



Dispositivo de administración de sistemas K1000 7.0 Dell KACE™

Notas de la versión

Noviembre de 2016

En este documento de notas de la versión, se proporciona información acerca de la versión 7.0 del dispositivo de administración de sistemas K1000.

Temas:

- [Acerca del dispositivo de administración de sistemas K1000 7.0](#) en la página 1
- [Nuevas características y mejoras](#) en la página 1
- [Problemas resueltos](#) en la página 16
- [Problemas conocidos](#) en la página 18
- [Requisitos del sistema](#) en la página 19
- [Licencia de producto](#) en la página 20
- [Instrucciones de instalación](#) en la página 20
- [Más recursos](#) en la página 23
- [Globalización](#) en la página 24

Acerca del dispositivo de administración de sistemas K1000 7.0

El dispositivo de administración de sistemas K1000 es un dispositivo físico o virtual diseñado para automatizar la administración de dispositivos, la implementación de aplicaciones, los parches, la administración de activos y la administración de tickets de la Mesa de servicio. Para obtener más información acerca de los dispositivos de la serie K1000, visite <http://software.dell.com/products/kace-k1000-systems-management-appliance/>.

Nuevas características y mejoras

Los siguientes módulos del dispositivo de administración de sistemas K1000 incluyen nuevas características y mejoras en esta versión:

- [Mesa de servicio y consola de usuario](#) en la página 2
- [Aplicación de parches y seguridad](#) en la página 6
- [Inventario y administración de activos](#) en la página 7
- [Distribución y scripting](#) en la página 9
- [Mejoras a la administración del usuario](#) en la página 10
- [Mejoras a la ubicación](#) en la página 11
- [Informes entre dispositivos](#) en la página 12
- [Administración de dispositivos basada en agente](#) en la página 12
- [Administración de dispositivos sin agente](#) en la página 13
- [Supervisión](#) en la página 14
- [Configuración y seguridad](#) en la página 15
- [Compatible con API](#) en la página 16

ⓘ IMPORTANTE: En esta versión, el servicio AMPAgent y el protocolo AMP se han reemplazado con el protocolo y servicio Konea. Para obtener más información, consulte [Administración de dispositivos basada en agente](#) en la página 12.

Para obtener toda la información acerca de estas características, consulte la *Guía para el administrador*.

Para obtener más información acerca de las nuevas características de esta versión, vea los videos instructivos disponibles en nuestro sitio de soporte: <https://support.quest.com/k1000-systems-management-appliance/kb/video-articles?k=what%27s+new>.

Mesa de servicio y consola de usuario

La mesa de servicio y la consola de usuario incluyen las siguientes características y mejoras:

- [Configuración de colas](#) en la página 2
- [Proceso de flujo de trabajo](#) en la página 3
- [Aprobaciones de flujo de trabajo](#) en la página 5

Configuración de colas

Esta versión incluye las siguientes características de configuración de colas:

- **Validación de la configuración de SMTP en cola.** La configuración de SMTP en cola incluye nombre de usuario, contraseña, nombre de servidor y número de puerto. El no proporcionar esta información podría impedir el envío de los correos electrónicos a usuarios específicos. En esta versión, se agregó un proceso de validación para garantizar que estos valores se añadan cuando la configuración de SMTP se active.
- **Capacidad de mostrar comentarios en la página Nuevo ticket.** La página *Personalización de cola* ahora permite indicar si desea mostrar los comentarios y archivos adjuntos en la página de tickets. Puede marcar o desmarcar esta opción según sea necesario:

- **Mostrar comentarios en los tickets:** Por defecto, esta opción solo está activada para las colas existentes que no muestran el campo Resumen en la página de tickets.
- **Mostrar los archivos adjuntos en los tickets:** Por defecto, esta opción está activada para las colas nuevas y existentes.
- **Agregar comentarios a un ticket origina notificaciones de correo electrónico.** Las notificaciones de correo electrónico se envían cuando se agrega un comentario a un ticket, después de usar el botón **Guardar** o **Aplicar** en la página de tickets.
- **Personalización de formularios de entrada de tickets mejorada.** La sección *Campos de tickets de diseño* en la página *Personalización de cola* se actualiza para dar pleno control a los administradores sobre la visibilidad y el posicionamiento de los campos que aparecen en la página *Nuevo ticket*.
- **Vistas previas de diseño de tickets.** Durante la personalización del diseño de los tickets, ahora los administradores tienen la posibilidad de acceder a una vista previa para visualizar el diseño de un ticket específico en diferentes modos antes de guardar los cambios (página *Nuevo ticket: Administrador*, página *Nuevo ticket: Usuario*, página *Detalles del ticket: Administrador*, *Detalles del ticket: Usuario*).
- **Capacidad de mostrar subcategorías cuando se filtra o informa sobre una categoría principal.** Seleccionar una categoría principal mediante vista personalizada, búsqueda o informe arroja todos los tickets de la categoría principal y todas las subcategorías relacionadas.

Proceso de flujo de trabajo

Esta versión incluye las siguientes características de proceso:

- **Mejoras del proceso.**
 - En esta versión, se incluye el nuevo asistente para *Crear plantilla de proceso* que le permite crear plantillas de proceso. Utilice una plantilla de proceso (anteriormente conocida como *proceso*) cuando desee crear tickets de proceso que contengan tareas relacionadas.
 - El asistente proporciona un flujo de trabajo intuitivo para especificar aprobaciones, además de notificaciones y flujo de trabajo de tickets. Si utiliza el flujo de trabajo de estado de proceso en lugar del flujo de trabajo de ticket, el ticket principal asociado avanza automáticamente a través de diversos estados específicos de proceso. Si decide no seleccionar esta opción y usar los flujos de trabajo de ticket, debe crear reglas del ticket personalizadas para conseguir lograr una funcionalidad de aprobación y notificación, según sea necesario.
 - Los pasos del proceso pueden estar ocultos de los usuarios finales, si es necesario.
 - Los remitentes y propietarios de procesos pueden cancelar el proceso en cualquier momento, de modo que no se trabaje más en este proceso. Se registra la cancelación de un proceso en el historial de tickets de proceso.
 - Las vistas de *Todos los tickets por estado de proceso* y *Mis tickets por estado de proceso* se han agregado a la página *Tickets*.
- **Actualizaciones a la página Tickets.**

- La columna *Proceso* en la página *Tickets* indica si el ticket está basado en una plantilla de proceso (*Sí* o *No*).
- Se han agregado las columnas *Tipo de proceso* y *Tipo de ticket* a la página *Tickets*. Para un ticket basado en un proceso, la columna *Estado* muestra el estado del proceso relacionado.
- Se han agregado nuevas vistas del sistema listas para usarse en esta versión: *Por tipo de proceso* y *Por estado del proceso*.

Actualización a la vista personalizada y la búsqueda avanzada. Estas vistas ahora incluyen las opciones de estado y tipo de proceso. Puede utilizarlas para buscar un tipo o estado de proceso específicos.

- **Actualizaciones a las plantillas de proceso.**

- Se han agregado las siguientes columnas a la lista *Plantillas de procesos*: *Tipo de proceso* y *Aprobación requerida* (*Sí* o *No*).
- La columna *Todos los usuarios* ahora se denomina *Visibilidad*. Muestra *Todos los usuarios* o los nombres de etiqueta apropiados separados por comas.
- La columna *Estado* ahora se denomina *Habilitado*. Se establece en *Sí* o *No*.
- La columna *Descripción* se eliminó de la lista.
- Durante la configuración de una plantilla de proceso, los administradores pueden configurar automáticamente el remitente o propietario del ticket secundario como el remitente o propietario del ticket principal, de modo que puedan establecer los usuarios predeterminados dinámicamente en un proceso, basado en cómo se envió el ticket principal inicial.
- Ahora es posible diferenciar entre diversos tipos de proceso a la hora de gestionar e informar sobre los tickets, como cambiar registros y solicitudes de servicio.
- La página *Detalles del ticket* para el ticket principal asociado con un proceso incluye los campos *Tipo de proceso* y *Estado del proceso*.
- Los propietarios de procesos pueden mover el proceso a un estado *Completo* en cualquier momento para indicar que el proceso se ha completado correctamente, incluso si todas las aprobaciones o los tickets secundarios no están actualizados correctamente en el sistema.
- Cuando se crea un nuevo ticket basado en un proceso, el primer paso es ver el nombre y la descripción del proceso. El contenido de esta página permite hipervínculos y contenido HTML/Markdown, tal como se ha configurado para el proceso. Esta página se puede ocultar, cuando sea necesario, desactivando la casilla **Mostrar página de descripción del proceso mientras se crean nuevas solicitudes de proceso** en la página *Opciones de publicación* del asistente para *Crear plantilla de proceso*. Cuando haga clic en *Continuar* en la página de descripción y nombre del proceso, aparece la página *Nuevo ticket*, que le permite especificar los detalles del ticket principal.
- Los administradores pueden configurar notificaciones automáticas de correo electrónico para distintos eventos dentro del flujo de trabajo de las tareas para controlar el contenido y los destinatarios de las notificaciones para cada evento en el ciclo de vida del proceso.
- Hay un conjunto de plantillas de correo electrónico disponible para las notificaciones de correo electrónico relacionadas con los procesos. Estas plantillas se pueden seleccionar en el asistente para *Crear plantilla de proceso*. Se debe crear una plantilla independiente para cada evento de proceso: *Proceso enviado*, *aprobación*

requerida, aprobación con tiempo de espera agotado, aprobación recibida, aprobación rechazada, proceso cancelado y proceso completo.


- Se han agregado nuevos tokens en esta versión para compatibilizar con las notificaciones de correo electrónico relacionadas con los procesos: `$process_description`, `$process_name`, `$process_status` y `$process_type`.

Aprobaciones de flujo de trabajo

Esta versión incluye las siguientes características de aprobación del flujo de trabajo:

- **Situaciones de aprobación flexibles.** Los tickets basados en procesos pueden estar sujetos a diferentes situaciones de aprobación. Por ejemplo, puede crear tickets de procesos que no requieran aprobaciones o que requieran una o varias. El flujo de trabajo del proceso comienza cuando se reciben todas las aprobaciones aplicables. El siguiente procedimiento ilustra un flujo de trabajo típico:
 - 1 Un usuario crea un nuevo ticket basado en proceso.
 - 2 Se crea un ticket principal.
 - 3 Si se requiere cualquier aprobación:
 - a Se envían las solicitudes de aprobación a los aprobadores.
 - b Si los recordatorios de aprobación están activados:
 - Se envían los recordatorios de aprobación a los aprobadores de acuerdo con el programa especificado.
 - c Si una aprobación supera el tiempo de espera o se rechaza:
 - El proceso se cierra con el estado apropiado.
 - d Cuando se reciben todas las respuestas de aprobación y todas las aprobaciones se conceden antes de que se acabe el tiempo de espera:
 - El proceso avanza y se crean todos los tickets de la etapa 1.
 - 4 Si no se requieren aprobaciones:
 - El proceso avanza y se crean todos los tickets de la etapa 1.
- **Configuración de las aprobaciones.**
 - Es posible que haya varias situaciones de aprobación, las que incluyen:
 - Sin aprobación
 - Aprobación de nivel individual

- Aprobación de nivel grupal
- Aprobación secuencial

 **NOTA:** Cada fase de la secuencia puede tener aprobación de nivel individual o grupal.

- Los administradores pueden omitir el requisito de aprobación para garantizar que el proceso continúe en caso de que uno o más de los aprobadores no estén disponibles, o podrían no proporcionar la aprobación necesaria antes de agotarse el tiempo de espera. Esta acción solo se puede realizar para los procesos en el estado Pendiente de aprobación. No está disponible para los procesos para los que ya se agotó el tiempo de espera y se cerraron debido a la denegación de la aprobación.
- Los administradores pueden configurar el tiempo de espera de las aprobaciones para especificar cuánto tiempo tiene cada aprobador de tickets para aprobar o rechazar un ticket basado en un proceso.
- **Notificaciones de aprobación.**
 - Cuando se requiere una, las notificaciones se envían a los aprobadores, lo que les permite aprobar o rechazar el proceso y proporcionar información adicional sobre su acción.
 - Los administradores pueden especificar un período de recurrencia de notificaciones para cada aprobador.
 - Se notifica a todos los autorizadores si ya no se requiere su aprobación debido a que alguien más haya emitido una aprobación antes que ellos.
- **Cambios a los tickets basados en procesos.**
 - El ticket de proceso principal hereda su estado del flujo de trabajo del estado de aprobación y los estados de los tickets secundarios (si corresponde). Si el proceso no contiene ningún ticket secundario, el propietario del proceso recibe todas las aprobaciones, define el estado del proceso como *En curso* y lo puede completar o cancelar.
 - La información relacionada con la aprobación aparece en las páginas de tickets relacionadas con los propietarios y aprobadores de tickets.
 - La información relacionada con la aprobación puede aparecerles de forma opcional a quienes no son propietarios.
 - Se crea un registro del historial para el ticket de un proceso cada vez que se proporciona una aprobación o se excede el tiempo de espera.

Aplicación de parches y seguridad

Esta versión incluye las siguientes características de aplicación de parches y seguridad:

- **Configuración de los valores predeterminados de detección e implementación de parches y del tiempo de espera.** Los administradores pueden modificar los valores predeterminados de la detección e implementación de parches y del tiempo de espera, dentro de un intervalo razonable.
- **Deshabilitar la aplicación de parches de todos los dispositivos.** Se ha agregado la casilla *Todos los dispositivos* a la página *Detalles del programa de parches*. La selección de esta opción impide que los técnicos configuren

de forma accidental un programa de implementación de parches para todos los dispositivos de la red, lo que puede conducir a consecuencias inesperadas, como el reinicio de los sistemas de producción.

- **Programa de aplicación de parches.** Ahora los administradores pueden programar trabajos de aplicación de parches usando un programa deseado, según sea necesario. Puede ejecutar un trabajo de parches un determinado día de la semana dentro de un mes (por ejemplo, el segundo miércoles de cada mes).

Inventario y administración de activos

El inventario y la administración de activos incluyen las siguientes características y mejoras:

- **Archivo de dispositivos** en la página 7
- **Códigos de barras de activos** en la página 7
- **Títulos de catálogo de software asociados con instalaciones administradas** en la página 9
- **Portal de usuario y descargas de software** en la página 9
- **Mejoras en la administración de licencias de software** en la página 9

Archivo de dispositivos

Esta versión incluye las siguientes características de archivado de activos de dispositivos.

- **Archivado de dispositivos.** Los administradores pueden archivar los activos de dispositivos que ya no están en uso. Cuando archiva un activo de dispositivo, ese dispositivo ya no se incluye en el número de licencias de nodos para el dispositivo K1000. Los activos archivados tampoco aparecen en la vista del inventario o los informes. Los activos de dispositivos marcados para archivar se archivan automáticamente después de un período de tiempo configurado, como se especifica en la *Configuración general*. El período predeterminado son tres días. Esto permite que los administradores reviertan que el dispositivo sea marcado para archivado, si es necesario.
- **Características de los informes.** La columna *Archivo* se puede agregar a los informes para indicar si hay algún dispositivo archivado, pendiente para archivarse o que no se haya archivado. La búsqueda avanzada en la página de la lista *Activos* también le permite filtrar el estado *Archivo completo*, *Pendiente* y *No archivado*.
- **Capacidad para archivar dispositivos MIA.** Puede habilitar el archivado de dispositivos de activos MIA (Missing In Action) en la página de configuración de MIA.

Códigos de barras de activos

Esta versión incluye las siguientes características de códigos de barras de activos:

- **Agregar códigos de barras a los activos.** Un código de barras le permite asociar dispositivos o recuperar rápidamente los detalles del dispositivo. Se pueden agregar códigos de barras a los registros de activos por medio del escaneo de la aplicación móvil K1000 GO, mediante su ingreso manual o importación desde un archivo CSV (valores separados por comas). Se admiten formatos de códigos de barras estándar, tales como UPC-A, código 11, UPC-E y otros. Para obtener más información, visite <https://support.software.dell.com/kb/212519>.
- **Capacidad de escanear códigos de barras y administrar activos con la aplicación móvil K1000 GO.**

- La pantalla de inicio también se actualizó e incluye los botones **Scripting**, **Activos**, **Crear Ticket** y **Escanear código de barras**, lo que permite acceder a estas funciones.
- La pantalla de inicio *Activo*, que se agregó a la aplicación móvil K1000 GO en esta versión, contiene el comando **Escanear código de barras** que permite escanear un código de barras y asociarlo con un activo.
- Escanear un código de barras de un activo le permite crear un nuevo activo para hacer un seguimiento del nuevo inventario en cuanto ingresa a la organización. Un activo puede tener uno más códigos de barras, según sea necesario.
- La información de la ubicación, el código de barras y la mesa de servicio aparece en la página de detalles del activo. Es posible acceder a los detalles del inventario del dispositivo desde la página de la lista *Activos*.
- Los técnicos que necesitan encontrar información sobre un activo al que no tienen acceso directo, pueden buscar los activos y ver o editar su información.
- El nivel de permisos de los usuarios controla el acceso a los vínculos con los activos y las funciones de escaneo de los códigos de barras:
 - Los botones **Activos** y **Escanear el código de barras** en la pantalla de inicio principal y el vínculo de la barra lateral **Activos** solo están habilitados para usuarios con permisos de lectura y escritura.
 - La edición de los detalles de activos solo está habilitada para usuarios con permisos de escritura.
 - Los usuarios con acceso oculto no tienen acceso a las funciones de escaneo de los códigos de barras y activos.
- **Capacidades de búsqueda.** Los administradores pueden buscar un código de barras de dispositivo para recuperar rápidamente la información de inventario del activo de dispositivo asociado.
- **Restricciones de acceso.** Los administradores pueden restringir el acceso a las funciones de escaneo de códigos de barras.
- **Características de los informes.** Puede utilizar el asistente para informes para crear informes sobre determinados atributos asociados con un código de barras e identificar los dispositivos que no se analizan durante un período específico.
- **Cargas masivas.** Puede realizar cargas masivas de varios códigos de barras en lugar de ingresar manualmente la información requerida.
- **Seguimiento de cambios.** El aparato hace un seguimiento de los cambios realizados en el campo de código de barras. Los técnicos del dispositivo pueden usar esta información para comprender aspectos importantes como la primera o la última vez que un activo se escanea físicamente.
- **Búsqueda de etiquetas de servicio de Dell.** Los administradores del dispositivo pueden buscar en el campo de código de barras y buscar con el dispositivo tanto la sintaxis de código de barras interno y el valor de la etiqueta de servicio de Dell para encontrar una coincidencia.

Títulos de catálogo de software asociados con instalaciones administradas

Esta versión incluye las siguientes características de catálogo de software e instalaciones administradas:

- **Cargar y asociar archivos con instalaciones administradas o el catálogo de software.** Ahora puede asociar uno o más archivos de instalación con los elementos del catálogo de software. También puede elegir un título del catálogo de software cuando crea una instalación administrada.

Portal de usuario y descargas de software

Esta versión incluye las siguientes características del portal de usuario de descargas de software:

- **Mejoras a las descargas de usuario.**
 - Los administradores pueden ver información adicional sobre los títulos del catálogo de software en la página *Detalle de las descargas del usuario*.
 - Cuando un usuario descarga un título del catálogo de software, el software se implementa en el dispositivo asignado al usuario. Si hay varios dispositivos asignados al usuario, el usuario puede elegir en la lista de los dispositivos que tiene asignados. El dispositivo principal del usuario es la opción predeterminada.
 - La página *Detalle de las descargas del usuario* hace una clara distinción entre tres tipos de descargas de software: *Descargar (software catalogado o no)*, *Instalar (Instalación administrada o Instalación predeterminada)* o *Script*.
 - Las instalaciones del usuario ahora se ponen en la cola de inmediato a través de la acción Ejecutar ahora.
 - La página *Historial de descargas* en la Consola de usuario muestra un estado final de instalación de software de autoservicio y proporciona un historial preciso de softwares instalados por medio de la Consola de usuario.
 - Las solicitudes de instalación de software para un sistema Mac OS® se ejecutan e instalan automáticamente después de descargarse sin interacción del usuario final.
- **Nueva ventana de perfil de usuario.** La ventana *Mi perfil*, a la cual puede acceder haciendo clic en el nombre de usuario en la esquina superior derecha, enumera los dispositivos asignados al usuario.
- **Página Mis dispositivos.** La página *Mi dispositivo* se ha reemplazado con la página *Mis dispositivos*. Esta página muestra una lista de todos los dispositivos asociados con los usuarios y la información de su inventario.

Mejoras en la administración de licencias de software

Esta versión incluye las siguientes características de administración de licencias de software:

Los administradores tienen un mejor control sobre cómo se gestionan los derechos de actualización y degradación para las licencias de software, ya que pueden asociar las versiones y ediciones con estos derechos.

Distribución y scripting

Los componentes de distribución y scripting incluyen las siguientes características y mejoras:

- [Ejecutar ahora para instalaciones administradas](#) en la página 10
- [Mejoras a las descargas del usuario con instalaciones administradas](#) en la página 10

Ejecutar ahora para instalaciones administradas

Los administradores del dispositivo tienen ahora la opción de forzar una instalación administrada para que se ejecute de inmediato en lugar de esperar al siguiente intervalo del inventario, o para forzar manualmente que el inventario se ejecute en los dispositivos seleccionados a fin de distribuir rápidamente el software requerido.

Mejoras a las descargas del usuario con instalaciones administradas

Esta versión incluye las siguientes características de descargas del usuario:

- **Mejoras a la página Detalle de descargas del usuario.** La página *Detalles de las descargas del usuario* le permite elegir una instalación administrada existente. Cuando se selecciona esta opción se indica al proceso de instalación utilizar las opciones de configuración asociadas con la instalación administrada seleccionada.
- **Degradación de las acciones del dispositivo ActiveX® de Microsoft®.** Las acciones del dispositivo ActiveX se eliminan de las acciones de muestra. Cualquier acción de un dispositivo ActiveX existente continuará funcionando (si el navegador lo admite).

Mejoras a la administración del usuario

Esta versión incluye las siguientes características de administración del usuario:

- **Mejoras a la gestión general del usuario.**
 - Un registro de usuario permite mantener varias direcciones de correo electrónico.
 - Se puede configurar una función predeterminada para un usuario.
 - Los administradores del dispositivo pueden buscar un usuario basado en un conjunto extendido de atributos de usuario (como administrador, direcciones de correo electrónico adicionales, asociaciones de dispositivos y nuevos campos personalizados).
 - Los técnicos del dispositivo pueden filtrar la lista de usuarios según sus relaciones jerárquicas y subir o bajar el árbol de relaciones para ver los activos asociados en niveles específicos.
 - Los administradores del dispositivo pueden configurar una importación de LDAP para configurar automáticamente el administrador para un usuario a partir de un atributo dado.
 - Los administradores del dispositivo pueden inspeccionar la jerarquía de usuario para identificar fácilmente y navegar por la estructura corporativa al manipular las escalaciones y solicitudes de aprobación.

- Esta versión permite hacer cambios masivos a los usuarios existentes para modificar rápida y fácilmente los registros del usuario sin tener que realizar varios cambios a los registros individuales.
- El dominio al que pertenece un usuario aparece ahora en las páginas *Usuarios* y *Detalles del usuario*.
- **Página Nuevo perfil de usuario.** La página *Mi perfil* permite que cada usuario cambie rápidamente su contraseña, revise los dispositivos y los activos que tiene asignado y todos los tickets de la mesa de servicio que ha creado. Los usuarios con permisos de nivel administrativo también pueden editar algunos parámetros adicionales, como su nombre, correo electrónico, administrador y configuración regional. También puede acceder a la página *Detalles del usuario* para revisar la información adicional sobre su cuenta y hacer cambios, según sea necesario.
- **Integración del dispositivo/usuario.**
 - Los administradores del dispositivo pueden activar cuentas de usuario para hacer referencia a varios dispositivos y especificar un dispositivo principal.
 - Los técnicos del dispositivo pueden asignar dispositivos a individuos específicos a la hora de asignar los recursos de la empresa. Los administradores del dispositivo pueden asignar masivamente dispositivos a los usuarios.
 - El dispositivo coincide con usuarios con un dispositivo basado en el inventario específico del usuario y sus credenciales de Active Directory. Esto permite que los administradores identifiquen fácilmente a los usuarios de dispositivos específicos.
 - Cuando un dispositivo está asociado con un usuario o un dominio, en que esa información aparece en las páginas *Dispositivos* y *Detalle del dispositivo*.
 - Los administradores del dispositivo pueden utilizar la *Búsqueda avanzada* para identificar los dispositivos con atributos de usuario específico, ubicación y departamento.
 - Los atributos de los dispositivos relacionados con el usuario ahora están disponibles en el asistente para informes.

Mejoras a la ubicación

Esta versión incluye las siguientes características de ubicación:

- **Páginas Nuevas ubicaciones y Detalle de ubicación.**
 - La página con la lista *Ubicación* contiene una lista de sus ubicaciones físicas. Una entidad de ubicación representa un sitio físico que contiene uno o más de sus activos y usuarios. Puede agregar, desplazar o eliminar las entidades de ubicación, según sea necesario.
 - Los administradores del dispositivo pueden buscar determinados atributos de ubicación en la página con la lista *Ubicación* para encontrar rápidamente una ubicación específica.
 - Los administradores del dispositivo pueden realizar actualizaciones masivas a las ubicaciones existentes a fin de hacer cambios en los registros de ubicación de forma rápida y fácil, sin tener modificar las ubicaciones individuales.

- Se ha agregado la página *Detalle de ubicación* en esta versión. Además de un conjunto de campos esperados, como *Nombre*, *Descripción* o *Dirección*, esta página puede incluir campos personalizados. Los administradores pueden ver y editar estos campos personalizados, según sea necesario.
- De forma predeterminada, todos los registros que incluyen un campo de ubicación tienen ese campo como *sin asignar*.
- **Cambios a la página Detalle del dispositivo.** Los técnicos del dispositivo pueden asignar manualmente los dispositivos a ubicaciones específicas en la página *Detalle del dispositivo* durante la asignación de recursos de la empresa.
- **Cambios a las páginas Usuarios y Detalles del usuario.**
 - La página con la lista *Usuarios* muestra la ubicación asociada con cada registro de usuario.
 - Los administradores del dispositivo pueden asociar ubicaciones con usuarios en forma masiva para hacer cambios rápida y fácilmente en los registros del usuario sin tener que modificar los usuarios individuales.
 - La página con la lista *Usuarios* se puede filtrar para mostrar solo los usuarios asociados con ubicaciones específicas.
 - Los técnicos del dispositivo pueden asignar manualmente usuarios a las ubicaciones.
- **Cambios a la página Lista de activos.** La página con la lista *Activos* se puede filtrar para mostrar solo los activos asociados con ubicaciones específicas.

Informes entre dispositivos

Esta versión incluye las siguientes características de informes entre dispositivos:

- **Página Nuevo informe vinculado.**
 - Un informe vinculado contiene información consolidada de varios dispositivos.
 - La lista *Informes vinculados* y el asistente *Editar informe vinculado* se agregaron al systemui K1000.
 - Cuando están habilitados los informes vinculados, cada dispositivo vinculado tiene acceso a la configuración de API de Federation y se le concede la función de administrador, puede ejecutar informes vinculados.
- **Programar informes vinculados.**
 - Los administradores pueden detener la ejecución de un informe en un dispositivo remoto, por ejemplo, si los datos ya no son necesarios o después de detectar un problema con el mismo informe, mientras se ejecuta en otro dispositivo vinculado.
 - Puede programar el dispositivo para ejecutar informes vinculados y enviárselos a los administradores en horas e intervalos determinados.
 - Los administradores pueden programar un informe vinculado para ejecutarse a una hora diferente en cada servidor que es parte del informe vinculado, a fin de capturar un tipo específico de información.

Administración de dispositivos basada en agente

Se ha mejorado la administración de dispositivos basada agente y ahora incluye las siguientes características nuevas:

- **Agente de AMP reemplazado con KONEA.** Antes de esta versión, el agente K1000 se conectaba al servidor mediante el protocolo de AMP, implementado por AMPAgent. En esta versión, el servicio AMPAgent y el protocolo de AMP se han reemplazado con el protocolo y servicio Konea. Konea brinda comunicaciones optimizadas en tiempo real para las operaciones de administración de sistemas. A diferencia de AMPAgent, Konea no necesita puertos propietarios abiertos en la red.

¡ IMPORTANTE: A la vez que garantiza la conexión del agente, Konea está diseñado para adherirse al primer certificado que descarga del dispositivo durante la conexión inicial. Si se restaura o reemplaza el cuadro, o si cualquier otra operación causa que se genere un nuevo certificado para Konea, todas las instancias existentes del agente quedarán huérfanas, ya que no confiarán en el dispositivo con el certificado nuevo.

- **Mejora a las listas negras.** Los usuarios ya no pueden eludir la política de la lista negra simplemente cambiando el nombre de un archivo ejecutable de esta lista. A partir de esta versión, el dispositivo utiliza la descripción del archivo junto con el nombre del archivo original para determinar si un archivo ejecutable es parte de una aplicación de la lista negra.

Administración de dispositivos sin agente

La administración de dispositivos sin agente se ha mejorado para incluir las siguientes características y mejoras:

- [Integración AirWatch](#) en la página 13
- [Inventario y seguimiento de activos de host virtual](#) en la página 14

Integración AirWatch

Esta versión incluye las siguientes características de AirWatch:

- **Características generales de la integración de General AirWatch® de VMware®.**
 - AirWatch es una plataforma de administración de movilidad empresarial que le permite gestionar diferentes tipos de dispositivos. El dispositivo se puede integrar con AirWatch para descubrir dispositivos administrados con AirWatch.
 - Los valores específicos de AirWatch se almacenan en la base de datos de K1000 como parte del inventario de dispositivos.
 - Cada dispositivo de un entorno de AirWatch de terceros requiere una licencia de activos.
 - Los administradores del dispositivo pueden configurar un programa de descubrimiento a fin de incluir dispositivos AirWatch.
 - La comunicación entre una solución AirWatch y el dispositivo se realiza a través de una conexión segura.
- **Recopilación y visualización de datos de AirWatch.**
 - Los técnicos del dispositivo pueden recopilar datos de inventario (sobre dispositivos, aplicaciones, estadísticas de datos/usuario y estado) desde un entorno AirWatch integrado con la visualización de activos e inventario para tener una visión colectiva de los activos de la empresa.
 - Esta característica también le permite ver la información de inventario sobre los dispositivos móviles AirWatch integrados, además de resumir y analizar la información de activos relacionados.

- Para cualquier dispositivo AirWatch visualizado, la interfaz de usuario indica claramente que la información acerca de ese dispositivo provino de una fuente AirWatch.
- Los dispositivos suministrados e inventariados por la integración de AirWatch tienen el grupo de campos *Información móvil* en la página *Detalle del dispositivo* completa con información de ubicación y móvil pertinente, según corresponda.

Inventario y seguimiento de activos de host virtual

El inventario y seguimiento de activos de host virtual se ha mejorado e incluye las siguientes características:

- **Recopilación y visualización de datos de VMware.**
 - El dispositivo puede recopilar información de inventario sobre hosts ESXi a través de un vCenter. Se incluye información de inventario específica de VMware en los detalles del dispositivo, informes y el historial de objetos.
 - Para cada servidor físico, hay disponible una vista del consumo de recursos de cada máquina virtual, lo que le permite predecir rápidamente los posibles cuellos de botella y optimizar los activos sobreutilizados y subutilizados. Los administradores pueden ver e informar sobre las relaciones entre hosts ESXi y sus sistemas huéspedes, lo que mejora la funcionalidad de la administración de activos.
 - Los administradores pueden ver las CPU, la memoria y el uso del almacén de datos de cada máquina virtual, lo que les permite encontrar rápidamente los mayores consumidores de los recursos del host y prevenir problemas relacionados.
 - Los dispositivos VMware inventariados tienen el tipo de activo VMware.
 - Los administradores pueden ajustar el tiempo de espera de conexión para la recopilación de datos de un entorno VMware, ya que algunas conexiones pueden requerir más tiempo.

Supervisión

Receptor de captura SNMP

Esta versión incluye las siguientes características del receptor de captura SNMP:

- **Nuevo receptor de captura SNMP.**
 - El receptor de trampas SNMP alerta a los administradores de las notificaciones SNMP que se envían desde dispositivos SNMP, tales como impresoras, routers, conmutadores, etc.
 - El receptor de capturas lee y analiza todas las capturas recibidas y genera alertas cuando recibe capturas específicas.
 - El receptor de capturas puede utilizar archivos MIB para convertir capturas SNMP en mensajes legibles. Los archivos MIB cargados se respaldan y se ponen disponibles cuando el dispositivo se restaura desde una copia de seguridad.

- Se agrega un nuevo perfil de monitoreo para dispositivos SNMP.
- Los archivos de registro de captura SNMP rotan todas las noches con otros archivos de registro de dispositivo.

Configuración y seguridad

Los aspectos de seguridad y configuración del dispositivo K1000 se han mejorado en esta versión con las siguientes características:

- [Actualización a FreeBSD 10.3](#) en la página 15
- [Seguridad de contraseña raíz](#) en la página 15
- [Compatibilidad con TLS 1.2](#) en la página 15
- [SHA-1 actualizado a SHA-256](#) en la página 16
- [Uso de algoritmos seguros](#) en la página 16

Actualización a FreeBSD 10.3

El dispositivo de administración de sistemas K1000 incluye una serie de componentes de terceros, FreeBSD entre ellos.

En esta versión, FreeBSD está actualizado a la versión 10.3. Esta versión incluye un número de características nuevas, incluida la compatibilidad con el protocolo TLS (Transport Layer Security) 1.2. Para obtener más información, consulte [Compatibilidad con TLS 1.2](#) en la página 15

Seguridad de contraseña raíz

Esta versión incluye las siguientes características de seguridad de la contraseña raíz:

- **Autenticación de dos factores (2FA).** Habilitar el acceso SSH al dispositivo y la creación de un tether le permite al equipo de soporte de KACE iniciar sesión en el back-end del dispositivo K1000 con la contraseña raíz del dispositivo y un token de acceso. Esta característica le permite controlar el acceso al back-end del dispositivo y le proporciona al equipo de soporte de KACE tokens de acceso, cuando sea necesario. Cada token se puede usar solo una vez. Cada vez que se utiliza un token, este caduca y se debe reemplazar. Debe mantener una lista actualizada de tokens.
- **Generación de token 2FA.** Los tokens se proporcionan en el *Asistente de configuración inicial*. Se pueden ver y volver a generar mediante la página *Autenticación de dos factores* en el dispositivo Consola del sistema.

Compatibilidad con TLS 1.2

A partir de esta versión, el dispositivo de administración de sistemas de K1000 es compatible y prefiere la versión 1.2 del protocolo de seguridad de la capa de transporte (TLS) en los portales web del dispositivo y la comunicación de clientes.

Las versiones 1.1 y 1.0 también son compatibles, pero es preferible usar la versión 1.2.

SHA-1 actualizado a SHA-256

Las versiones anteriores del dispositivo K1000 utilizaban SHA-1 (Algoritmo de Hash Seguro 1).

Se considera que esta versión no está actualizada y es potencialmente insegura. En esta versión, el dispositivo utiliza SHA-256.

Uso de algoritmos seguros

A partir de esta versión, el dispositivo utiliza un conjunto de algoritmos seguros más recientes, como el protocolo TLS (consulte [Compatibilidad con TLS 1.2](#) en la página 15), ECDHE (Diffie-Hellman de curva elíptica), ECDSA (Algoritmo de firma digital de curva elíptica), AES-256 (Estándar de cifrado avanzado con un tamaño clave de 256 bits), GCM (Modo de Galois/contador) y SHA-384.

Compatible con API

En esta versión, se han agregado las siguientes API:

- **API de instalación administrada.** La API de instalación administrada permite acceder a las instalaciones administradas, las máquinas y los archivos y actuar en ellos.
- **API de administración de activos.** La API de administración de activos le permite ver, crear, actualizar y eliminar activos.
- **API de inventario.** La API de inventario le permite administrar solicitudes de inventario en una máquina con K1000.
- **API de scripting.** La API de scripting le permite administrar solicitudes de inventario en un dispositivo K1000.

Problemas resueltos

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

Tabla 1. Problemas generales resueltos

Problema resuelto	Id. del problema
Los campos personalizados de la mesa de servicio no son visibles en los resultados de las consultas SQL.	ESMAS-3344
En Microsoft Windows® 10, Microsoft cambió la manera de informar la versión del sistema operativo. Las actualizaciones más importantes, como Windows 10 Anniversary Edition, tienen nuevos números de compilación, pero informan el mismo nombre. Hay algunas áreas donde se pueden seleccionar versiones específicas de sistemas operativos: <ul style="list-style-type: none">• <i>Página Detalles de scripts</i>• <i>Página Detalles del software</i>• <i>Ajustes de Wake-on-LAN</i>	ESMEA-2550

Problema resuelto	Id. del problema
Si anteriormente eligió una versión Windows 10, revise su selección para asegurarse de que todas las compilaciones de Windows 10 estén seleccionadas.	
La fecha del <i>Ticket modificado</i> podría ser incorrecta si los acuerdos de nivel de servicio (SLA) están habilitados.	K1-18730
Un mensaje de error de una copia de respaldo era incorrecto si las copias estaban desactivadas.	K1-18688
No se podían ejecutar scripts con credenciales de usuario, a menos que el usuario iniciara sesión en la máquina del agente.	K1-18674
En Microsoft Windows®, la implementación de parches no eliminaba los archivos temporales.	K1-18649
El menú <i>Vista del catálogo de parches por</i> contenía la opción del sistema operativo Windows 10 en una ubicación incorrecta.	K1-18606
Solo un comentario de un propietario se podía enviar al remitente si el cambio de estado se realizaba al mismo tiempo y se guardaban los cambios.	K1-18595
Un agente de Windows que ejecutaba varios archivos <code>explorer.exe</code> causaba alertas de usuario duplicadas.	K1-18591
Los <i>Recuentos de parches instalados y faltantes</i> eran incorrectos en la página del <i>catálogo</i>	K1-18504
Es posible que los archivos de registro del agente sobrescriban los archivos de registro previamente rotados.	K1-18472
SCAP (Protocolo de automatización de contenido de seguridad) no procesaba resultados cuando el nombre de archivo de referencia contenía más de 50 caracteres.	K1-18471
Se informaba un error al exportar los resultados de la búsqueda del software un archivo CSV (valores separados por comas).	K1-18425
Cuando se agregaba un ticket principal, solo era posible buscar los primeros 4 octetos.	K1-18367
Durante la implementación de un script, se podía generar un error por la falta de una etiqueta.	K1-18256
La configuración del <i>retraso del reinicio</i> de los parches no se respetaba cuando se excedía el tiempo de espera de una alerta de reinicio del parche.	K1-18153
Se podía informar un error cuando un mensaje o archivo adjunto de correo electrónico contenía un <i>emoji</i> .	K1-18111
Un campo de activos personalizado de un dispositivo informático no se podía vincular correctamente en la página <i>Detalles de activos</i> .	K1-18091
Un informe de inventario informático se ordenaba de forma incorrecta por tiempo de actividad actual.	K1-17803

Problema resuelto	Id. del problema
La configuración del estado de un ticket en la página con la lista <i>Tickets</i> no funcionaba correctamente.	K1-17396
No se podía establecer una acción de tiempo de espera cuando se configuraba un programa de actualización de Dell.	K1-17395
Los activos se duplicaban en los resultados de búsqueda global.	K1-17364
Los archivos adjuntos de la mesa de servicio que contenían el símbolo "#" no se gestionaban correctamente	K1-17363
Los correos electrónicos a la mesa de servicio omitían las imágenes incrustadas si había también archivos adjuntos	K1-17362
En la lista de archivos del ticket, se podía informar un error cuando se realizaba una búsqueda avanzada por <i>Creado</i> .	K1-17252
Cuando se veían los tickets por propietario, los tickets cerrados se incluían en los resultados.	K1-17235
Con el SSO activado, solo era posible acceder al recurso compartido de Samba con su dirección IP.	K1-17170
No se aplicaba un límite de longitud de las alertas asociadas con los scripts, lo que impedía ver las alertas.	K1-17155
La búsqueda avanzada de activos informáticos no completó la columna del nombre de los propietarios.	K1-17154
El informe de garantía Dell creado con el asistente para informes arrojó duplicados y números de serie junto con información de la garantía incorrectos.	K1-16250
Las IP privadas no se podían asociar con un activo.	K1-12370

Problemas conocidos

La siguiente es una lista de problemas, incluidos aquellos atribuidos a productos de terceros, conocidos al momento del lanzamiento de la versión.

Tabla 2. Problemas generales

Problema conocido	Id. del problema
Un propietario de activos solo se puede establecer <i>Sin asignar</i> en la lista <i>Activos</i> o <i>Dispositivos</i> .	K1-18955
El monitoreo de Microsoft Windows® Server 2016 todavía no es totalmente compatible.	K1-18929
La página <i>Programa de parches</i> enumera los dispositivos que no son compatibles con parches en la lista <i>Tareas de parches</i> (por ejemplo, Linux®).	K1-18926

Problema conocido	Id. del problema
La opción <i>Desactivar la detección de dispositivos duplicados</i> en la página <i>Configuración del agente</i> no es compatible con el agente 7.0.	K1-18923
Los conteos de instalación del catálogo de software pueden ser incorrectos después de que se hace una restauración. Solución alternativa: Para actualizar el conteo, seleccione <i>Forzar actualización</i> .	K1-18910
Los cambios de <i>Configuración del inventario basado en SNMP</i> no se reflejan adecuadamente en el historial de objetos.	K1-18909
La ayuda en línea para la autenticación de dos factores es errónea. Para obtener más información, consulte Seguridad de contraseña raíz en la página 15.	K1-18901
Si se inicia un informe de ubicación desde la página con la lista <i>Ubicación</i> , solo se enumeran las ubicaciones de nivel superior. Solución alternativa: Para un informe completo que incluya niños, utilice el <i>Asistente para informes</i> en Informes.	K1-18882
Los cambios de contraseña de usuario no se registran en el historial de objetos.	ESMP-4423
Al ejecutar los <i>servicios</i> de utilidad de diagnóstico, <code>z.kmsgx.sh</code> se indica como INCORRECTO erróneamente, si la configuración del sistema <i>Habilitar asistencia previa al agente 7.0</i> está desmarcada.	ESMP-4388
Si se eliminan los aprobadores de tickets, cualquier creación subsiguiente de tickets mediante ese proceso fallará, pero aún se creará el ticket.	ESMAS-3291
Los usuarios de tabletas Android™ de Google® que ejecutan una versión anterior del SO (inferior a 5.1) pueden no recibir notificaciones de inserciones en su tableta.	ESMAS-3237

Requisitos del sistema

La versión mínima necesaria para instalar K1000 7.0 es 6.4 SP3 (6.4.120822). 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 en K1000 6.3 o inferior, inicie sesión en Consola del administrador, y, a continuación, haga clic en **Acerca de K1000** en la parte inferior izquierda de la página.

NOTA: En la versión 7.0, el vínculo *Acerca de K1000* se encuentra en el panel de *Ayuda*. Haga clic en el signo de interrogación situado en la esquina superior derecha de la página y luego haga clic en *Acerca de K1000* en la esquina inferior derecha de la ventana que aparece.

Antes de actualizar o instalar la versión 7.0, verifique que su sistema cumpla con los requisitos mínimos. Estos requisitos están disponibles en las especificaciones técnicas del K1000.

- Para dispositivos físicos: Ir a <http://documents.software.dell.com/k1000-systems-management-appliance/7.0/technical-specifications-for-physical-appliances/>.
- Para dispositivos virtuales: Ir a <http://documents.software.dell.com/k1000-systems-management-appliance/7.0/technical-specifications-for-virtual-appliances/>.
- Para K1000 como servicio: Ir a <http://documents.software.dell.com/k1000-systems-management-appliance/7.0/technical-specifications-for-k1000-as-a-service/>.

Licencia de producto

Si actualmente posee una licencia de producto para el K1000, no se requiere una licencia adicional.

Si es la primera vez que utiliza K1000, consulte la guía de configuración del dispositivo para ver los detalles de licencias del producto. Vaya a [Más recursos](#) en la página 23 para ver la guía adecuada.

- NOTA:** Las licencias del producto para la versión 7.0, se pueden usar solamente en dispositivos K1000 que ejecutan la versión 6.3 o posterior. Las licencias de la versión 7.0 no se pueden utilizar en dispositivos que ejecutan versiones anteriores del K1000, como 6.0.

Instrucciones de instalación

Puede aplicar el Service Pack mediante una actualización anunciada o mediante la carga y ejecución manual de un archivo de actualización. Para obtener instrucciones, consulte los siguientes temas:

- [Preparación para la actualización](#) en la página 20
- [Actualización del servidor K1000 mediante una actualización anunciada](#) en la página 21
- [Carga y ejecución manual de una actualización](#) en la página 21
- [Tareas posteriores a la actualización](#) en la página 22

Preparación para la actualización

Antes de comenzar

Antes de actualizar el servidor K1000, siga estas recomendaciones:

- **Verifique la versión del servidor K1000:** La versión mínima necesaria para instalar esta edición es 6.4.120822. Si su dispositivo ejecuta una versión anterior, deberá actualizarla a la versión indicada antes de continuar con la instalación.


- NOTA:** En la versión 7.0, el vínculo *Acerca de K1000* se encuentra en el panel de *Ayuda*. Haga clic en el signo de interrogación situado en la esquina superior derecha de la página y luego haga clic en *Acerca de K1000* en la esquina inferior derecha de la ventana que aparece.

- **Realizar 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 K1000 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 del K1000*, <http://documents.software.dell.com/kace-k1000/7.0/administrator-guide/>.

Actualización del servidor K1000 mediante una actualización anunciada

Puede actualizar el servidor K1000 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 K1000 de forma manual durante una actualización.

Procedimiento

- 1 Realice una copia de respaldo de la base de datos y los archivos. Para ver las instrucciones, consulte la *Guía para el administrador de K1000*, <http://documents.software.dell.com/kace-k1000/7.0/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 systemui de K1000: `http://K1000_hostname/system` o seleccione **Sistema** en la lista desplegable de la esquina superior derecha de la página y, a continuación, 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**.
Se aplica la versión 7.0 y el servidor K1000 se reinicia varias veces. El progreso aparece en la consola del administrador.

Carga y ejecución manual de una actualización

Si cuenta con un archivo de actualización de Dell KACE, puede cargarlo manualmente para actualizar el servidor K1000.

 **PRECAUCIÓN:** Nunca reinicie el servidor K1000 de forma manual durante una actualización.

Procedimiento

- 1 Realice una copia de respaldo de la base de datos y los archivos. Para ver las instrucciones, consulte la *Guía para el administrador de K1000*, <http://documents.software.dell.com/kace-k1000/7.0/administrator-guide/>.
- 2 Con sus credenciales de inicio de sesión de cliente, inicie sesión en el sitio web de Dell Software en <https://support.software.dell.com/k1000-systems-management-appliance/download-new-releases>, descargue el archivo `.kbin` del servidor K1000 para la versión 7.0 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 7.0 y el servidor K1000 se reinicia varias veces. La Consola del administrador no estará disponible hasta que se haya completado la actualización. El progreso aparece en la ventana del navegador y en la Consola del administrador.

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 K1000.

Procedimiento

- 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 systemui de K1000: `http://K1000_hostname/system` o seleccione **Sistema** en la lista desplegable de la esquina superior derecha de la página y, a continuación, haga clic en **Ajustes**.
- 2 Haga clic en el signo de interrogación situado en la esquina superior derecha de la página y luego haga clic en **Acerca de K1000** en la esquina inferior derecha de la ventana que aparece para verificar la versión actual.


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.

Procedimiento

- 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 systemui de K1000: `http://K1000_hostname/system` o seleccione **Sistema** en la lista desplegable de la esquina superior derecha de la página y, a continuación, 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.** Fortalecer la contraseña de root (2FA) y acceder al dispositivo.
 - a En la Consola del sistema, haga clic en **Configuración > Soporte**.
 - b En la página *Soporte*, en *Herramientas de solución de problemas*, haga clic en **Autenticación de dos factores**.
 - c En la página *Soporte de autenticación de dos factores*, haga clic en **Reemplazar clave secreta**.
 - d Registre los tokens y conserve esta información en un lugar seguro.
Si se establece un tether, se debe proporcionar un token al soporte de KACE. Para obtener más información, consulte [Seguridad de contraseña raíz](#) en la página 15.

Más recursos

Podrá encontrar información adicional a través de los siguientes recursos:

- Documentación del producto en línea (<http://documents.software.dell.com/ProductsAZ.aspx#K>)
 - **Especificaciones técnicas:** Información sobre los requisitos mínimos para instalar o actualizar a la última versión del producto.
Para dispositivos físicos: Ir a <http://documents.software.dell.com/k1000-systems-management-appliance/7.0/technical-specifications-for-physical-appliances/>.
Para dispositivos virtuales: Ir a <http://documents.software.dell.com/k1000-systems-management-appliance/7.0/technical-specifications-for-virtual-appliances/>.

Para K1000 como servicio: Ir a <http://documents.software.dell.com/k1000-systems-management-appliance/7.0/technical-specifications-for-k1000-as-a-service/>.

- **Guías de configuración:** Instrucciones para configurar dispositivos físicos y virtuales. Ir a <https://support.software.dell.com/k1000-systems-management-appliance/release-notes-guides> para ver la documentación de la última versión.
- **Guía para el administrador:** Instrucciones para usar el dispositivo. Ir a <http://documents.software.dell.com/k1000-systems-management-appliance/7.0/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 Estados 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 Dell

Dell escucha a sus clientes y les proporciona la tecnología innovadora, las soluciones y los servicios empresariales que valoran y en los que confían en todo el mundo. Para obtener más información, visite <http://software.dell.com>.

Comuníquese con Dell

Para ventas u otras consultas, visite <http://software.dell.com/company/contact-us.aspx> o llame al 1-949-754-8000.

Recursos del soporte técnico

El soporte técnico se encuentra disponible para los clientes que han comprado software de Dell con un contrato válido de mantenimiento y para los clientes que poseen versiones de prueba. Para acceder al portal de soporte, vaya a <https://support.software.dell.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. Además, el portal de soporte proporciona acceso directo a los ingenieros de soporte de productos mediante un sistema de solicitudes de servicio en línea.

El portal de soporte le permite:


- Crear, actualizar y administrar las solicitudes de servicio (casos).
- Consultar artículos de la base de conocimientos.
- Obtener notificaciones de productos.
- Descargar software. Para software de prueba, vaya a <http://software.dell.com/trials>.
- Ver videos de procedimientos.


- Participar en debates de la comunidad.
- Hablar por chat con un ingenieros de soporte.

Copyright© 2016 Dell Inc. All rights reserved.

This product is protected by U.S. and international copyright and intellectual property laws. Dell™, the Dell logo, KACE, Latitude, OptiPlex, PowerEdge, PowerVault, and Precision are trademarks of Dell Inc. Adobe, Acrobat, and Reader are registered trademarks of Adobe Systems Incorporated in the United States and/or other countries. AMD-V is a trademark of Advanced Micro Devices, Inc. Apache is a trademark of The Apache Software Foundation. Apple, iPad, iPhone, iPod touch, Mac, Macintosh, Mac OS, OS X, and Safari are trademarks of Apple Inc., registered in the U.S. and other countries. App Store is a service mark of Apple Inc. Ubuntu is a registered trademark of Canonical Ltd. Cisco is a registered trademark of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. Facebook is a registered trademark of Facebook Inc. FreeBSD is a registered trademark of The FreeBSD Foundation. Google, Android, Chrome, Chromebook, and Google Play are trademarks of Google Inc. Intel, vPro, and Xeon are trademarks of Intel Corporation in the U.S. and/or other countries. IBM and AIX are registered trademarks of International Business Machines Corporation. Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both. McAfee and VirusScan are registered trademarks of McAfee, Inc. in the United States and other countries. LinkedIn is registered trademark of LinkedIn Corporation. Lumension is a registered trademark of Lumension Security, Inc. Microsoft, Access, ActiveX, Active Directory, Excel, Hyper-V, Internet Explorer, Microsoft Edge, Visual Studio, Windows, Windows Server, and Windows Vista are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Mozilla and Firefox are registered trademarks of the Mozilla Foundation. NETGEAR is a registered trademark of NETGEAR, Inc. and/or its subsidiaries in the United States and/or other countries. Novell and SUSE are registered trademarks and SLES is a trademark of Novell, Inc. in the United States and other countries. Oracle, Java, MySQL, and Solaris are trademarks or registered trademarks of Oracle and/or its affiliates. CentOS, Fedora, Red Hat, and Red Hat Enterprise Linux are registered trademarks or trademarks of Red Hat, Inc. in the U.S. and other countries. Debian is a registered trademark of Software in the Public Interest, Inc. DameWare is a registered trademark of SolarWinds Worldwide, LLC. Symantec and Ghost are trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Twitter is a registered trademark of Twitter, Inc. UNIX is a registered trademark of The Open Group in the United States and other countries. VeriSign is a registered trademark of VeriSign, Inc. and its subsidiaries in the United States and in foreign countries. VMware, ESX, ESXi, Fusion, Player, vCenter Converter, vCenter Lab Manager, vCloud, vSphere, Workstation, and AirWatch are registered trademarks or trademarks of VMware, Inc. in the United States and/or other jurisdictions. VNC is a registered trademark of RealVNC Ltd. in the U.S. and in other countries. Wi-Fi is a registered trademark of Wireless Ethernet Compatibility Alliance, Inc. WinZip is a registered trademark of Corel Corporation and/or its subsidiaries in Canada, the United States and/or other countries. Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Dell disclaims any proprietary interest in the marks and names of others.

Legenda

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

 **ADVERTENCIA:** Un ícono de ADVERTENCIA indica la posibilidad de sufrir daño a la propiedad, heridas personales o la muerte.

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

Notas de la versión del dispositivo de administración de sistemas K1000 KACE

Actualizado: noviembre de 2016

Versión del software: 7.0