Quest

Dispositivo de administración de sistemas KACE® 13.0

Notas de la versión

Índice

Notas de la versión 13.0 del dispositivo de administración de sistemas KACE® de Quest®

En este documento, se proporciona información acerca de la versión 13.0 de KACE Systems Management Appliance.

Acerca del dispositivo de administración de sistemas KACE 13.0

El dispositivo de administración de sistemas KACE está 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.

Nuevas características

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

- **Notificaciones de usuario procesables**: El dispositivo incluye ahora una amplia gama de configuraciones de notificación predefinidas. Varias categorías disponibles se centran en los aspectos específicos de su entorno, como la seguridad o la aplicación de parches. Cuando revisa las notificaciones activadas, los colores de fondo indican la gravedad de la alerta: información (azul), advertencia (amarillo) y advertencia (rojo). Algunas notificaciones incluyen vínculos prácticos que le permiten desglosar el objeto asociado con la notificación. Por ejemplo, si ve un aviso de expiración de licencia, el vínculo en la notificación lo lleva directamente a la instancia de licencia que está a punto de caducar.

  NOTA: La información de la sección Alerta en la página *Detalles del panel* se ha trasladado al panel de notificaciones.

- **Desinstalación del software simplificada**: Ahora puede agregar o eliminar rápidamente un elemento de la lista de software de una instalación administrada mediante la página *Detalles de la lista de software*.
- **Integración de Let's Encrypt para la administración sencilla de certificados**: Let's Encrypt es una entidad de certificación (CA, del inglés Certificate Authority) gratuita, automatizada y abierta. Cuando obtiene un certificado de Let's Encrypt, sus servidores validan que controla los nombres de dominio en ese certificado mediante un desafío. Debe tener una cuenta de Let's Encrypt registrada en el improbable caso de que el certificado expire.
- **Integración de la autenticación de Google Workspace**: A partir de esta versión, el dispositivo puede autenticar a los usuarios con las credenciales de Google Workspace. Este proceso se utiliza en Inventario,

Distribución, Scripts y Mesa de servicio. Los siguientes componentes administrados por el dispositivo se pueden autenticar a través de la API de Google:

  - **Detección e Inventario de dispositivos de Google Workspace**: Esto incluye tanto Chromebooks como dispositivos móviles administrados por un dominio de Google Workspace (anteriormente *G Suite*).
  - **Correo electrónico entrante de cola de la mesa de servicio**: Esto incluye cuentas de correo que forman parte de un Google Workspace o una cuenta pública de Gmail.

- **Análisis de virus de los datos adjuntos de la mesa de servicio**: El dispositivo ahora incluye una función de detección de malware para adjuntos de archivo de la mesa de servicio. Este proceso automatizado garantiza que las listas de definiciones de virus se actualicen regularmente. Todos los datos adjuntos de tickets se analizarán antes de que se agreguen a los tickets. Administre los archivos en cuarentena a través de la página *Cuarentena por antivirus*. Utilice esta página para revisar y administrar los archivos adjuntos de la mesa de servicio en cuarentena. Aparece una notificación cuando se detecta una amenaza, con un vínculo al dispositivo asociado con el archivo. También puede crear notificaciones cuando se detectan tipos específicos de amenazas o según su cambio de estado.
- **Distribución de datos adjuntos de la mesa de servicio a través del correo electrónico**: El dispositivo ahora puede enviar archivos adjuntos al ticket en lugar de proporcionar vínculos de archivos. También puede agregar archivos adjuntos a plantillas de correo electrónico cuando sea necesario.

NOTA: Los requisitos mínimos de memoria para ejecutar (o actualizar un sistema 12.1) a 13.0 han cambiado. Se requiere un mínimo de 8 GB para operar correctamente el dispositivo. Además, el monitoreo ahora es compatible con dispositivos macOS 12.0 administrados. Para obtener más detalles, consulte *Especificaciones técnicas*.

Mejoras

La siguiente es una lista de las mejoras implementadas en esta versión.

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

Enhancement	Issue ID
Added DirectX version to inventory data.	K1A-3898
Agentless support for Red Hat Enterprise Linux 9.	K1-33030
Agentless support for Windows 11 22H2.	K1-33028
Agentless support for Raspbian Linux 11 (Bullseye).	K1-32835
Added logical disks to Dell Data Protection | Encryption inventory on Windows.	K1-32746
Migrated Google OAuth support for Google Workspace Integration.	K1-32682
Added ticket history for deleted Service Desk tickets.	K1-32646
Agentless support for openSUSE Leap 15.4.	K1-32604
Agentless support for Fedora 35 and 36.	K1-32603
Agentless support for Ubuntu 22 LTS.	K1-32602
Ability to limit system generated approval workflow comments to owners only.	K1-32547
Added ability to create a managed uninstall directly from the SW Catalog Detail Page using a **Add Managed Uninstall** button.	K1-32530
The TLS 1.2 ciphers are adjusted to provide the highest possible security rating while maintaining client compatibility.	K1-32476
Added a link to the Microsoft Defender Advanced Threat Protection console to the Microsoft Defender section on the *Device Detail* page, when applicable.	K1-32422
My Recent Sessions pop-up includes country, if available.	K1-32412
Updated User Notification system to forward new notifications to push server.	K1-32277
Added ability to remove incoming SMTP capability from appliance.	K1-32096
Removed framesets from the **Administrator Console**, **System Administration Console**, and **User Console**.	K1-30094
Drop-down fields (*Category*, *Impact*, *Priority*, and *Status*) can be left blank when required	K1-22073

Problemas resueltos

Esta sección contiene los problemas resueltos en esta versión:

Resolved Service Desk issues

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

Resolved Service Desk issues

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

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

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

Resolved API issues

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

Resolved API issues

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

Resolved Reporting issues

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

Resolved Reporting issues

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

Resolved Server issues

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

Resolved server issues

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

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

Resolved KACE Agent issues

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

Resolved KACE Agent issues

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

Problemas conocidos

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

NOTA: El inventario de dispositivos Ubuntu 21.04 sin agente falla para los usuarios que tienen un shell no predeterminado de Bash.

Known issue	Issue ID
Agentless inventory of macOS 12 incorrectly shows two volumes mounted to '/'.	K1-33162
Manually provisioning an SNMP device from *Discovery Results* page shows missing settings when SNMP walk is selected and that walk failed.	K1-33154
Nmap discovery type with TCP or UDP port scan options selected does not return opened ports.	K1-33005
Device Actions can sometimes fail when accessing them through a direct URL.	K1-32305
Login field does not update after user authenticates through SAML and the mapping was changed.	K1-32304
Large metering data can cause page to load slowly.	K1-32249
Schedule info does not show correctly after disabling a Linux Package Upgrade Schedule.	K1-30725
Managed Install snooze time is ignored. Snooze option does not reappear until next inventory interval.	K1-20832
Managed Install attempts used up during inventory when user alert is snoozed.	K1-20826

Requisitos del sistema

La versión mínima requerida para instalar KACE Systems Management Appliance 13.0 es 12.1. 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 11.0. Recomendamos que siempre utilice la misma versión del agente y el dispositivo de administración de sistemas KACE.

A partir de la versión 12.0 del aparato, las versiones anteriores del agente de KACE, como 11.1, deben firmarse específicamente para la versión del dispositivo. Por ejemplo, si utiliza el agente de KACE 11.1 con la versión 12.1 del dispositivo, debe obtener e instalar el archivo KBIN del agente de KACE 11.1 que está firmado con la clave de dispositivo 12.1. Puede descargar archivos KBIN del agente de KACE firmados desde la página de *descargas de software* del dispositivo de administración de sistemas KACE.

NOTA: El paquete RPM del agente de KACE se puede instalar en dispositivos SUSE Linux administrados solo cuando se instala el paquete `libxslt-tools` antes del paquete del agente.

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 13.0, 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/13.0-common-documents/technical-specifications-for-virtual-appliances/.
- Para KACE como servicio: vaya a https://support.quest.com/technical-documents/kace-systems-management-appliance/13.0-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 13.0 se pueden usar solamente en KACE Systems Management Appliance de versión 13.0 o posterior. Las licencias de la versión 13.0 no se pueden utilizar en dispositivos de versiones anteriores, como la versión 12.0.

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:

- **IMPORTANTE: Activar el arranque del BIOS heredado**:

  Se puede activar un problema en el arranque del BIOS de UEFI durante una actualización. Para evitarlo, debe asegurarse de que el arranque del BIOS heredado esté activado. Es necesario apagar el dispositivo antes de realizar un cambio. Además, para las máquinas virtuales basadas en ESX, asegúrese de que la versión de hardware sea 13 o posterior.

  Antes de aplicar la actualización del dispositivo, debe asegurarse de que la caché del navegador esté limpia y que el puerto 52231 esté disponible desde el navegador hasta el dispositivo. Es posible que los usuarios que trabajan desde casa deban tener su firewall corporativo configurado para permitir las comunicaciones del puerto 52231.

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

La versión mínima requerida para instalar KACE Systems Management Appliance 13.0 es 12.1. 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 11.0. Recomendamos que siempre utilice la misma versión del agente y el dispositivo de administración de sistemas KACE.

  A partir de la versión 12.0 del aparato, las versiones anteriores del agente de KACE, como 11.1, deben firmarse específicamente para la versión del dispositivo. Por ejemplo, si utiliza el agente de KACE 11.1 con la versión 12.1 del dispositivo, debe obtener e instalar el archivo KBIN del agente de KACE 11.1 que está firmado con la clave de dispositivo 12.1. Puede descargar archivos KBIN del agente de KACE firmados desde la página de *descargas de software* del dispositivo de administración de sistemas KACE.

  NOTA: El paquete RPM del agente de KACE se puede instalar en dispositivos SUSE Linux administrados solo cuando se instala el paquete `libxslt-tools` antes del paquete del agente.

- **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/13.0-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 13.0. 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 13.0. 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 del dispositivo de administración de sistemas KACE 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/13.0-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 el dispositivo Consola de administración del sistema: `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 13.0 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 13.0.

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/13.0-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 13.0 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 13.0 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 13.0.

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 el dispositivo Consola de administración del sistema: `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 el dispositivo Consola de administración del sistema: `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/13.0/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/13.0-common-documents/technical-specifications-for-virtual-appliances/.
    Para KACE como servicio: vaya a https://support.quest.com/technical-documents/kace-systems-management-appliance/13.0-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/13.0/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/13.0-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

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.

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.

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.

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 2022

Versión del software: 13.0