Kaseya 2

Antivirus

Guía del usuario

Versión 7.0

Español

Septiembre 16, 2014

Agreement

The purchase and use of all Software and Services is subject to the Agreement as defined in Kaseya's "Click-Accept" EULATOS as updated from time to time by Kaseya at http://www.kaseya.com/legal.aspx. If Customer does not agree with the Agreement, please do not install, use or purchase any Software and Services from Kaseya as continued use of the Software or Services indicates Customer's acceptance of the Agreement."

Contenido

Introducción a Antivirus

Antivirus (KAV) proporciona seguridad de extremo con el antivirus Kaspersky para las máquinas administradas. **Antivirus** garantiza protección contra amenazas conocidas y nuevas para la computadora. Cada tipo de amenaza se procesa con componentes de aplicación independientes, cada uno de los cuales se puede habilitar o deshabilitar por medio del perfil de configuración. Los perfiles de configuración le permiten aplicar rápidamente diferentes tipos de soluciones de **Antivirus** a varias máquinas al mismo tiempo. **Antivirus** se puede instalar en forma independiente de **Endpoint Security** o **AntiMalware**.

Antivirus incluye las siguientes herramientas de protección:

- Componentes de protección residente en la memoria para lo siguiente:
  - Servidores y estaciones de trabajo, con una licencia independiente para cada uno
  - Archivos y datos personales
  - Sistema
  - Red
- Análisis de virus periódicos y programados de archivos, carpetas, unidades, áreas o de toda la computadora.
- Actualizaciones de clientes de **Antivirus** y sus componentes, así como de las bases de datos de definiciones de **Antivirus** que se usan para buscar programas malintencionados.
- Tablero de estado para todas las máquinas administradas que cuentan con **Antivirus**.
- Una página de detecciones para todas las amenazas de virus que **Antivirus** no resuelve automáticamente.
- Alertas administradas con el módulo.
- Comprobación del Centro de seguridad de Windows.
- Opción Actualización lista, que permite identificar y actualizar clientes de **Antivirus** desactualizados.
- La administración de directivas puede administrar la asignación de perfiles de **Antivirus**.
- Procedimientos de agente específicos que se proporcionan con **Antivirus** y que lo ayudan a implementar previamente el paquete de instalación de **Antivirus** en los extremos, lo que reduce el ancho de banda requerido. Consulte el **artículo de la Base de conocimientos** *(https://helpdesk.kaseya.com/entries/34261116)*.
- **Personalización de la interfaz de usuario del cliente de Antivirus en el extremo** *(https://helpdesk.kaseya.com/entries/32410117)*.

> **Nota:** **Antivirus** 6.5 admite tanto la versión 10 de Kaspersky como la versión 6 heredada, para extremos de estación de trabajo y servidor. Se proporcionan perfiles específicos para administrar cada tipo de máquina. **Antivirus** *6.5 no admite extremos de la versión 2010 de Kaspersky.* **Antivirus** 6.5 sólo instala o actualiza extremos en la versión 10 de Kaspersky. *Se recomienda ampliamente la versión 10.* Puede actualizar un extremo de la versión 6 de Kaspersky a la versión 10 con el botón **Actualizar versión del cliente**, en Instalar, del Panel de control.

Caché de LAN

La memoria caché de LAN permite que varias máquinas recuperen los mismos archivos desde una máquina LAN local en lugar de descargarlos de manera reiterada deKaseya Server. Esto reduce los problemas de ancho de banda de la red. Los archivos que se descargan para los extremos de **Antivirus** —los paquetes de instalación, las definiciones de actualizaciones y antivirus— usan la memoria caché de LAN automáticamente si ya está configurada para dichos extremos. No se necesita configuración adicional en **Antivirus**. Para obtener más información, consulte **Memoria caché de LAN** *(http://help.kaseya.com/webhelp/ES/VSA/7000000/index.asp#9328.htm)* en Agente.

Nota: Consulte **Requisitos del sistema para Antivirus** *(página 3)*.

Funciones	Descripción
Máquinas *(página 3)*	Permite instalar el software Antivirus en las máquinas seleccionadas y desinstalarlo de ellas, y proporciona una vista detallada del estado de Antivirus de cualquier máquina seleccionada.
Tableros *(página 13)*	Muestra una vista de tablero del estado de todas las máquinas que tienen instalado Antivirus.
Detecciones *(página 14)*	Muestra las amenazas de virus sobre las que puede actuar.
Perfiles *(página 15)*	Permite administrar los perfiles de Antivirus que se asignan a los ID de máquinas.
Alertas *(página 25)*	Permite administrar las alertas de los módulos Antivirus.

Requisitos del módulo Antivirus

Kaseya Server

- El módulo Antivirus 7.0 requiere el VSA 7.0.

Requisitos de agente

- KAV 7.0 requiere la versión de agente 7.0.0.0 o una versión superior.

Requisitos para todas las estaciones de trabajo administradas

- CPU de 1 GHz o superior
- 1 GB de RAM disponible
- 1 GB de espacio libre en la unidad de disco duro
- Compatibilidad con Microsoft Windows XP, Vista, 7, 8, 8.1
- Microsoft Windows Installer 3.0
- Consulte **Versión 10.x del antivirus Kaspersky para estaciones de trabajo Windows** *(http://support.kaspersky.com/kes10wks#requirements)* para obtener una lista completa de los requisitos del sistema de las estaciones de trabajo.

Requisitos para todos los servidores administrados

- Se admite Server 2003, 2003 R2, SBS 2003 R2, 2008 SP1, SBS 2008 SP1, 2008 R2 SP1, SBS 2011, 2012, 2012 R2.
- Sólo se admite el SO de SBS 2011. No incluye los servidores de correo electrónico Exchange que hospeda SBS 2011.
- Consulte **Versión 10.x del antivirus Kaspersky para servidores Windows** *(http://support.kaspersky.com/kes10fs#requirements)* para obtener una lista completa de los requisitos del sistema de servidores, *incluidos los del paquete de servicios para cada SO*.

> **Nota:** Consulte **Requisitos generales del sistema** *(http://help.kaseya.com/webhelp/ES/VSA/7000000/reqs/index.asp#home.htm)*.

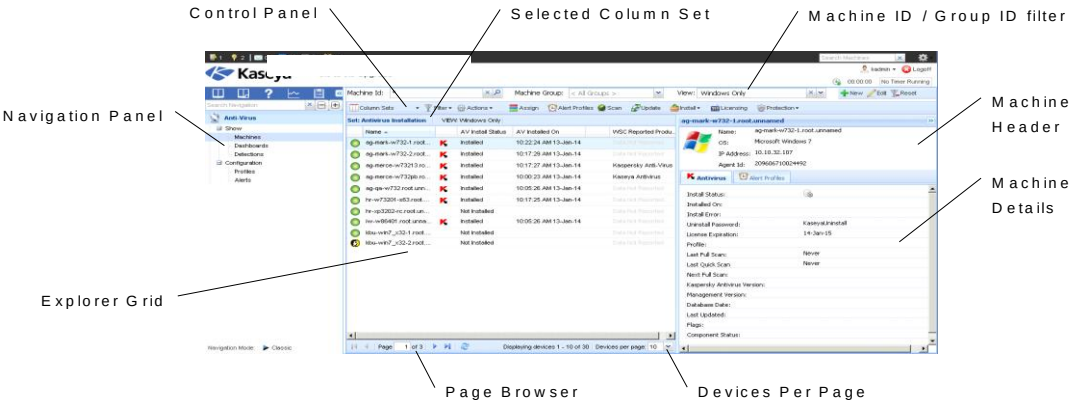
Máquinas

Antivirus > Mostrar > Máquinas

En la página **Máquinas**, se puede instalar y desinstalar el software **Antivirus** en las máquinas seleccionadas. En esta misma página se proporciona una vista detallada del estado de **Antivirus** de cualquier máquina seleccionada.

Diseño de página

La composición de la página **Máquinas** *(página 3)* comprende los siguientes elementos de diseño:



- **Panel de navegación**: se usa para navegar a las páginas dentro del módulo **Antivirus**.
- **Cuadrícula de explorador**: todas las máquinas administradas en el VSA se incluyen en este panel.
  - **Explorador de páginas**: si se muestra más de una página de dispositivos, se pueden avanzar o retroceder páginas.
  - **Filas por página**: establece la cantidad de dispositivos que se muestran por página (10, 30 o 100).
- **Filtro ID de máquina/ID de grupo**: filtra la lista de los ID de máquina que se incluyen en la **Cuadrícula de explorador**.
- **Panel de control**: ejecuta tareas, ya sea para toda la **Cuadrícula de explorador** o para una única máquina seleccionada.
- **Panel de detalles**: en este panel, se muestran las propiedades y el estado de una única máquina.
  - **Encabezado**: identifica la máquina seleccionada en la **Cuadrícula de explorador**.
  - **Antivirus**: muestra un resumen del estado de **Antivirus** de una máquina.
  - **Perfiles de alerta**: se enumeran los perfiles de alerta asignados a una máquina.

Cuadrícula de explorador

En la **Cuadrícula de explorador** de la página **Máquinas** *(página 3)*, se enumeran todas las máquinas que actualmente tienen instalado **Antivirus** *y* que se incluyen en el **filtro ID de máquina/ID de grupo** *(http://help.kaseya.com/webhelp/ES/VSA/7000000/index.asp#209.htm)*.

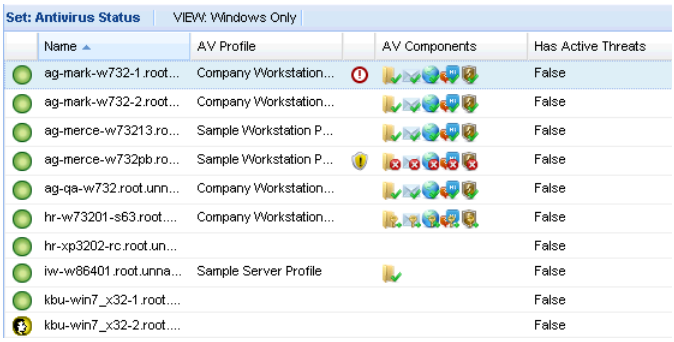
Nota: La única excepción se da cuando está seleccionada la opción `Antivirus Installation`. En este caso, se muestran todas las máquinas que se incluyen en el filtro ID de máquina/ID de grupo.

- El *conjunto de columnas* que se muestra está determinado por la selección de **conjunto de columnas** en el **Panel de control** *(página 6)*. El conjunto de columnas seleccionado se muestra en la barra que se encuentra inmediatamente sobre la **Cuadrícula de explorador**.

  Nota: Consulte **Columnas de Antivirus** *(página 9)* para obtener una descripción de todas las columnas disponibles para mostrarse en *cualquier* conjunto de columnas de la **Cuadrícula de explorador**.

- La opción de avanzar página permite visualizar varias páginas de máquinas.

- La opción de máquinas por página permite establecer la cantidad de filas en cada página.



Íconos de columna

	Definiciones desactualizadas
	Reinicio requerido
	Análisis completo en curso
	Licencia caducada
	La configuración de extremo no cumple los requisitos del perfil
	Asignación pendiente
	Habilitación pendiente
	Deshabilitación pendiente
	Análisis pendiente
	Desinstalación pendiente
	Verificación Pendiente
	Instalación Pendiente
	Actualización pendiente
	Falló la Instalación
	Instalación correcta
	Endpoint Security está instalado en esta máquina.

Convenciones de íconos de componentes

Si se mantiene el mouse sobre un ícono de componente, se muestra información sobre herramientas que describe el estado del componente. En general, se usan las siguientes convenciones de íconos de componentes.

Estado	Tipo de ícono mostrado	Ejemplo: Íconos de protección de archivo
Deshabilitado	X gris	
Falla	signo de exclamación	

	amarillo	
En ejecución/habilitado	marca de verificación verde	
Iniciando	llave con flecha verde	
Detenido	X roja	
Deteniendo	llave con signo menos rojo	

Panel de control

El **Panel de control** que se encuentra en la parte superior de la página **Máquinas** *(página 3)* ejecuta tareas para toda la **Cuadrícula de explorador** *(página 4)* o para una única máquina seleccionada.

Conjuntos de columnas

Cuando se selecciona un conjunto de columnas, se muestra un conjunto de columnas predefinido.

- **Modificar columnas**: personaliza el conjunto de columnas que se muestra en *cualquier* conjunto de columnas.

  Nota: Consulte **Columnas de Antivirus** *(página 9)* para obtener una descripción de todas las columnas disponibles para mostrarse en *cualquier* conjunto de columnas de la **Cuadrícula de explorador**.

- **Instalación de Antivirus**: muestra las columnas de instalación de **Antivirus** en la **Cuadrícula de explorador** *para todas las máquinas con agente*.
- **Estado de Antivirus**: muestra las columnas de estado en la **Cuadrícula de explorador** para todas las máquinas con agente *que tienen un cliente de* **Antivirus** *instalado.*

Filtro

Filtra la lista de filas que se muestran por software instalado, actualización recomendada, reinicio requerido, definiciones desactualizadas, máquina que no cumple los requisitos del perfil, versión más reciente instalada o clientes no compatibles.

Nota: El filtro `Upgrade RecommendedAntivirus` lo ayuda a identificar cuáles son las máquinas que cumplen con los requisitos para la actualización a la versión más reciente. Para actualizar, realice la instalación sobre una instalación existente de **Antivirus**.

Acciones

- **Cancelar acción pendiente**: cancela las acciones pendientes en las máquinas seleccionadas.
- **Reiniciar**: reinicia las máquinas seleccionadas.

Asignar

Asigna un perfil de configuración de **Antivirus** a las máquinas seleccionadas. Se pueden seleccionar y asignar estaciones de trabajo y servidores al mismo tiempo No es necesario seleccionar sólo estaciones de trabajo o sólo servidores. A las estaciones de trabajo se les asigna el perfil de estación de trabajo seleccionado. A los servidores se les asigna el perfil de servidor seleccionado. Consulte **Perfiles** *(página 15)* para obtener más información.

Perfiles de alerta

Asigna o quita un perfil de alerta para las máquinas seleccionadas. En la pestaña **Perfiles de alerta** en el

Panel de detalles *(página 11)*, se muestran todos los perfiles asignados a una máquina.

Explorar

Programa un análisis de **Antivirus** en las máquinas seleccionadas.

- **Fecha de inicio**: la fecha de inicio del análisis.
- **Hora**: la hora de inicio del análisis.
- **Período de distribución**: reprograma varios análisis de manera uniforme a lo largo de un período de distribución en un plazo inferior a la cantidad de períodos especificados, para distribuir el tráfico de red y la carga del servidor.

Existen dos tipos de análisis para **Antivirus**:

- **Análisis completo**: un análisis minucioso de todo el sistema. Los siguientes objetos se analizan de manera predeterminada: memoria del sistema, programas cargados en el inicio, copia de seguridad del sistema, bases de datos de correo electrónico, unidades de disco duro, medios de almacenamiento extraíbles y unidades de red.
- **Análisis de área crítico/rápido**: análisis antivirus de objetos de inicio del sistema operativo. El análisis rápido pasó a llamarse análisis crítico a partir de la versión 10.x de **Antivirus**.

Actualizar

Programa una actualización en las máquinas seleccionadas con las definiciones de **Antivirus** más recientes.

- **Fecha de inicio**: la fecha de inicio de la actualización.
- **Hora**: la hora de inicio de la actualización.
- **Período de distribución**: reprograma varias actualizaciones de manera uniforme a lo largo de un período de distribución en un plazo inferior a la cantidad de períodos especificados, para distribuir el tráfico de red y la carga del servidor.

Instalar

- **Instalar o actualizar Antivirus**: instala o actualiza el cliente de **Antivirus** en las máquinas seleccionadas.
  - **Selección de perfil**: se pueden seleccionar e instalar estaciones de trabajo y servidores al mismo tiempo. A las estaciones de trabajo se les asigna el perfil de estación de trabajo seleccionado. A los servidores se les asigna el perfil de servidor seleccionado. Sólo se pueden seleccionar perfiles de estaciones de trabajo y servidores de las versiones 10.x.
  - **Permitir reinicio**: si está seleccionada, permite un reinicio si es necesario. Para las estaciones de trabajo solamente, se requiere reiniciar después de la instalación.
  - **Opciones avanzadas**: haga clic para visualizar las siguientes opciones.
    - ✓ **Fecha y hora de inicio**: la fecha y la hora de inicio de la instalación.
    - ✓ **Período de distribución**: reprograma varias instalaciones de manera uniforme a lo largo de un período de distribución en un plazo inferior a la cantidad de períodos especificados, para distribuir el tráfico de red y la carga del servidor.
    - ✓ **Preguntar antes de instalar**: si está seleccionada, se lleva a cabo la instalación solamente si el usuario inició sesión y acuerda proseguir.
    - ✓ **Omitir si la máquina está desconectada**: si está seleccionada, se omite la instalación si la computadora está desconectada en el momento en que está programada la instalación. Si no está activada, la instalación se lleva a cabo cuando la computadora vuelve a conectarse.
    - ✓ **Contraseña**: establece una contraseña personalizada para usar con esta máquina. Las contraseñas evitan que se produzca una desinstalación o reconfiguración no autorizadas. Deje esta opción vacía para usar la contraseña predeterminada. La contraseña se muestra en el **Panel de detalles** *(página 11)*. Las contraseñas deben ser alfanuméricas. No se admiten caracteres especiales.

Advertencia: Las contraseñas sólo se pueden establecer durante la instalación inicial. Debe desinstalar el extremo para cambiar una contraseña existente.

- ✓ **Bloqueo de problemas en la instalación**: se enumeran los problemas que pueden evitar que la instalación se realice correctamente en las máquinas seleccionadas.

Nota: Con **Antivirus**, se proporcionan procedimientos de agente específicos que le permiten a implementar previamente el paquete de instalación de **Antivirus** en los extremos, lo que reduce el ancho de banda requerido. Consulte el **artículo de la Base de conocimientos** *(https://helpdesk.kaseya.com/entries/34261116)*.

- **Desinstalar Antivirus**: desinstala el cliente de **Antivirus** en las máquinas seleccionadas.
  - **Fecha de inicio**: la fecha de inicio de la desinstalación.
  - **Hora**: la hora de inicio de la desinstalación.
  - **Período de distribución**: reprograma varias desinstalaciones de manera uniforme a lo largo de un período de distribución en un plazo inferior a la cantidad de períodos especificados, para distribuir el tráfico de red y la carga del servidor.
- **Reparar la instalación de Antivirus**: vuelve a instalar los archivos faltantes en un cliente de **Antivirus** instalado previamente para repararlo. El cliente de **Antivirus** se debe haber instalado previamente con el mismo VSA.
  - **Fecha de inicio**: la fecha de inicio de la reparación.
  - **Hora**: la hora de inicio de la reparación.
  - **Período de distribución**: reprograma varias reparaciones de manera uniforme a lo largo de un período de distribución en un plazo inferior a la cantidad de períodos especificados, para distribuir el tráfico de red y la carga del servidor.
- **Conectar Kaseya Antivirus**: restablece una conexión a una máquina anteriormente administrada por **Antivirus**, a la que se le quitó el agente de Kaseya y luego se le volvió a instalar. Esto incluye el restablecimiento de una conexión a las máquinas que eran administradas por un VSA diferente.
  - **Fecha de inicio**: la fecha de inicio de la reparación.
  - **Hora**: la hora de inicio de la reparación.
  - **Período de distribución**: efectúa nuevas programaciones de manera uniforme a lo largo de un período de distribución en un plazo inferior a la cantidad de períodos especificados, para distribuir el tráfico de red y la carga del servidor.
  - **Selección de perfil**: selecciona los perfiles de estaciones de trabajo y de servidores que se aplican.

Licencias

- **Recuentos de licencias**: enumera la cantidad de licencias de **Antivirus** para servidores y estaciones de trabajo. Las licencias para servidores y estaciones de trabajo se adquieren y rastrean por separado. Los recuentos de licencias de **Antivirus** también se muestran en la página **Administrador de licencias** *(http://help.kaseya.com/webhelp/ES/VSA/7000000/index.asp#2924.htm)*, en Administración > Administrar.
  - Total comprados hasta la fecha
  - Completamente disponible (comprada no asignada, aplicada, parcial o vencida)
  - Asignada (programada para instalación, pero la instalación aún no está completa)
  - Aplicada (licencia activa aplicada a una máquina)
  - Parcialmente disponible (asignada antes a una máquina, pero devuelta al grupo antes del vencimiento)
  - Parcialmente asignada (disponibilidad parcial que se programó para la instalación, pero la instalación aún no está completa)

- Total (licencias compradas menos las vencidas)
- Licencias expiradas
- Con vencimiento en los próximos 30 días
- Con vencimiento en los próximos 60 días
- Con vencimiento en los próximos 90 días

Protección

- **Obtener estado**: vuelve al estado habilitado o deshabilitado de los componentes de **Antivirus** en una máquina y, si es necesario, corrige la vista de los íconos de estado del componente en la **Cuadrícula de explorador**. Además, devuelve la información de versión de la firma de instalación y de base de datos.
- **Habilitar Antivirus temporalmente**: vuelve a habilitar la protección de **Antivirus** en las máquinas seleccionadas.
- **Deshabilitar Antivirus temporalmente**: deshabilita la protección de **Antivirus** en las máquinas seleccionadas. Algunas instalaciones de software requieren que se deshabilite **Antivirus** para completar la instalación.

Columnas de Antivirus

Los conjuntos de columnas determinan las columnas que se muestran en la **Cuadrícula de explorador** *(página 4)*. Puede editar *cualquier* conjunto de columnas que se indique en la lista desplegable **Conjunto de columnas** en el **Panel de control** *(página 6)*.

1. Seleccione un conjunto de columnas en la lista desplegable **Conjunto de columnas**.
2. Seleccione **Modificar columnas** en la misma lista desplegable para visualizar la ventana **Editar conjunto de columnas**.

   Las columnas asignadas en la lista de la derecha son las que se muestran cuando guarda cambios en el conjunto de columnas.

Las siguientes columnas están disponibles para seleccionarse cuando se modifica *cualquier* conjunto de columnas en la **Cuadrícula de explorador** *(página 4)*. Seleccione **Conjunto de columnas** en el **Panel de control** *(página 6)* para modificar un conjunto de columnas.

Antivirus

- **Fecha de vencimiento de AV**: la fecha de vencimiento programada para la seguridad de **Antivirus**.
- **Estado de instalación de AV**: `Not Installed`, `Script Scheduled`, `Installed`
- **Ícono de fase de instalación**: si está seleccionada, **Antivirus** está instalado en la máquina.

Detecciones

- **Eliminado**: número de detecciones eliminadas automáticamente.
- **Detectado**: número de detecciones.
- **Desinfectado**: número de detecciones desinfectadas automáticamente.
- **Tiene amenazas activas**: número de detecciones que no se pudieron desinfectar o eliminar automáticamente y que requiere atención del usuario.
- **Infectado**: número de detecciones infectadas.
- **Otro**: número de detecciones que no se pueden clasificar en ninguna otra categoría. Se aplica cuando Kaspersky presenta una nueva categoría de detección que **Antivirus** todavía no reconoce.
- **Sospechoso**: número de detecciones sospechosas que no se eliminaron ni se desinfectaron y que el usuario posiblemente quiera revisar.

Protección de extremo

- **Cadena de GUID del agente**: el GUID único del agente de Kaseya en formato de cadena.
- **ID**: el GUID único del agente de Kaseya en formato numérico.
- **Último reinicio**: la fecha y la hora en que se reinició la máquina por última vez.
- **Nombre de inicio de sesión**: el usuario de la sesión actual.
- **Nombre**: el machine ID.group ID.organization ID de la máquina.
- **Estado en línea**: Estos íconos indican el estado de registro del agente de cada máquina administrada. Al mantener el mouse sobre un ícono de registro, se muestra la ventana de QuickView del agente.
  - En línea pero esperando que se completa la primer auditoría
  - Agente en línea
  - Agente en línea y usuario actualmente conectado.
  - Agente en línea y usuario actualmente registrado, pero el usuario ha estado inactivo durante 10 minutos.
  - Agente actualmente fuera de línea
  - Agente no se ha registrado nunca
  - Agente en línea pero el control remoto se ha deshabilitado
  - El agente ha sido suspendido
- **Sistema operativo**: el sistema operativo de la máquina.
- **Ajuste de zona horaria**: muestra la cantidad de minutos. Consulte Sistema > Configuración del usuario > **Preferencias** *(http://help.kaseya.com/webhelp/ES/VSA/7000000/index.asp#503.htm)*.

Explorar

- **Próximo análisis completo de AV**: la fecha y la hora programadas para el próximo análisis completo de **Antivirus**.
- **Último análisis completo de AV**: la fecha y la hora en que se realizó el último análisis completo de **Antivirus**. Un análisis completo de **Antivirus** proporciona una exploración minuciosa de todo el sistema. Incluye: memoria del sistema, programas cargados en el inicio, copia de seguridad del sistema, bases de datos de correo electrónico, unidades de disco duro, medios de almacenamiento extraíbles y unidades de red.
- **Último análisis rápido de AV**: la fecha y la hora en que se realizó un análisis rápido de los objetos de inicio del sistema operativo con **Antivirus** por última vez. El análisis rápido pasó a llamarse análisis crítico a partir de la versión 10.x de **Antivirus**.
- **Estado de análisis de AV**: el estado del análisis.

Pestaña de Seguridad

- **Fecha de instalación de AV**: la fecha en que se instaló **Antivirus**.
- **Perfil de AV**: el perfil de **Antivirus** asignado a esta máquina.

Estado

- **Componentes de AV**: identifica el estado de los componentes de **Antivirus** instalados en esta máquina.
- **Última actualización del estado de AV**: identifica la fecha y la hora en que se actualizó **Antivirus** por última vez.
- **Indicadores de AV**: entre los posibles indicadores se incluye `Definitions out of date`
- **Acciones pendientes**: instalación, asignación, actualización y análisis.
- **Reinicio requerido**: si se lee `Yes`, se requiere un reinicio.

Actualización lista

- **Versión disponible del cliente de AV**: el número de versión de Kaspersky del cliente de **Antivirus** disponible para actualizar en esta máquina.

Versión

- **Versión del cliente de AV**: el número de versión de Kaspersky del cliente de **Antivirus** instalado en esta máquina.
- **Fecha de base de datos de AV**: la fecha y la hora de la base de datos de definiciones de **Antivirus** que usa la máquina en este momento.
- **Versión de servicio de AV**: la versión del cliente de **Antivirus**.
- **Versión de agente**: la versión del agente de Kaseya.
- **Actualización**: el estado de la actualización.

Centro de seguridad de Windows

- **Activo**: si está seleccionada, el producto antivirus está en uso.
- **Fabricante**: el fabricante del producto antivirus.
- **Actualizado**: si está seleccionada, el producto antivirus está actualizado.
- **Versión**: la versión del producto antivirus.
- **Nombre del producto informado al WSC**: el nombre del producto antivirus registrado con el *Centro de seguridad de Windows* (WSC). **Antivirus** en sí no se registra con el *Centro de seguridad de Windows*.

> **Nota:** En Windows 7 y versiones posteriores, el *Centro de seguridad de Windows* se denomina *Centro de actividades*.

Panel de detalles

Encabezado

- **Nombre**: el machine ID.group ID.organization ID de la máquina.
- **SO**: el sistema operativo de la máquina.
- **Dirección IP**: la dirección IP de la máquina.
- **ID de agente**: el GUID del agente en la máquina administrada.

Pestaña de estado

- **Estado de instalación**: si está seleccionada, la seguridad de **Antivirus** está instalada.
- **Fecha de instalación**: la fecha en que se instaló **Antivirus**.
- **Error de instalación**: si se produce un error de instalación, se muestra un vínculo `View Log` al registro de instalación de Kaspersky.
- **Contraseña de desinstalación**: la contraseña que se requiere para volver a configurar o desinstalar el cliente de **Antivirus**.
- **Vencimiento de licencia**: la fecha de vencimiento programada para la seguridad de **Antivirus**.
- **Perfil**: el perfil de configuración de **Antivirus** asignado a esta máquina.
- **Último análisis completo**: la fecha y la hora en que se realizó un análisis exhaustivo de todo el sistema por última vez. Incluye: memoria del sistema, programas cargados en el inicio, copia de seguridad del sistema, bases de datos de correo electrónico, unidades de disco duro, medios de almacenamiento extraíbles y unidades de red.
- **Último análisis rápido**: la fecha y la hora en que se realizó un análisis de área crítico de los objetos de inicio del sistema operativo por última vez. El análisis rápido pasó a llamarse análisis crítico a partir de la versión 10.x de **Antivirus**.
- **Próximo análisis completo**: la fecha y la hora programadas para el próximo análisis de **Antivirus**.
- **Versión del antivirus Kaspersky**: el número de versión de Kaspersky del cliente de **Antivirus** instalado en esta máquina.

- **Versión de administración**: el número de versión del paquete de **Antivirus** instalado en la máquina administrada.
- **Fecha de base de datos**: la fecha y la hora de la base de datos de definiciones de **Antivirus** que usa la máquina en este momento.
- **Última actualización**: la fecha y la hora en que se actualizó el cliente de **Antivirus** por última vez.
- **Indicadores**: entre los posibles indicadores se incluyen `Virus definitions out of date`, `Configuration is out of compliance with the profile`.

  Nota: Una vez que la máquina vuelve a cumplir con los requisitos, el indicador de falta de cumplimiento de los requisitos se sigue mostrando. Para que el indicador de falta de cumplimiento de los requisitos deje de aparecer, vuelva a asignar el perfil a la máquina.

- **Estado del componente**: identifica el estado de los componentes de **Antivirus** instalados en esta máquina. La protección de los componentes se especifica en la pestaña **Protección** *(página 17)*, en Perfiles.

  - **Habilitar Antivirus de archivos**: si está seleccionada, se analizan todos los archivos que están abiertos, guardados o ejecutados. *Se aplica a estaciones de trabajo y servidores.*
  - **Habilitar Antivirus de correo electrónico**: si está seleccionada, se analizan los mensajes entrantes y salientes para determinar la presencia de objetos malintencionados. Se inicia cuando se carga el sistema operativo; se ubica en la RAM de la computadora y analiza todos los mensajes de correo electrónico que se reciben mediante los protocolos POP3, SMTP, IMAP, MAPI y NNTP. *Se aplica a estaciones de trabajo solamente.*
  - **Habilitar Antivirus de Web**: si está seleccionada, garantiza la seguridad mientras se usa Internet. Protege la computadora contra los datos que ingresan a esta mediante el protocolo HTTP y, además, evita que se ejecuten scripts peligrosos en la computadora. *Se aplica a estaciones de trabajo solamente.*
  - **Habilitar Antivirus de MI**: si está seleccionada, garantiza la operación segura de los clientes de MI. Protege la información que ingresa a la computadora mediante protocolos de MI. El uso de este producto garantiza la operación segura de diversas aplicaciones de mensajería instantánea, como ICQ, MSN, AIM y Yahoo! Messenger, Jabber, Google Talk, Mail.Ru Agent e IRC. *Se aplica a estaciones de trabajo solamente.*
  - **Habilitar Antivirus proactivo**: si está seleccionada, reconoce una nueva amenaza en la computadora por la secuencia de acciones que ejecuta un programa. Si la secuencia de acciones de la aplicación se considera sospechosa como resultado del análisis de la actividad, **Antivirus** bloquea la actividad de esta aplicación. *Se aplica a estaciones de trabajo solamente.*
  - **Habilitar filtro de correo no deseado**: si está seleccionada, se integra en el cliente de correo instalado en la computadora y supervisa todos los mensajes de correo electrónico entrantes para determinar si hay contenido no deseado. Todos los mensajes que contienen correo no deseado se marcan con un encabezado especial. Además, el componente analiza los mensajes de correo electrónico para detectar suplantación de identidad (phishing). *Se aplica a estaciones de trabajo solamente.*
  - **Habilitar antispyware**: si está seleccionada, se interceptan los marcadores clandestinos que intentan establecer una conexión con sitios web de pago por uso y se bloquean. *Se aplica a estaciones de trabajo solamente.*
  - **Habilitar control de acceso**: si está seleccionada, evita la ejecución automática de aplicaciones y dispositivos en medios extraíbles conectados a la computadora, incluida la ejecución de archivos `autorun.inf`. *Se aplica a estaciones de trabajo solamente.*

Pestaña Perfiles de alerta

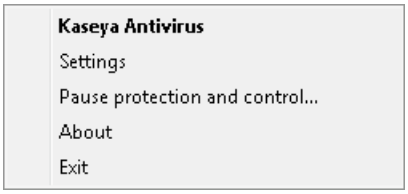
Se muestra la lista de **perfiles de alerta** *(página 25)* asignados a la máquina seleccionada.

Nota: En la pestaña **Extremos** *(página 27)*, en Alertas > <perfil>, se indican todas las máquinas que usan un perfil de alertas seleccionado.

Menú de agente Antivirus

Una vez instalado en una máquina, el agente **Antivirus** muestra un ícono en la bandeja del sistema de la computadora. Este ícono proporciona acceso a la interfaz de usuario del agente **Antivirus**.

Al hacer clic con el botón secundario del mouse en el ícono del agente, aparece un menú de opciones.



- **Antivirus Kaseya**: muestra la interfaz de usuario del agente **Antivirus**.
- **Configuración**: establece toda la configuración general de protección de **Antivirus**.
- **Pausar protección...**: pone en pausa la protección en la máquina durante un período especificado.
- **Acerca de**: muestra el cuadro Acerca de para el agente **Antivirus**.
- **Salir**: finaliza el servicio del agente **Antivirus** en la máquina administrada. La máquina ya no está protegida por **Antivirus**.

Nota: **Personalización de la interfaz de usuario del cliente de Antivirus en el extremo** *(https://helpdesk.kaseya.com/entries/32410117)*.

Tableros

Antivirus > Mostrar > Tableros

En la página **Tableros**, se proporciona una vista de tablero del estado de las máquinas que tienen instalado **Antivirus**. Las estadísticas del tablero que se muestran dependen del **filtro ID de máquina/ID de grupo** *(http://help.kaseya.com/webhelp/ES/VSA/7000000/index.asp#209.htm)* y de los grupos de máquinas que el usuario está autorizado a ver en Sistema > **Ámbitos** *(http://help.kaseya.com/webhelp/ES/VSA/7000000/index.asp#4578.htm)*.

Acciones

- **Acciones**
  - **Nuevo**: crea un tablero nuevo.
  - **Guardar**: guarda los cambios en el tablero que se muestra en ese momento.
  - **Guardar como**: guarda el tablero que se muestra en ese momento con un nombre nuevo.
  - **Eliminar**: elimina el tablero que se muestra en ese momento.
- **Seleccionar tablero**: selecciona un tablero para mostrar.
- **Agregar partes**: agrega partes al tablero que se muestra en ese momento. Consulte la lista de partes a continuación.
- **Abrir en otra ventana**: muestra el tablero seleccionado en una pestaña o una ventana aparte.

Partes del tablero de Antivirus

- **Extensión automática de licencia de Antivirus**: gráfico de barras en el que se muestra la cantidad de máquinas que tienen habilitada la opción **Extensión automática** y para las que se vencen las licencias en 30, 60, 90 o más de 91 días.
- **Vencimiento de licencia de Antivirus**: gráfico de barras en el que se muestra la cantidad de máquinas cuyas licencias vencieron o vencen en 30, 60, 90 o más de 91 días.
- **Máquinas con Antivirus que necesitan atención**: gráfico de barras en el que se muestra la cantidad de máquinas administradas que cuentan con **Antivirus** que necesitan atención, según su categoría. Las categorías incluyen `No AV Installed`, `Uncured Threats`, `Out of Date`, `Reboot Needed`, `Component`.
- **Cantidad de máquinas con Antivirus con detecciones**: gráfico de barras en el que se muestra la cantidad de detecciones.
- **Estado de protección de Antivirus**: gráfico circular en el que se muestran categorías de porcentajes de máquinas con protección de **Antivirus**. Las categorías de porcentajes incluyen `Not Installed`, `Out of Date`, `Not Enabled` y `Up to Date`.
- **Principales amenazas que detecta Antivirus**: se enumeran las máquinas con la mayor cantidad de amenazas. Al hacer clic en la ID de máquina con hipervínculo, se muestran las amenazas que pertenecen a dicha ID de máquina en la página **Detecciones** *(página 14)*.
- **Resumen licencias de Antivirus** sin filtrar: en un gráfico, se muestra la cantidad de máquinas que están `Available`, `Expired`, `In Use`, `Partials` y `Pending Install`.

Detecciones

Antivirus > Mostrar > Detecciones

En la página **Detecciones**, se muestran amenazas de virus que **Antivirus** no resuelve automáticamente. Use la información que se incluye en esta página para investigar en profundidad las amenazas y eliminarlas en forma manual. La lista de máquinas que se muestra depende del **filtro ID de máquina/ID de grupo** *(http://help.kaseya.com/webhelp/ES/VSA/7000000/index.asp#209.htm)* y de los grupos de máquinas que el usuario está autorizado a ver en Sistema > **Ámbitos** *(http://help.kaseya.com/webhelp/ES/VSA/7000000/index.asp#4578.htm)*.

Acciones

- **Detalles**: haga clic para obtener más información sobre una amenaza seleccionada en el sitio web Securelist de Kaspersky.
- **Agregar exclusión**: agrega filas seleccionadas a la **lista de exclusiones** *(página 24)*.
- **Eliminar**: envía una solicitud al extremo para eliminar el archivo en cuarentena.
- **Restaurar**: envía una solicitud al extremo para quitar el archivo de cuarentena. El archivo ya no se considera una amenaza.
- **Ocultar**: no mostrar en esta lista. Ocultar la amenaza no significa que se elimine.
- **Filtrar**: filtra la lista según una de las siguientes categorías:
  - **Amenazas activas**: se muestran las amenazas de **Antivirus** que se detectaron, pero que aún no se desinfectaron, eliminaron o excluyeron.
  - **Archivos en cuarentena**: se muestran los archivos en cuarentena.
  - **Archivos eliminados**: se muestra una lista de los archivos eliminados.
  - **Últimos <N períodos> de amenazas**: filtra la lista por uno o varios de los períodos predefinidos.
  - **Borrar filtro**: quita todos los filtros de la lista.

Columnas de tabla

- **Nombre de la máquina**: el ID de la máquina.

- **Nombre**: el nombre de la amenaza.
- **Ruta**: la ubicación de la amenaza en la máquina administrada.
- **Hora**: la fecha y la hora en que se detectó la amenaza.
- **Estado**: el estado de la amenaza. Los mensajes de estado incluyen, entre otros, lo siguiente:
  - `Infected`: se determinó que el archivo está infectado por un virus.
  - `Suspicious`: el archivo es sospechoso. Por lo general, significa que es malware, pero no es un virus confirmado y conocido.
  - `Disinfected`: Kaspersky eliminó el virus del archivo.
  - `Deleted`: se eliminó el archivo, ya sea en forma automática o después de haber estado en cuarentena.
  - `Quarantined`: el archivo está en cuarentena; el usuario no puede acceder a este, pero se puede restaurar o eliminar. Para restaurar un archivo en cuarentena, use la contraseña que se muestra para una máquina en Máquinas > **Panel de detalles** *(página 11)*.
  - `Detected`: Kaspersky hizo una detección, pero no se tomó ninguna medida: no se puso en cuarentena, no se eliminó, etc. Esto puede ser una posible amenaza activa. El usuario debe procesar la amenaza con las opciones disponibles en **Administrar detección**.
  - `Not Found`: el archivo ya no existe. Es posible que se haya eliminado después de haberse detectado, pero no lo eliminó Kaspersky. Esto puede ocurrir cuando se encuentra un archivo temporal, como una cookie o un archivo temporal, que ya se eliminó al eliminar la memoria caché del explorador.
  - `Unknown`: las definiciones de virus de Kaspersky no reconocen el archivo. Si se requiere una investigación más completa, cree un **ticket de soporte** *(https://helpdesk.kaseya.com/home)* de Kaseya.
  - `RemediatedByUser`: el usuario se encargó del archivo en forma manual. En este caso, el usuario visualiza una venta emergente en la que se le pregunta si desea eliminar, poner en cuarentena u omitir esta amenaza, y el usuario actúa por su cuenta.
- **Tipo**: la categoría de la amenaza.
- **Nombre de perfil**: el nombre del perfil que estaba en uso cuando se detectó la amenaza.

Perfiles

Antivirus > Configuración > Perfiles

En la página **Perfiles**, se administran los perfiles de **Antivirus**. Cada perfil representa un conjunto distinto de opciones de **Antivirus** habilitadas o deshabilitadas. Los cambios en un perfil afectan a todos los ID de máquina asignados a ese perfil. Los perfiles se asignan a los ID de máquina en Antivirus > **Máquinas** *(página 3)* > **Asignar**. En general, los diferentes tipos de máquinas o redes requieren diferentes perfiles. Los perfiles sólo son visibles si el usuario creó el perfil o si el perfil se asignó a una máquina asignada al ámbito que se está utilizando.

Tipos de perfil: servidores y estaciones de trabajo

Las licencias de **Antivirus** se adquieren y rastrean por separado para los servidores y las estaciones de trabajo. A cada uno se le asignan diferentes tipos de perfiles. Un perfil de servidor sólo se puede asignar a servidores. Un perfil de estación de trabajo sólo se puede asignar a estaciones de trabajo. Se le proporcionan ejemplos de cada tipo de perfil. Se pueden seleccionar y asignar estaciones de trabajo y servidores al mismo tiempo

Acciones

- **Nuevo**: crea un nuevo perfil de configuración. Cada tipo de perfil instala un tipo diferente de cliente en el extremo. Los tipos de perfil incluyen lo siguiente:

- `Kaspersky Workstation 10 Profile`
- `Kaspersky Workstation 6 Profile`
- `Kaspersky Server 10 Profile`
- `Kaspersky Server 6 Profile`

Nota: **Antivirus** 6.5 admite tanto la versión 10 de Kaspersky como la versión 6 heredada, para extremos de estación de trabajo y servidor. Se proporcionan perfiles específicos para administrar cada tipo de máquina. **Antivirus** *6.5 no admite extremos de la versión 2010 de Kaspersky.* **Antivirus** 6.5 sólo instala o actualiza extremos en la versión 10 de Kaspersky. *Se recomienda ampliamente la versión 10.* Puede actualizar un extremo de la versión 6 de Kaspersky a la versión 10 con el botón **Actualizar versión del cliente**, en Instalar, del Panel de control.

- **Abrir**: abre un perfil existente para editarlo. También puede hacer doble clic en un perfil para abrirlo.
- **Eliminar**: elimina un perfil existente.
- **Guardar**: guarda los cambios en el perfil seleccionado en ese momento.
- **Copiar**: guarda el perfil seleccionado con un nombre nuevo. Los perfiles de servidor sólo se pueden copiar a un nuevo perfil de servidor. Los perfiles de estación de trabajo sólo se pueden copiar a un nuevo perfil de estación de trabajo.
  - **al perfil de Kaspersky 10**: se copia un perfil seleccionado a un perfil de la versión 10 de Kaspersky.
- **Filtro**
  - `Show Kaspersky Workstation Profiles Only`
  - `Show Kaspersky Server Profiles Only`
  - `Show Kaspersky 10.0.0.0 Profiles Only`
  - `Show Kaspersky 6.0.4.1424 Profiles Only`
- **Quitar filtro**: quita el filtro.

Adición y edición de perfiles

Haga clic en **Nuevo** y, a continuación, en un *tipo de perfil*, para visualizar la ventana **Nuevo perfil**, o haga clic en un perfil existente y, a continuación, en **Abrir** para visualizar la ventana **Editar perfil**.

- **Pestaña Resumen** *(página 17)*
- **Pestaña Protección** *(página 17)*
- **Pestaña Análisis rápido** *(página 21)*
- **Pestaña Análisis completo** *(página 22)*
- **Pestaña Opciones de actualización** *(página 23)*
- **Pestaña Exclusiones** *(página 24)*
- **Pestaña Extremos** *(página 25)*

Columnas de tabla

- **Nombre**: nombre del perfil.
- **Tipo de perfil**: `Kaspersky File Server` o `Kaspersky Workstation`
- **Máquinas aplicadas**: cantidad de máquinas que utilizan este perfil.
- **Creado por**: usuario del VSA que creó este perfil.
- **Versión**
  - `6.0.4.1424` o `6.0.4.1611`: versión 6, servidor o estación de trabajo
  - `10.x.x.x`: Kaspersky Endpoint Security for Business, versión 10

Pestaña Resumen

Antivirus > Configuración > Perfiles > pestaña Resumen

Nota: Las opciones que no son compatibles para cada versión de perfil están deshabilitadas (en gris).

- **Nombre**: el nombre del perfil.
- **Descripción**: una descripción del perfil.
- **Tipo de perfil**: servidor de archivos o estación de trabajo de **Antivirus**.
- **Versión del Perfil**
  - `6.0.4.1424` o `6.0.4.1611`: versión 6, servidor o estación de trabajo
  - `10.x.x.x`: Kaspersky Endpoint Security for Business, versión 10

Pestaña Protección

Antivirus > Configuración > Perfiles > Protección

Nota: Las opciones que no son compatibles para cada versión de perfil están deshabilitadas (en gris).

Opciones

- **Habilitar protección**: si está seleccionada, se habilitan todos los componentes de protección seleccionados para este perfil.
- **Iniciar Antivirus en el inicio de la computadora**: si está seleccionada, todos los componentes de protección seleccionados para este perfil se habilitan en el inicio.
- **Habilitar defensa propia**: evita el acceso no autorizado a los archivos de **Antivirus**, incluida la protección contra software que posee la opción de clic automático.

Protección interactiva

- **Seleccionar acción automáticamente**: si está seleccionada, se llevan a cabo acciones recomendadas por Kaspersky Lab en forma automática. Una vez que se detecta una amenaza, la aplicación intenta desinfectar el objeto. Si la desinfección falla, la aplicación intenta eliminarla. Los objetos sospechosos se omiten sin procesarlos. Los mensajes emergentes informan al usuario sobre nuevos eventos. Si no está seleccionada, la protección usa la configuración personalizada que se indica a continuación.
  - **No eliminar objetos sospechosos**: si está seleccionada y se aplican acciones en forma automática, los objetos sospechosos no se eliminan.
- **Mostrar "Protegido por Kaspersky Lab" en la pantalla de inicio de sesión de Microsoft Windows**: si está seleccionada, muestra la etiqueta.
- **Mostrar ícono en la barra de tareas**: si está seleccionada, se muestra el ícono del cliente de **Antivirus** en la bandeja del sistema de la computadora del usuario. El usuario puede hacer clic con el botón principal o secundario en el ícono para acceder al **Menú de agente de Antivirus** *(página 13)*.
- **Mostrar en el menú "Inicio"**: si está seleccionada, se muestra el cliente de **Antivirus** como un programa en el menú Inicio del usuario.
- **Mostrar en la lista "Agregar o quitar programas" ("Programas y características")**: si está seleccionada, se muestra el cliente de **Antivirus** como un programa en la lista "Agregar o quitar programas" del usuario. El usuario puede desinstalar el cliente de **Antivirus**.

Nota: Para cada lista de componentes a continuación, se muestran los íconos correspondientes en el campo **Estado del componente** del **Panel de detalles** *(página 11)* de la página **Máquinas**.

Antivirus de archivos

Se aplica a estaciones de trabajo y servidores.

- **Habilitar Antivirus de archivos**: si está seleccionada, se analizan todos los archivos que están abiertos, guardados o ejecutados.
- **Analizar sólo archivos nuevos y modificados**: si está seleccionada, se analizan sólo archivos nuevos y modificados desde el último análisis.
- **Proteger unidades de red**: si está seleccionada, se incluyen unidades de red asignadas.
- **Proteger unidades extraíbles**: si está seleccionada, se incluyen unidades extraíbles.
- **Analizar archivos**: si está seleccionada, se analizan los archivos almacenados.
- **Analizar paquetes de instalación**: si está seleccionada, se analizan los paquetes de instalación.
- **Analizar objetos OLE incrustados**: si está seleccionada, se analizan los objetos OLE incrustados en archivos.
- **Análisis heurístico**: si está seleccionada, se usa el análisis heurístico para identificar el comportamiento de objetos malintencionados o sospechosos, incluso si aún no se los identificó como amenazas conocidas en la base de datos de firmas. Esto permite que se detecten nuevas amenazas incluso antes de que las hayan investigado analistas de virus.
- **Profundidad**: profundidad del análisis heurístico para utilizar: `Light`, `Medium`, `Deep`.
- **Extraer archivos compuestos en segundo plano**: si está seleccionada, los archivos compuestos de mayor tamaño que el especificado en **Tamaño mínimo de archivo (MB)** se extraen y analizan en segundo plano mientras el usuario comienza a trabajar con el archivo compuesto. Esto elimina el retraso que se requiere para analizar archivos compuestos de gran tamaño. Los archivos compuestos incluyen archivos almacenados, archivos de instalación y objetos OLE incrustados.
- **Tamaño mínimo de archivo (MB)**: especifica el tamaño mínimo de archivo para el análisis en segundo plano de los archivos compuestos.
- **No desempaquetar archivos compuestos de gran tamaño**: si está seleccionada, los archivos compuestos de mayor tamaño que el que se especifica en **Tamaño máximo de archivo (MB)** no se analizan. Los archivos que se extraen de archivos almacenados siempre se analizan, independientemente de este parámetro.
- **Tamaño máximo de archivo (MB)**: especifica el tamaño máximo de archivo para suprimir el análisis de los archivos.
- **Tecnología iSwift**: si está seleccionada, la tecnología iSwift se usa para acelerar los análisis. Se omite un nuevo análisis para los *objetos NTFS* analizados previamente, a menos que se haya modificado el objeto, la configuración del análisis o la base de datos del antivirus.
- **Tecnología iChecker**: si está seleccionada, la tecnología iChecker se usa para acelerar los análisis. Se omite un nuevo análisis para los *objetos* analizados previamente, a menos que se haya modificado el archivo, la configuración del análisis o la base de datos del antivirus.

Antivirus de correo

Se aplica a estaciones de trabajo solamente.

- **Habilitar Antivirus de correo electrónico**: si está seleccionada, se analizan los mensajes entrantes y salientes para determinar la presencia de objetos malintencionados. Se inicia cuando se carga el sistema operativo; se ubica en la RAM de la computadora y analiza todos los mensajes de correo electrónico que se reciben mediante los protocolos POP3, SMTP, IMAP, MAPI y NNTP.
- **Comprobar sólo mensajes entrantes**: si está seleccionada, sólo se analiza el correo electrónico entrante. Si no está seleccionada, se analiza el correo electrónico entrante y saliente.
- **Tráfico POP3/SMTP/NMTP/IMAP**: si está seleccionada, se analiza el tráfico de correo electrónico POP3/SMTP/NMTP/IMAP.
- **Tráfico ICQ/MSN**: si está seleccionada, se analiza el tráfico de mensajería instantánea ICQ y MSN.
- **Adicional: complemento de Microsoft Office Outlook**: si está seleccionada, se instala un complemento para el cliente de correo electrónico Outlook que permite la configuración de las opciones del antivirus de correo electrónico en **Herramientas > Opciones > pestaña Correo antivirus** en Outlook.

- **Adicional: The Bat!** : si está seleccionada, se instala un complemento del cliente de correo electrónico The Bat! que permite la configuración de las opciones del antivirus de correo electrónico mediante el elemento Protección antivirus en **Propiedades> Configuración**, en The Bat!
- **Comprobar si las URL figuran en la base de las direcciones web sospechosas**: si está seleccionada, se analizan los vínculos de los mensajes de correo electrónico incluidos en la base de datos de direcciones web sospechosas.
- **Comprobar si las URL figuran en la base de las direcciones web de suplantación de identidad (phishing)**: si está seleccionada, se analizan los vínculos de los mensajes de correo electrónico incluidos en la base de datos de direcciones web de suplantación de identidad.
- **Análisis heurístico**: si está seleccionada, se usa el análisis heurístico para identificar el comportamiento de objetos malintencionados o sospechosos, incluso si aún no se los identificó como amenazas conocidas en la base de datos de firmas. Esto permite que se detecten nuevas amenazas incluso antes de que las hayan investigado analistas de virus.
- **Profundidad**: profundidad del análisis heurístico para utilizar: `Light`, `Medium`, `Deep`.

Antivirus de Web

Se aplica a estaciones de trabajo solamente.

- **Habilitar Antivirus de Web**: si está seleccionada, garantiza la seguridad mientras se usa Internet. Protege la computadora contra los datos que ingresan a esta mediante el protocolo HTTP y, además, evita que se ejecuten scripts peligrosos en la computadora.
- **Comprobar si las URL figuran en la base de las direcciones web sospechosas**: si está seleccionada, se analizan los vínculos de los mensajes de correo electrónico incluidos en la base de datos de direcciones web sospechosas.
- **Comprobar si las URL figuran en la base de las direcciones web de suplantación de identidad (phishing)**: si está seleccionada, se analizan los vínculos de los mensajes de correo electrónico incluidos en la base de datos de direcciones web de suplantación de identidad.
- **Limitar tiempo de almacenamiento en caché de fragmentos**: si está seleccionada, se limita el tiempo permitido para analizar cada fragmento de un objeto por separado mientras se descarga. Si se excede el límite para un fragmento, este se descarga sin analizarse. Si no está seleccionada, nunca se omite el análisis de fragmentos. De cualquier modo, se analiza todo el objeto una vez que se completa la descarga. Es útil cuando el almacenamiento en caché de fragmentos provoca que se agote el tiempo de espera de las conexiones HTTP y los exploradores lentos.
- **Tiempo de almacenamiento en caché en segundos**: especifica el tiempo límite para el almacenamiento en caché de fragmentos.
- **Análisis heurístico**: si está seleccionada, se usa el análisis heurístico para identificar el comportamiento de objetos malintencionados o sospechosos, incluso si aún no se los identificó como amenazas conocidas en la base de datos de firmas. Esto permite que se detecten nuevas amenazas incluso antes de que las hayan investigado analistas de virus.
- **Profundidad**: profundidad del análisis heurístico para utilizar: `Light`, `Medium`, `Deep`.

Antivirus de IM

Se aplica a estaciones de trabajo solamente.

- **Habilitar Antivirus de IM**: si está seleccionada, garantiza la operación segura de los clientes de IM. Protege la información que ingresa a la computadora mediante protocolos de MI. El uso de este producto garantiza la operación segura de diversas aplicaciones de mensajería instantánea, como ICQ, MSN, AIM y Yahoo! Messenger, Jabber, Google Talk, Mail.Ru Agent e IRC.

Antivirus proactivo

Se aplica a estaciones de trabajo solamente.

- **Habilitar Antivirus proactivo**: si está seleccionada, reconoce una nueva amenaza en la computadora por la secuencia de acciones que ejecuta un programa. Si la secuencia de acciones de la aplicación es sospechosa, **Antivirus** bloquea la actividad de esta aplicación.

- **Habilitar supervisión de actividad de aplicaciones**: si está seleccionada, se supervisa la actividad de las aplicaciones en la computadora para determinar eventos sospechosos.
- **Habilitar protección de registro**: si está seleccionada, se protege el registro contra cambios sospechosos en aplicaciones esenciales.

Control de acceso

Se aplica a estaciones de trabajo solamente.

- **Habilitar control de acceso**: si está seleccionada, evita el acceso de ejecución automática.
- **Deshabilitar ejecución automática para todos los dispositivos**: si está seleccionada, se deshabilita la ejecución automática de aplicaciones y dispositivos en medios extraíbles conectados a la computadora.
- **Deshabilitar procesamiento autorun.inf**: si está seleccionada, se deshabilita la ejecución automática de los archivos `autorun.inf` .

Anti-Spy

Se aplica a estaciones de trabajo solamente.

- **Habilitar antispyware**: si está seleccionada, se interceptan los marcadores clandestinos que intentan establecer una conexión con sitios web de pago por uso y se bloquean.
- **Habilitar Anti Banner**: si está seleccionada, se bloquean las publicidades en los banners especiales en la Web o integrados en las interfaces de diversos programas instalados en la computadora.
- **Habilitar Anti Dialer**: si está seleccionada, se notifica al usuario mediante una ventana emergente que se intenta establecer una conexión secreta en la computadora del usuario para marcar una conexión a un número de teléfono. Al usuario se le da la opción de bloquear o permitir la conexión.

Anti-Spam

Se aplica a estaciones de trabajo solamente.

- **Habilitar filtro de correo no deseado**: si está seleccionada, se integra en el cliente de correo instalado en la computadora y supervisa todos los mensajes de correo electrónico entrantes para determinar si hay contenido no deseado. Todos los mensajes que contienen correo no deseado se marcan con un encabezado especial. Además, el componente analiza los mensajes de correo electrónico para detectar suplantación de identidad (phishing).
- **Tráfico POP3/SMTP/NMTP/IMAP**: si está seleccionada, se analiza el tráfico de correo electrónico POP3/SMTP/NMTP/IMAP.
- **Adicional: complemento de Microsoft Office Outlook**: si está seleccionada, se instala un complemento para el cliente de correo electrónico Outlook que permite la configuración de las opciones del filtro de correo no deseado en **Herramientas > Opciones> pestaña Filtro de correo no deseado** en Outlook.
- **Adicional: complemento de Microsoft Outlook Express**: si está seleccionada, se instala un complemento para el cliente de correo electrónico Outlook Express que permite la configuración de las opciones del filtro de correo no deseado. Al hacer clic en el botón **Configuración** junto a los botones **Correo no deseado** y **No es correo no deseado** en la barra de tareas de Outlook Express, se abre una ventana especial.
- **Adicional: The Bat!** : si está seleccionada, se instala un complemento del cliente de correo electrónico The Bat! que permite la configuración de las opciones del filtro de correo no deseado mediante el elemento Protección contra correo no deseado en **Propiedades > Configuración**, en The Bat!
- **Abrir Mail Dispatcher al recibir un correo electrónico a través de POP3**: si está seleccionada, el usuario puede obtener una vista previa del correo electrónico almacenado en un servidor POP3 en una ventana de **Dispatcher** antes de descargar el correo electrónico en la computadora local. Esto reduce el riesgo de descargar correo no deseado o virus.
- **Capacitar en correo saliente**: si está seleccionada, una vez que se habilita esta opción, se agregan a la lista blanca del usuario las direcciones de correo electrónico de los primeros 50 correos

electrónicos salientes que envía el usuario. La lista blanca es una lista de direcciones de correo electrónico de confianza y de frases que clasifican el correo electrónico como útil.

- **No comprobar mensajes nativos de Microsoft Exchange Server**: si está seleccionada, no se analiza el correo electrónico que envía Microsoft Exchange Server del propio usuario en forma interna.
- **Comprobar si las URL figuran en la base de las direcciones web sospechosas**: si está seleccionada, se analizan los vínculos de los mensajes de correo electrónico incluidos en la base de datos de direcciones web sospechosas.
- **Comprobar si las URL figuran en la base de las direcciones web de suplantación de identidad (phishing)**: si está seleccionada, se analizan los vínculos de los mensajes de correo electrónico incluidos en la base de datos de direcciones web de suplantación de identidad.

Opciones de red

- **Kaspersky supervisa los siguientes puertos (delimitado por comas)**: especifica la lista de puertos de red que están bajo la supervisión de los componentes de Antivirus de correo, Antivirus de Web y Antivirus de IM.

Pestaña Análisis rápido o Análisis crítico

Antivirus > Configuración > Perfiles > Análisis rápido o Análisis crítico

Nota: Las opciones que no son compatibles para cada versión de perfil están deshabilitadas (en gris).

Nota: El análisis rápido pasó a llamarse análisis crítico a partir de la versión 10.x de **Antivirus**.

El **análisis rápido o crítico de** **Antivirus** examina los objetos de inicio del sistema operativo.

- **Nivel de seguridad**: se proporcionan tres niveles de seguridad:
  - **Alto**: establezca este nivel si sospecha que hay altas probabilidades de que se infecte la computadora.
  - **Recomendado**: este nivel proporciona un equilibrio óptimo entre eficacia y seguridad, y es el adecuado en la mayoría de los casos.
  - **Bajo**: si la máquina funciona en un ambiente protegido, el nivel de seguridad bajo puede ser el adecuado. También se puede establecer un nivel de seguridad bajo si la máquina funciona con aplicaciones que consumen recursos.
- **Programa**
  - **Manual**: los análisis de las máquinas con este perfil sólo se programan en forma manual.
  - **Por programación/Hora de ejecución del análisis/Ejecutar cada**: se programan los análisis de las máquinas que usan este perfil según la cantidad especificada de períodos. El tiempo se basa en el agente.
  - **Ejecutar tareas omitidas**: se muestra sólo si hay tareas programadas para realizarse a diario, semanalmente o mensualmente. Si está seleccionada y la máquina está desconectada en el momento en que está programada la ejecución de una tarea, ejecute la tarea no bien la máquina esté en línea nuevamente. Si no está seleccionada y la máquina está desconectada, omita y ejecute el siguiente período y hora programados.
  - **Pausar análisis programados cuando el protector de pantalla está inactivo o la computadora está desbloqueada**: si está seleccionada, se pone en pausa el análisis cuando la computadora está en uso.
  - **Solicitar acción cuando se completa el análisis**: si está seleccionada y se detecta una amenaza durante el análisis, se pregunta al usuario al *final* de dicho análisis si desea que se desinfecten los archivos en cuarentena. Si la desinfección falla, también se pregunta al usuario si desea eliminar los archivos en cuarentena.

- **Solicitar acción durante el análisis**: si está seleccionada y se detecta una amenaza *durante* el análisis, se pregunta al usuario durante este si desea que se desinfecte un archivo en cuarentena, y si la desinfección falla, si desea eliminarlo.
- **No solicitar acción**: no se le hacen preguntas al usuario si se detectan amenazas.
  - ✓ **Desinfectar**: si está seleccionada, se intenta desinfectar un archivo en cuarentena.
  - ✓ **Eliminar si la desinfección falla**: si no se puede desinfectar un archivo en cuarentena, este se elimina.
- **Conceder recursos a otras aplicaciones**: si está seleccionada, cuando aumenta la carga en el sistema de archivos de otras aplicaciones, las tareas de análisis se pausan.

Pestaña Análisis completo

Antivirus > Configuración > Perfiles > Análisis completo

Nota: Las opciones que no son compatibles para cada versión de perfil están deshabilitadas (en gris).

En un **análisis completo**, se realiza una exploración minuciosa con **Antivirus** de todo el sistema. Los siguientes objetos se analizan de manera predeterminada: memoria del sistema, programas cargados en el inicio, copia de seguridad del sistema, bases de datos de correo electrónico, unidades de disco duro, medios de almacenamiento extraíbles y unidades de red.

- **Nivel de seguridad**: se proporcionan tres niveles de seguridad:
  - **Alto**: establezca este nivel si sospecha que hay altas probabilidades de que se infecte la computadora.
  - **Recomendado**: este nivel proporciona un equilibrio óptimo entre eficacia y seguridad, y es el adecuado en la mayoría de los casos.
  - **Bajo**: si la máquina funciona en un ambiente protegido, el nivel de seguridad bajo puede ser el adecuado. También se puede establecer un nivel de seguridad bajo si la máquina funciona con aplicaciones que consumen recursos.
- **Programa**
  - **Manual**: los análisis de las máquinas con este perfil sólo se programan en forma manual.
  - **Por programación/Hora de ejecución del análisis**: se programan los análisis de las máquinas que usan este perfil según la cantidad especificada de períodos. El tiempo se basa en el agente.
  - **Ejecutar tareas omitidas**: se muestra sólo si hay tareas programadas para realizarse a diario, semanalmente o mensualmente. Si está seleccionada y la máquina está desconectada en el momento en que está programada la ejecución de una tarea, ejecute la tarea no bien la máquina esté en línea nuevamente. Si no está seleccionada y la máquina está desconectada, omita y ejecute el siguiente período y hora programados.
  - **Pausar análisis programados cuando el protector de pantalla está inactivo o la computadora está desbloqueada**: si está seleccionada, se pone en pausa el análisis cuando la computadora está en uso.
  - **Solicitar acción cuando se completa el análisis**: si está seleccionada y se detecta una amenaza durante el análisis, se pregunta al usuario al *final* de dicho análisis si desea que se desinfecten los archivos en cuarentena. Si la desinfección falla, también se pregunta al usuario si desea eliminar los archivos en cuarentena.
  - **Solicitar acción durante el análisis**: si está seleccionada y se detecta una amenaza *durante* el análisis, se pregunta al usuario durante este si desea que se desinfecte un archivo en cuarentena, y si la desinfección falla, si desea eliminarlo.
  - **No solicitar acción**: no se le hacen preguntas al usuario si se detectan amenazas.
    - ✓ **Desinfectar**: si está seleccionada, se intenta desinfectar un archivo en cuarentena.
    - ✓ **Eliminar si la desinfección falla**: si no se puede desinfectar un archivo en cuarentena, este

se elimina.

- **Conceder recursos a otras aplicaciones**: si está seleccionada, cuando aumenta la carga en el sistema de archivos de otras aplicaciones, las tareas de análisis se pausan.

Pestaña Opciones de actualización

Antivirus > Configuración > Perfiles > Opciones de actualización

Nota: Las opciones que no son compatibles para cada versión de perfil están deshabilitadas (en gris).

En la pestaña **Opciones de actualización**, se programa la descarga de las actualizaciones de **Antivirus** en los equipos cliente.

Programa

- **Automático**: se comprueba si hay actualizaciones en intervalos específicos. Cuando se encuentra una nueva actualización, se descarga y se instala en las máquinas administradas con **Antivirus** mediante este perfil.
- **Manual**: las actualizaciones de las máquinas con este perfil sólo se programan en forma manual. Actualice las máquinas en forma manual en el panel de control de la página **Máquinas** *(página 3)*.
- **Por programación/Hora de ejecución de la actualización/Ejecutar cada**: se programan las actualizaciones del cliente de **Antivirus** y de su base de datos de definiciones en todas las máquinas administradas con **Antivirus** que usan este perfil según la cantidad especificada de períodos. El tiempo se basa en el agente.
- **Ejecutar tareas omitidas**: se muestra sólo si hay tareas programadas para realizarse a diario, semanalmente o mensualmente. Si está seleccionada y la máquina está desconectada en el momento en que está programada la ejecución de una tarea, ejecute la tarea no bien la máquina esté en línea nuevamente. Si no está seleccionada y la máquina está desconectada, omita y ejecute el siguiente período y hora programados.

Configuración de proxy

Especifique un servidor proxy si los equipos cliente requieren uno para descargar las actualizaciones de **Antivirus** de la Web.

- **Usar configuración personalizada del servidor proxy**: si está seleccionada, se especifica en forma manual el servidor proxy para descargar actualizaciones. Si no está seleccionada, la configuración del proxy se detecta automáticamente.
  - **Dirección**: introduzca una dirección IP o un nombre de servidor proxy válidos.
  - **Puerto** : ingrese un número de puerto.
- **Especificar datos de autenticación**: si está seleccionada, se requiere la autenticación de proxy.
  - **Nombre de usuario**: si está seleccionada la opción **Especificar datos de autenticación**, introduzca un nombre de usuario válido.
  - **Contraseña cifrada**: si está seleccionada la opción **Especificar datos de autenticación**, introduzca una contraseña válida.
- **Omitir el servidor proxy para las direcciones locales**: si está seleccionada, las direcciones IP locales no usan el servidor proxy.

Pestaña Exclusiones

Antivirus > Configuración > Perfiles > Exclusiones

Nota: Las opciones que no son compatibles para cada versión de perfil están deshabilitadas (en gris).

En la pestaña **Exclusiones** para los perfiles de **Antivirus**, se excluyen objetos de la supervisión de **Antivirus**.

Reglas de exclusión

- **Agregar exclusión**: se agregan máscaras de archivo o máscaras con ruta de acceso del directorio para excluirlas del análisis y la protección, con un límite de hasta 256 exclusiones.
- **Eliminar**: elimina una regla de exclusión seleccionada.

Las exclusiones compatibles incluyen lo siguiente:

- Máscaras sin rutas de acceso del archivo
  - `*test*`: cualquier archivo con `test` en el nombre, que diga `12astestsdsd.sds`
  - `*test.*`: cualquier archivo cuyo nombre termine con `test`: `346dfghtest.gdh`
  - `test.*`: archivo con el nombre `test` y cualquier extensión
- Máscaras con rutas de acceso del archivo absolutas
  - `C:\dir\*.*` o `C:\dir\*` o `c:\dir\`: todos los archivos en la carpeta `C:\dir`
  - `C:\dir\*.exe`: todos los archivos con la extensión `exe` en la carpeta `C:\dir`
  - `C:\dir\*.ex?`: todos los archivos con la extensión `ex?` en la carpeta `C:\dir`, donde `?` puede representar cualquier carácter único
  - `C:\dir\test`: sólo el archivo `C:\dir\test`
- Máscaras con ruta de acceso del archivo
  - `dir\*.*` o `dir\*`: todos los archivos en todas las carpetas `dir`
  - `dir\test`: todos los archivos de prueba en las carpetas `dir\`
  - `dir\*.exe`: todos los archivos con la extensión `exe` en todas las carpetas `dir`
  - `dir\*.ex?` : todos los archivos con la extensión `ex?` en todas las carpetas `dir`, donde `?` puede representar cualquier carácter único

Aplic confiables

Las aplicaciones confiables no se supervisan por actividad sospechosa, actividad de archivos, actividad de red e intentos de acceder al registro del sistema.

- **Agregar aplicación confiable**: se agrega la ruta completa y el nombre de archivo de un archivo ejecutable.
- **Eliminar**: elimina la ruta y el nombre de archivo de una aplicación seleccionada.

Use la notación de variable de entorno estándar para especificar la ubicación de las aplicaciones. Ejemplos:

- `%SystemRoot%\system32\svchost.exe`
- `%ProgramFiles%\Messenger\msmsgs.exe`
- `%ProgramFiles%\MSN Messenger\MsnMsgr.Exe`

URL confiables

Antivirus de Web *(página 17)* no supervisa las URL confiables en busca de virus.

- **Agregar URL confiable**: agrega una URL.
- **Eliminar**: elimina una URL seleccionada.

Instrucciones de formato:

- Introduzca `http://` o `https://` antes de cualquier dirección.
- *: úselo para representar cualquier combinación de caracteres. Ejemplo: `http://www.kaseya.com/*`
- ? : úselo para representar cualquier carácter. Ejemplo: `http://Patch_123?.com`
- Si un carácter * o ? forman parte de una URL propiamente dicha, cuando se agrega la URL a la lista de URL confiables, se debe usar una barra diagonal inversa para reemplazar el carácter * o ? que le sigue. Ejemplo: `http://www.kaseya.com/test\?`

Pestaña Extremos

Antivirus > Configuración > Perfiles > Extremos

En la pestaña **Extremos**, se enumeran todas las máquinas que usan el perfil de **Antivirus** seleccionado.

Alertas

Antivirus > Configuración > Alertas

En la página **Alertas**, se administran los perfiles de alerta de **Antivirus**. Cada perfil de alerta representa un conjunto diferente de condiciones de alerta y de acciones que se realizan ante una situación de alerta. Se pueden asignar varios perfiles de alerta al mismo extremo. Los cambios en un perfil de alerta afectan a todos los ID de máquina asignados a ese perfil. Se asigna un perfil de alerta a los ID de máquina en Antivirus > **Máquinas** *(página 13)* > **Perfiles de alerta**. Los diferentes tipos de máquinas pueden requerir diferentes perfiles de alerta. Los perfiles de alerta están visibles para todos los usuarios del VSA.

Nota: Los perfiles de alerta creados en **Antivirus** o **AntiMalware** pueden verse y editarse en ambos productos. Si se asigna un perfil de alerta a una máquina mediante **Antivirus** o **AntiMalware**, el perfil de alerta se asigna a ambos productos en esa máquina.

Revisión de alarmas creadas por alertas de Antivirus

- Monitor > **Resumen de alarmas** *(http://help.kaseya.com/webhelp/ES/VSA/7000000/index.asp#1959.htm)*
- Monitor > Lista de tablero > cualquier **ventana Resumen de alarmas** *(http://help.kaseya.com/webhelp/ES/VSA/7000000/index.asp#4112.htm)* dentro de un dashlet
- Agente > Registros de agente > **Registro de agente** *(http://help.kaseya.com/webhelp/ES/VSA/7000000/index.asp#354.htm)*
- Agente > Registros de agente > **Registro de acciones de supervisión** *(http://help.kaseya.com/webhelp/ES/VSA/7000000/index.asp#354.htm)*: muestra las medidas que se toman ante una situación de alerta, se haya creado una alarma o no.
- **Live Connect** *(http://help.kaseya.com/webhelp/ES/VSA/7000000/index.asp#4796.htm)* > Datos de agente > Registros de agente > Registro de alarmas
- Info Center > Elaboración de informes > Informes heredados > Registros > Registro de alarmas

Acciones

- **Nuevo**: crea un nuevo perfil de alerta.
- **Abrir**: abre un perfil de alerta existente para editarlo. También puede hacer doble clic en un perfil de alerta para abrirlo.
- **Eliminar**: elimina un perfil de alerta existente.
- **Guardar**: guarda los cambios en el perfil de alerta seleccionado en ese momento.

- **Copiar**: guarda el perfil de alerta seleccionado con un nombre nuevo.
- **Configuración de alertas**: configura el formato de cada tipo de mensaje de notificación de alerta.

Adición y edición de perfiles

Haga clic en **Nuevo** para visualizar la ventana **Nuevo perfil de alerta** o haga clic en un perfil existente y, a continuación, en **Abrir** para visualizar la ventana **Editar perfil de alerta**.

- Pestaña Resumen
- Pestaña Tipos de alerta
- Pestaña Acciones
- **Pestaña Extremos** *(página 27)*

Columnas de tabla

- **Nombre**: nombre del perfil de alerta.
- **Descripción**: una descripción del perfil de alerta.

Pestaña Resumen

Antivirus > Configuración > Alertas > pestaña Resumen

- **Nombre**: el nombre del perfil de alerta.
- **Descripción**: una descripción del perfil de alerta.

Pestaña Tipos de alerta

Antivirus > Configuración > Alertas > pestaña Tipos de alerta

Selección de alertas y datos de configuración

- **Seguridad eliminada por el usuario**: se desinstaló un producto de seguridad administrada del extremo.
- **Protección deshabilitada (totalidad del motor)**: se deshabilitó la protección de un producto de seguridad administrada.
- **Definición no actualizada en X días/número de días**: las definiciones de un producto de seguridad administrada no se actualizaron en un número de días específico.
- **Actualización de definición incompleta**: no se completó la actualización de las definiciones de un producto de seguridad administrada.
- **Amenaza activa detectada**: se detectó una amenaza activa. Una amenaza activa es una detección que no se subsanó ni se eliminó. Se requiere la intervención del usuario en la página **Detecciones** *(página 14)*.
- **Amenaza detectada y subsanada**: se detectó una amenaza y se la subsanó. No se requiere intervención del usuario.
- **Análisis incompleto**: no se completó el análisis.
- **Reinicio requerido**: se requiere un reinicio.
- **La licencia vence en X días/número de días**: una licencia vence en un número de días específico.
- **La licencia venció y no se renovó**: la licencia de un producto de seguridad administrada venció y no se renovó.
- **Perfil no compatible**: un extremo no es compatible con su perfil.
- **Error en la asignación de perfil**: se produjo un error en la asignación de un perfil a una máquina.

- **Error en la instalación del cliente**: se produjo un error en la instalación de un producto de seguridad administrada.
- **Error en la reparación del cliente**: se produjo un error en la reparación de un producto de seguridad administrada.
- **Error en la desinstalación del cliente**: se produjo un error en la desinstalación de un producto de seguridad administrada.

Pestaña Acciones

Antivirus > Configuración > Alertas > pestaña Acciones

En la pestaña **Acciones** de un perfil de alerta, se determinan las acciones que se llevan a cabo ante cualquiera de los **Tipos de alerta** *(página 26)* que encuentra un extremo asignado a ese perfil de alerta.

- **Crear alarma**: si está seleccionada y se encuentra un tipo de alerta, se crea una alarma.
- **Crear ticket**: si está seleccionada y se encuentra una condición de alerta, se crea un ticket.
- **Destinatarios de correo electrónico (separados por coma)**: si está seleccionada y se encuentra una condición de alerta, se envía un correo electrónico a las direcciones especificadas.
- **Ejecutar script**: si está seleccionada y se encuentra una condición de alerta, se ejecuta un procedimiento de agente.
  - **Nombre de script**: seleccione el nombre del procedimiento de agente.
- **Enviar mensaje a Info Center**: si está seleccionada y se encuentra una condición de alerta, se envía un correo electrónico a las direcciones especificadas.
  - **Seleccionar usuarios para notificar**: seleccione los usuarios a los que se les debe notificar alertas de **Antivirus** en Info Center > **Buzón de entrada** *(http://help.kaseya.com/webhelp/ES/VSA/7000000/index.asp#9460.htm)*.
- **Enviar mensaje a barra de notificación**: si está seleccionada y se encuentra una condición de alerta, se envía un correo electrónico a las direcciones especificadas.
  - **Seleccionar usuarios para notificar**: seleccione los usuarios a los que se les debe notificar de las alertas de **Antivirus** en la **Barra de notificación** *(http://help.kaseya.com/webhelp/ES/VSA/7000000/index.asp#10634.htm)*.

Pestaña Extremos

Endpoint Protection > Configuración > Alertas > Extremos

En la pestaña **Extremos**, se enumeran todas las máquinas que usan el perfil de alertas seleccionado.

Nota: En la pestaña **Perfiles de alerta** en Máquinas > Detalles, se muestra la lista de perfiles de alerta asignados a una máquina seleccionada.

Índice