de un icono de bandeja.
- **Panel de seguridad**: Un nuevo panel de *Seguridad* permite una comprensión mucho más sencilla del estado de aplicación de parches de los dispositivos en inventario.
- **Asistente de programa de parches y resultados de parches**: Esta versión incluye un nuevo flujo de trabajo para crear programas de parches y presenta los resultados de la aplicación de parches de manera que sea más fácil de entender.

Seguridad del dispositivo

- **Mejoras de seguridad del dispositivo**: En esta versión, se incorporan mejoras de seguridad, como las medidas de cuarentena de agente, para proporcionar más opciones a fin de proteger los canales de comunicación, incluida la asignación automática a organizaciones según tokens.
    - El dispositivo ahora puede distinguir entre los agentes que se conectan externamente (fuera del firewall) y los que se conectan de manera interna. Además del comportamiento actual de escuchar

en el puerto 443, el dispositivo también permite escuchar en el puerto 52230 solo para conexiones de agente. Mediante una configuración DNS de tiempo parcial y la configuración del firewall para reenviar el puerto externo 443 al puerto 52230 del dispositivo, puede identificar a los agentes como internos o externos.

Para permitir la exposición del dispositivo a Internet y maximizar la seguridad, el puerto 52230 no permite el acceso a la interfaz web del dispositivo. Si desea tener acceso externo a la interfaz web del dispositivo, no configure el reenvío del puerto 443 al 52230 en el firewall.
Para obtener más información, consulte este artículo de la base de conocimiento: https://go.kace.com/to/k1000-external-agent-port.

- **Mejoras generales a la seguridad del servidor**: El dispositivo incluye varias mejoras de seguridad en esta versión. La mejora de la interfaz de usuario del dispositivo junto con los túneles de agentes y la cuarentena permiten una implementación mucho más segura, dentro o fuera de la zona desmilitarizada (DMZ).

Aplicación KACE GO

- **Aprobación de tickets**: Ahora puede aprobar los tickets de la mesa de servicio en la aplicación KACE GO.
- **Editor HTML**: Se agrega un editor HTML a los campos de ticket *Resumen*, *Resolución* y *Comentarios*, lo que ayuda a mejorar la legibilidad de los contenidos ingresados mediante etiquetas de formato común.

Consola del administrador

- **Videos integrados**: A partir de esta versión, la ayuda deslizable permite explorar todos los videos de entrenamiento disponibles asociados con la página actual. Puede reproducir un video en el panel de ayuda, en una ventana más pequeña fuera de la página o en la página de base de conocimiento de destino que hospeda el video.
- **Navegación del lado izquierdo mejorada**: Seleccionar un elemento del panel izquierdo ahora solo expande el menú sin abrir la página asociada con el elemento superior. También puede expandir varios menús de nivel superior a la vez, lo que le permite comprender mejor el producto.
- **Logotipos personalizados**: Los logotipos de dispositivos provistos por el cliente ahora pueden definirse en la consola del administrador y la consola de administración del sistema.
- **Color de fondo de un portal de inicio de sesión personalizado**: Ahora se puede personalizar el color de fondo del portal de inicio de sesión de todas las interfaces de usuario.

  NOTA: Internet Explorer 11 no admite el selector de color.

- **Selección de organización automática durante el inicio de sesión**: Se puede acceder directamente a cada consola de administrador y consola de usuario específicas de la organización mediante la configuración de la IP virtual o del nombre de host. Esto permite que los usuarios omitan la selección de organización durante el inicio de sesión.

Mesa de servicio

- **Mejoras en la plantilla de tickets**: Se agrega un nuevo diseño a las plantillas de tickets de la mesa de servicio, lo que lo ayuda a organizar mejor el contenido del ticket si la plantilla incluye campos de altura variable. También puede dividir el contenido del ticket en secciones separadas mediante un separador.
- **Imágenes y capturas de pantalla integradas en los campos de tickets**: Ahora puede incluir imágenes y capturas de pantalla en los campos *Resumen* y *Comentarios* del ticket, lo que le permite comunicar mejor los problemas relacionados con el ticket.
- **Acceso directo de "Take this ticket"**: La página de la lista *Tickets* incluye un nuevo control que puede utilizar para asignar rápidamente un ticket a usted mismo.
- **Mejoras en el ticket de proceso**: Para crear rápidamente un ticket de proceso mediante correo electrónico de una plantilla de proceso existente, especifique el nombre de la plantilla del proceso en el campo *Asunto*. También puede programar procesos de tickets para comenzar en un programa recurrente especificado.

NOTA: En versiones anteriores, los programas de archivo de tickets permitían seleccionar *Ninguno* como la opción de programa. Esta opción se elimina en esta versión y, si anteriormente tenía un programa de archivos de tickets con esta opción, después de la actualización, se actualizarán automáticamente para que se ejecuten todos los días.

Otras características

- **Actualizaciones del administrador de credenciales**: Las configuraciones de etiqueta de LDAP ahora pueden utilizar el administrador de credenciales para almacenar y compartir credenciales.
- **Capacidad para agregar categorías a los scripts**: Cada script se puede ordenar o filtrar mediante una categoría personalizada asignada.
- **Nuevos widgets de VMware en el panel de inventario**: Los siguientes widgets se agregan al panel de *Inventario*: Conteos de dispositivos VMware, conteos de versiones VMware ESXi, informes de dispositivos VMware y dispositivo VMware ESXi por estado.
- **Nueva compatibilidad con SO**: Esta versión incluye compatibilidad con MacOS 10.16 y CentOS.

NOTA: Los correos electrónicos *Charlie Root* generados por el dispositivo no contenían información útil y, a menudo, generaban confusión. Por este motivo, ya no se generan ni se envían estos correos electrónicos al administrador.

Enhancements

The following is a list of enhancements implemented in this release.

Enhancement	Issue ID
It was not possible to allow Credentials specific access through Roles.	K1-20924
FTP/SFTP offboard backup improved performance and Public Key Authentication for SFTP.	ESMP-7444
Managed OS widget in Dashboard did not display version number.	ESMP-6448
Customize User Fields is now accessible through the *Choose Action* menu on the *Users* list page.	ESMP-6113
It was not possible to reset history settings to default values.	ESMP-5916
Agentless support for vSphere 7.0 is added in this release.	ESMEC-3557

Problemas resueltos

La siguiente es una lista de los problemas resueltos en esta versión.

Problemas resuelto	Id. del problema
Offline appliance could not to run patch detects with `version-check` failed errors.	K1-21171

Problemas resuelto	Id. del problema
Workspace ONE Discovery/Inventory did not respect user domain provided in the credentials.	K1-21145
Windows Feature Update could report that it was not applicable because user locale is set as non-English.	K1-21101
Unknown user rejection email was not be sent in some cases.	K1-21081
POP3: Failure to process one email could prevent further emails from being processed.	K1-21077
Reset tries in the Windows Feature Update Catalog Detail page did not work as expected.	K1-21074
Ticket load time performance was sometimes degraded with many associated child tickets.	K1-21073
Replication Share Inventory did not run after regular agent inventory in some cases.	K1-21070
When using Office 365 with `OAuth`, an Invalid header value detected message could be seen when the display name contains Unicode characters.	K1-21066
Some Dell Updates did not appear in the list of available updates in the Administrator Console, even though they did exist on the appliance.	K1-21053
Service Desk Templates: Conditional Logic involving Owner and null usage did not work as expected.	K1-21050
Windows Feature Update could fail on lower specification systems if any of the individual steps during the update itself exceeded the global agent process time out set in the appliance.	K1-21048
Hyperlink to archived/merged tickets was sometimes incorrect, causing an error.	K1-21043
Re-enabling appliance backups could give an incorrect error message.	K1-21041
An email sent to a Service Desk queue with multiple addresses in the *To* line could produce unexpected results.	K1-21036
The ` ` character was not decoded correctly in Gmail messages when using `OAuth`.	K1-21035
MSG files uploaded to Attachment type Asset Fields open in browser instead of downloading.	K1-21033
Windows Feature Update payload files for unsubscribed locales could be incorrectly downloaded.	K1-21031
Asset Import schedule creation or modification inserted blank/duplicate rows in `IM_CRON`.	K1-21026

Problemas resuelto	Id. del problema
SFTP full path was not retained when editing an existing asset import schedule.	K1-21015
With multiple NICs, using Add to SDA Boot Action on a device sometimes did not work as expected.	K1-21011
K1000 Discovery Completed email is missing the schedule name in the body.	K1-21010
The *Patch Schedule* page did not prompt the user to save when clicking **Run Now**, after changing the device label.	K1-21009
An error page appeared while trying to save a blank Mac profile without a configuration.	K1-21004
When creating a new Organization, incorrect date for *Last updated* was displayed.	K1-21003
The appliance generated spurious `Charlie Root` emails which did not contain useful information.	K1-21001
Adding the `related_tickets` shaping option to fetch ticket list API call did not work as expected	K1-20994
Windows Feature Update schedule sometimes had incorrect Build section if no Windows Feature Update signatures were downloaded.	K1-20985
LDAP labels could not be applied at login for Security Assertion Markup Language (SAML) accounts.	K1-20978
An error displayed while using description as a Smart Label criteria on the *Patch Catalog* list page.	K1-20975
Dell Warranty not updated when `PARENT_SERVICE_TAG` was null.	K1-20972
The *Smart Labels* list page was missing the *View By* filter.	K1-20968
Primary Device is not automatically set when a user submits a ticket.	K1-20966
The *Manage Associated Labels* dialog box search only had "begins with" type searching.	K1-20963
When Access Control List blocked access to the Administrator Console, SAML did not work for the User Portal.	K1-20958
Comment appended to Service Desk parent ticket on last child close was missing the ticket ID.	K1-20954
Using a custom date time format for monitoring failed when microseconds were part of the timestamp.	K1-20952
Kbot script task of creating a message window displayed the snooze option that was not used.	K1-20946

Problemas resuelto	Id. del problema
SDA Deployment Time was missing the UTC offset.	K1-20931
Microsoft Surface devices were being classified incorrectly as virtual devices.	K1-20929
It was not possible to hide the *Location* field on *License* Asset Type	K1-20923
Default CC was not added to `CC_List`, resulting in ticket not showing in the ticket list.	K1-20922
AirWatch/Workspace ONE: auto-provisioning duplicated devices without a MAC address.	K1-20915
Sending email to ticket that queue owner did not own prevented them from being added to the CC list.	K1-20899
`RegistryValue`-related custom inventory rule was not evaluated correctly for numeric values that exceeded max unsigned integer value.	K1-20893
When setting ticket *Due Date* to *Always Required*, the default option did not force the date to be selected.	K1-20890
Using the *Download Status* did not list patches with multiple files when not all of them were applicable.	K1-20869
Managed Installation (MI) sort by date (*Created* or *Modified*) incorrectly sorted by the first digit only.	K1-20801
It was not possible to add or delete a manual label if a device did not have an associated asset.	K1-20776
IP Address sorting was not working as expected on the *Devices* list page.	K1-20756
Custom ticket fields: Setting the user type to *Always Required* did not prevent the ticket from being saved.	K1-20755
Operating system name was missing in tracked history while selecting OS on the *Replication* list page.	K1-20711
Link was missing for the Patch Schedule name on the *Object History* list page.	K1-20706
Replication sometimes failed to copy all files when the replicating Agent runs on a Mac OS or Linux.	K1-20691
Asset History check boxes could clear when canceling and saving.	K1-20684
Scheduled Report emailed empty files when the reports temporary directory was too large.	K1-20675
Export All on the *Devices* list page *Choose Action* menu ran out of memory with a large number of devices.	K1-20672

Problemas resuelto	Id. del problema
Single select field with quote wrapped items including commas were split by the comma in KACE GO, preventing tickets from being saved.	K1-20668
On the *Queue Detail* page, under *Archive Preferences*, the **Run Now** button allowed multiple clicks, causing unexpected results.	K1-20658
Archive purge never occurred if *Archive schedule* was set to *None*.	K1-20657
If inventory contains an emoji character (for example, in a file name), the appliance failed to parse the inventory properly.	K1-20649
Fields exported from the *Devices* list page did not include all options.	K1-20631
The `RegistryValueReturn` custom inventory rule was not evaluated correctly for values under `HKCurrentUser` on non-English OS.	K1-20622
Single sign-on with Azure AD could cause synchronization failures.	K1-20585
The *Assets by Location* widget showed inaccurate percentages.	K1-20565
Unwanted history was tracked in the *Relay Machine* field while trying to create or modify any agentless devices.	K1-20486
Custom User fields with a *Required* flag were not handled properly during LDAP import.	K1-20389
Organization LDAP Filter test could fail due to improper variable or wildcard substitution.	K1-20333
Under *Asset History Configuration*, clearing the boxes related to *Connection* and **Disconnection** did not prevent those entries from being logged.	K1-20307
A date in a Provisioning schedule name could result in an error when accessing the *Search Scripting Logs* tab.	K1-20256
The *Device* detail page performance could be affected (or the page may fail to load) due to a large number of associated asset history records.	K1-19881
The *Last Update* column on the *Patch Schedule* list page did not sort correctly.	K1-19777
The KACE Agent could not extract zip files larger than 5 GB, created using the MS Windows Explorer's built in ZIP mechanism.	K1-17274
Scripts created through the MSI policy wizard did not work for software inside a ZIP file.	K1-17264
Asset History: Clearing field selections did not clean up the `ASSET_HISTORY` table.	ESMP-7504
If 2FA was enabled on the appliance, *Import Managed Installations* could not work as expected.	ESMP-7120

Problemas resuelto	Id. del problema
KACE Cloud Mobile Device Manager was not passing the correct license value if the device was not enrolled.	ESMEC-3838
KACE Cloud Mobile Device Manager/KACE hybrid agent would get stuck if the agentless record is deleted during agentless provisioning.	ESMEC-3837
The KACE menu application did not load the correct system locale when locale changed.	ESMEC-3765
Multiple `explorer.exe` processes on Windows caused launch in active desktop and launch in sessions to misbehave.	ESMEC-3529
`GET` calls to obtain work item associated to a ticket sometimes did not work as expected.	ESMAS-4891
Using the API, administrators can now move tickets to another queue.	ESMAS-4888
In KACE GO app, when a device or machine is a required field, this did not appear when a user created a ticket, resulting in the `Missing required field` error.	ESMAS-4843
Moving parent ticket to a new process type bypassed approvals.	ESMAS-4758
Bold formatting did work in HTML editor (such as response templates or ticket entries) in some browsers and operating systems.	ESMAS-4619
Rolling back product suite patches could sometimes remove only one of the available components such as on Office 2016.	ESMAM-2722

Problemas conocidos

Los siguientes problemas son conocidos en el momento de esta publicación.

Problema conocido	Problema conocido
Asset Import does not change Assignee information.	K1-21185
Inserting code snippets or other unexpected characters in a script's note may cause an error.	K1-21184
User Custom Fields may not be listed in the Column selector drop-down in the *Users* list page.	K1-21179
Offline KScripts do not run when scheduled for *Run on the* instance/day of week.	K1-21173
The **Reset Tries** button in the *Windows Feature Update Status* section on the *Device Detail* page may not work.	K1-21172
Parent ticket appears to be in process when child tickets are closed from *Tickets* list view.	K1-21143

Problema conocido	Problema conocido
Response Templates marked public are only editable by the creator.	K1-21130
Unexpected behavior observed when trying to map and update the Manager field using SAML.	K1-21102
POP3 and IMAP cannot use self-signed certificates for inbound email.	K1-21086
Invalid filters (Smart Labels) can be saved, resulting in Smart Labels that never populate.	K1-20268
An error may be seen while creating custom view on the *Quarantine* page in the Consola de administración del sistema.	ESMP-7825
On the *Agent Tokens* list page, in the **Choose Action** menu, selecting **Create Report** does not work as expected.	ESMP-7799
In the Consola de administración del sistema, the *Agent Token Detail* page displays the organization ID instead of the name.	ESMP-7793
Device links on the *Agent Command Queue* and *Agent Task Status* pages may not function as expected.	ESMP-7774
Do not associate file Managed Installation option does not display correctly after saving.	ESMP-7753
Token Usage by Machine record is not updated when machine changes token or is removed from list.	ESMP-7588
Recurring alert messages keep spawning new windows on the device.	ESMEC-3913
Wake-on-LAN (WoL) through relay does not display error when the relay agent selected is down.	ESMEC-3898
Monitoring can fail with error in the Mac OS 11 system log because it has multi-line entries in `system.log`.	ESMEC-3883
Existing Patch Schedule name is allowed when duplicating the schedule.	ESMAM-2863
In KACE GO, any ticket attachments past the fifth on a single comment are not saved correctly.	ESMAS-5006

Requisitos del sistema

La versión mínima requerida para instalar KACE Systems Management Appliance 11.0 es 10.2. Si su dispositivo ejecuta una versión anterior, deberá actualizarla a la versión indicada antes de continuar con la instalación.

La versión mínima requerida para actualizar el agente de KACE es la 9.0. Recomendamos ejecutar la última versión del agente con KACE Systems Management Appliance 11.0.

Para comprobar el número de versión del dispositivo, inicie sesión en Consola del administrador y haga clic en **¿Necesita ayuda?** En el panel de ayuda que aparece en la parte inferior, haga clic en el botón "**i**" en un círculo.

Antes de actualizar o instalar la versión 11.0, verifique que su sistema cumpla con los requisitos mínimos. Estos requisitos están disponibles en las especificaciones técnicas de KACE Systems Management Appliance.

- Para dispositivos virtuales: vaya a https://support.quest.com/technical-documents/kace-systems-management-appliance/11.0-common-documents/technical-specifications-for-virtual-appliances/.
- Para KACE como servicio: vaya a https://support.quest.com/technical-documents/kace-systems-management-appliance/11.0-common-documents/technical-specifications-for-kace-as-a-service/.

Licencia de producto

Si actualmente posee una licencia de producto para KACE Systems Management Appliance, no se requiere una licencia adicional.

Si es la primera vez que utiliza KACE Systems Management Appliance, consulte la guía de configuración del dispositivo para ver los detalles de licencias del producto. Vaya a Más recursos para ver la guía adecuada.

NOTA: Las licencias del producto para la versión 11.0 se pueden usar solamente en KACE Systems Management Appliance de versión 11.0 o posterior. Las licencias de la versión 11.0 no se pueden utilizar en dispositivos de versiones anteriores, como la versión 9.0.

Instrucciones de instalación

Puede aplicar esta versión mediante una actualización anunciada o mediante la carga y aplicación manual de un archivo de actualización. Para obtener instrucciones, consulte los siguientes temas:

- Preparación para la actualización
- Actualización del servidor de KACE Systems Management Appliance mediante una actualización anunciada
- Carga y ejecución manual de una actualización
- Tareas posteriores a la actualización

NOTA: Para garantizar la precisión de la detección del software y los recuentos de instalación para dispositivos con un software particular, comenzando en la versión 7.0 de KACE Systems Management Appliance, el catálogo de software se reinstala con cada actualización.

Preparación para la actualización

Antes de actualizar el servidor de KACE Systems Management Appliance, siga estas recomendaciones:

- **Verifique la versión del servidor de KACE Systems Management Appliance**:

  La versión mínima requerida para instalar KACE Systems Management Appliance 11.0 es 10.2. Si su dispositivo ejecuta una versión anterior, deberá actualizarla a la versión indicada antes de continuar con la instalación.

  Para comprobar el número de versión del dispositivo, inicie sesión en Consola del administrador y haga clic en **¿Necesita ayuda?** En el panel de ayuda que aparece en la parte inferior, haga clic en el botón "**i**" en un círculo.

- **Verifique la versión del agente de KACE**.

La versión mínima requerida para actualizar el agente de KACE es la 9.0. Recomendamos ejecutar la última versión del agente con KACE Systems Management Appliance 11.0.

- **Realice una copia de seguridad antes de empezar**.

  Realice una copia de seguridad de la base de datos y los archivos. A continuación, guárdela en una ubicación que no esté en el servidor de KACE Systems Management Appliance por si tiene que acudir a ella más adelante. Para obtener instrucciones sobre cómo realizar una copia de seguridad de la base de datos y los archivos, consulte la Guía para el administrador, https://support.quest.com/technical-documents/kace-systems-management-appliance/11.0-common-documents/administrator-guide/.

- **Dispositivos instalados antes de la versión 7.0**.

  En el caso de los dispositivos instalados inicialmente antes de la versión 7.0 para los cuales no se haya recreado la imagen (dispositivos físicos) o que no se hayan reinstalado (de manera virtual), Quest Software recomienda encarecidamente exportar, volver a crear (una imagen o instalación de una máquina virtual desde un archivo OVF) y volver a importar la base de datos antes de actualizar a la versión 11.0. Para obtener más información, visite https://support.quest.com/kace-systems-management-appliance/kb/111810/how-to-re-image-the-k1000-appliance.

  Si la versión de su dispositivo no corresponde a la más actualizada, se incluyeron consejos útiles acerca de la actualización en el siguiente artículo: 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-.

  Hay muchas razones por las que debe recrear la imagen del dispositivo. Por ejemplo, la nueva disposición del disco ofrece una mejor compatibilidad con la versión 11.0. También cuenta con seguridad y rendimiento superiores.

  Para determinar si su sistema se beneficiaría de dicha actualización, puede usar un archivo `KBIN` para determinar la antigüedad exacta de su dispositivo y su diseño de disco. Para descargar el `KBIN`, visite https://support.quest.com/kace-systems-management-appliance/kb/210267/how-to-run-the-kace-systems-management-appliance-configuration-report.

- **Asegúrese de que el puerto 52231 esté disponible**.

  Antes de cualquier actualización `.kbin`, el puerto 52231 debe estar disponible para que se pueda acceder a la página de la consola de actualización de KACE. Si la actualización se inicia sin que este puerto esté disponible, no podrá supervisar el progreso de la actualización. Quest KACE recomienda permitir el tráfico al dispositivo a través del puerto 52231 desde un sistema confiable y monitorear la actualización desde la consola de actualización. Sin acceso a la consola de actualización, la actualización redirige a una página inaccesible que aparece en el navegador como tiempo de espera. Esto puede hacer que una persona crea que la actualización bloqueó el sistema, lo que provoca que se reinicie el equipo cuando, en realidad, la actualización aún está en curso. Si no está seguro acerca del progreso de la actualización, comuníquese con el equipo de soporte de KACE y **no reinicie el dispositivo**.

Actualización del servidor de KACE Systems Management Appliance mediante una actualización anunciada

Puede actualizar el servidor de KACE Systems Management Appliance mediante una actualización anunciada en la página *Panel* o en la página *Actualizaciones del dispositivo* de la Consola del administrador.

PRECAUCIÓN: Nunca reinicie el servidor de KACE Systems Management Appliance de forma manual durante una actualización.

1. Realice una copia de respaldo de la base de datos y los archivos. Para ver las instrucciones, consulte la Guía para el administrador, https://support.quest.com/technical-documents/kace-systems-management-appliance/11.0-common-documents/administrator-guide/.
2. Vaya al *Panel de control* del dispositivo:
   - Si el componente Organización no está habilitado en el dispositivo, haga clic en **Ajustes**.
   - Si el componente Organización sí está habilitado en el dispositivo: Inicie sesión en la Consola de administración del sistema del dispositivo: `http://`KACE_SMA_hostname`/system` o seleccione **Sistema** en la lista desplegable de la esquina superior derecha de la página y luego haga clic en **Ajustes**.
3. En la barra de navegación de la izquierda, haga clic en **Actualizaciones del dispositivo** para mostrar la página *Actualizaciones del dispositivo*.
4. Haga clic en **Comprobar actualizaciones**.

   Aparecen los resultados de la comprobación en el registro.
5. Cuando haya una actualización disponible, haga clic en **Actualizar**.

   IMPORTANTE: Puede que algunos navegadores parezcan congelarse durante los primero diez minutos en que se desempaqueta y verifica la actualización. No salga de la página, no actualice la página ni haga clic en cualquiera de los botones del navegador en la página durante este tiempo, ya que estas acciones interrumpen el proceso. Después de que se desempaqueta y se verifica la actualización, aparece la página de *Registros*. No reinicie manualmente el dispositivo en cualquier momento durante el proceso de actualización.

   Se aplica la versión 11.0 y se reinicia el servidor de KACE Systems Management Appliance. El progreso aparece en la ventana del navegador y en la Consola del administrador.
6. Cuando finalice la actualización del servidor, actualice todos sus agentes a la versión 11.0.

Carga y ejecución manual de una actualización

Si cuenta con un archivo de actualización de Quest, puede cargar ese archivo manualmente para actualizar el servidor de KACE Systems Management Appliance.

PRECAUCIÓN: Nunca reinicie el servidor de KACE Systems Management Appliance de forma manual durante una actualización.

1. Realice una copia de respaldo de la base de datos y los archivos. Para ver las instrucciones, consulte la Guía para el administrador, https://support.quest.com/technical-documents/kace-systems-management-appliance/11.0-common-documents/administrator-guide/.
2. Con sus credenciales de inicio de sesión de cliente, inicie sesión en el sitio web de Quest en https://support.quest.com/kace-systems-management-appliance/download-new-releases, descargue el archivo `.kbin` del servidor de KACE Systems Management Appliance para la versión 11.0 GA (disponibilidad general) y guárdelo localmente.
3. En la barra de navegación de la izquierda, haga clic en **Actualizaciones del dispositivo** para mostrar la página *Actualizaciones del dispositivo*.
4. En la sección *Actualizar manualmente*:
   a. Haga clic en **Examinar** o en **Elegir archivo** y ubique el archivo de actualización.
   b. Haga clic en **Actualizar** y luego haga clic en **Sí** para confirmar.

   Se aplica la versión 11.0 y se reinicia el servidor de KACE Systems Management Appliance. El progreso aparece en la ventana del navegador y en la Consola del administrador.
5. Cuando finalice la actualización del servidor, actualice todos sus agentes a la versión 11.0.

Tareas posteriores a la actualización

Luego de la actualización, verifique que esta haya sido exitosa y verifique la configuración, según sea necesario.

Verificación de finalización correcta

Para verificar que la actualización se haya realizado correctamente, vea el número de la versión de KACE Systems Management Appliance.

1. Vaya al *Panel de control* del dispositivo:
   - Si el componente Organización no está habilitado en el dispositivo, haga clic en **Ajustes**.
   - Si el componente Organización sí está habilitado en el dispositivo: Inicie sesión en la Consola de administración del sistema del dispositivo: `http://`KACE_SMA_hostname`/system` o seleccione **Sistema** en la lista desplegable de la esquina superior derecha de la página y luego haga clic en **Ajustes**.
2. Para comprobar la versión actual, haga clic en **¿Necesita Ayuda?** en la esquina superior derecha de la página y, en el panel de ayuda que aparece, en la parte inferior, haga clic en el botón **i** en un círculo.

Verificación de ajustes de seguridad

Para mejorar la seguridad, el acceso a la base de datos a través de HTTP y FTP está deshabilitado durante la actualización. Si utiliza estos métodos para acceder a los archivos de la base de datos, cambie los ajustes de seguridad luego de la actualización, según sea necesario.

1. Vaya al *Panel de control* del dispositivo:
   - Si el componente Organización no está habilitado en el dispositivo, haga clic en **Ajustes**.
   - Si el componente Organización sí está habilitado en el dispositivo: Inicie sesión en la Consola de administración del sistema del dispositivo: `http://`KACE_SMA_hostname`/system` o seleccione **Sistema** en la lista desplegable de la esquina superior derecha de la página y luego haga clic en **Ajustes**.
2. En la barra de navegación de la izquierda, haga clic en **Ajustes de seguridad** para mostrar la página *Ajustes de seguridad*.
3. En la sección superior de la página, modifique los siguientes ajustes:
   - **Habilitar archivos de copia de seguridad seguros**: desactive esta casilla de verificación para habilitar que los usuarios accedan a los archivos de copia de seguridad de la base de datos a través de una HTTP sin autenticación.
   - **Habilitar acceso a la base de datos**: seleccione esta casilla de verificación para habilitar que los usuarios accedan a la base de datos a través del puerto 3306.
   - **Habilitar copia de seguridad a través del FTP**: seleccione esta casilla de verificación para habilitar que los usuarios accedan a los archivos de copia de seguridad de la base de datos a través de un FTP.

   PRECAUCIÓN: No se recomienda la modificación de estos ajustes, ya que disminuye la seguridad de la base de datos.
4. Haga clic en **Guardar**.
5. **Solo actualizaciones KBIN**. Fortalezca el acceso al dispositivo con la contraseña raíz (2FA).
   a. En la Consola de administración del sistema, haga clic en **Ajustes** > **Soporte**.
   b. En la página de *Soporte*, en *Herramientas para la solución de problemas*, haga clic en **Autenticación de dos factores**.

c. En la página *Autenticación de dos factores*, haga clic en **Reemplazar clave secreta**.
d. Registre los tokens y coloque esta información en un lugar seguro.

Más recursos

Podrá encontrar información adicional a través de los siguientes recursos:

- Documentación del producto en línea (https://support.quest.com/kace-systems-management-appliance/11.0/technical-documents)
  - **Especificaciones técnicas**: información sobre los requisitos mínimos para instalar o actualizar a la última versión del producto.

    Para dispositivos virtuales: vaya a https://support.quest.com/technical-documents/kace-systems-management-appliance/11.0-common-documents/technical-specifications-for-virtual-appliances/.
    Para KACE como servicio: vaya a https://support.quest.com/technical-documents/kace-systems-management-appliance/11.0-common-documents/technical-specifications-for-kace-as-a-service/.
  - **Guías de configuración**: instrucciones para configurar dispositivos virtuales. Vaya a https://support.quest.com/kace-systems-management-appliance/11.0/technical-documents para ver la documentación de la última versión.
  - **Guía para el administrador**: instrucciones para usar el dispositivo. Vaya a https://support.quest.com/technical-documents/kace-systems-management-appliance/11.0-common-documents/administrator-guide/ para ver la documentación de la última versión.

Globalización

Esta sección contiene información acerca de la instalación y el funcionamiento de este producto en configuraciones que no están en idioma inglés, como las que necesitan los clientes de fuera de los Estado Unidos. Esta sección no reemplaza la información acerca de plataformas y configuraciones admitidas que se encuentra en otras secciones de la documentación del producto.

Esta versión es compatible con Unicode y admite cualquier conjunto de caracteres. En esta versión, todos los componentes del producto deben estar configurados para utilizar la misma codificación de caracteres, o una compatible, y deben estar instalados para que utilicen el mismo idioma y las mismas opciones regionales. Esta versión está destinada a brindar soporte a las operaciones en las siguientes regiones: América del Norte, Europa Occidental y América Latina, Europa Central y del Este, Lejano Oriente, Japón.

La versión está localizada en los siguientes idiomas: Francés, alemán, japonés, portugués (Brasil), español.

Acerca de nosotros

Quest crea soluciones de software que hacen reales los beneficios de las nuevas tecnologías en un panorama de TI cada vez más complejo. Desde administración de bases de datos y de sistemas hasta administración de Active Directory y Office 365 y resistencia a la seguridad cibernética, Quest ayuda a los clientes a resolver su próximo desafío de TI ahora. En todo el mundo, más de 130.000 empresas y el 95 % de la lista Fortune 500 confían en Quest para disfrutar de administración y monitoreo proactivos en la próxima iniciativa empresarial, encontrar la siguiente solución para los desafíos complejos de Microsoft y mantenerse a la vanguardia ante la próxima amenaza. Quest Software. Donde convergen el futuro y el presente. Para obtener más información, visite www.quest.com.

Recursos del soporte técnico

El soporte técnico se encuentra disponible para los clientes de Quest con un contrato válido de mantenimiento y para los clientes que poseen versiones de prueba. Puede acceder al portal del Soporte de Quest en https://support.quest.com.

El portal de soporte proporciona herramientas de autoayuda que puede utilizar para resolver problemas de forma rápida e independiente, las 24 horas al día, los 365 días del año. El portal de soporte le permite:

- Enviar y gestionar una solicitud de servicio
- Consultar los artículos de la base de conocimientos
- Suscribirse a las notificaciones de productos
- Descargar documentación del software y técnica
- Ver videos de procedimientos
- Participar en debates de la comunidad
- Chatear en línea con ingenieros de soporte
- Ver servicios para ayudarlo con su producto

Avisos legales

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.

Patentes

Quest Software se enorgullece de nuestra tecnología avanzada. Es posible que se apliquen patentes y patentes pendientes a este producto. Para obtener la información más actual sobre las patentes aplicables a este producto, visite nuestro sitio web en https://www.quest.com/legal.

Leyenda

PRECAUCIÓN: Un ícono de PRECAUCIÓN indica la posibilidad de daños al equipo o pérdida de datos si no se siguen las instrucciones.

IMPORTANTE, NOTA, SUGERENCIA, MÓVIL o VIDEO: Un ícono de información indica información de soporte.

Notas de la versión del dispositivo de administración de sistemas KACE

Actualizado en: octubre del 2020

Versión del software: 11.0