Endpoint Security

Guía del usuario

Versión R91

Español

Junio 9, 2015

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

Resumen de seguridad

Endpoint Security (KES) proporciona protección de seguridad para las máquinas administradas, mediante tecnología antimalware completamente integrada de AVG Technologies. El término **malware** comprende virus, spyware, adware y otros tipos de programas no deseados. **Endpoint Security** borra o elimina automáticamente los archivos infectados y otras amenazas como troyanos, gusanos y spyware. **Endpoint Security** supervisa en forma continua el estado de seguridad de todos los servidores, las estaciones de trabajo y los equipos portátiles ligeros Windows que tienen protección de seguridad instalada. Las alarmas pueden activarse por eventos de protección de seguridad y puede significar enviar notificaciones de correo electrónico, ejecutar procedimientos y crear tickets de trabajo.

Los perfiles de seguridad administrados en forma central se definen e implementan en las máquinas mediante la interfaz de la consola del VSA. Las modificaciones en un perfil de seguridad actualizan automáticamente todas las máquinas que usan ese perfil. **Endpoint Security** cuenta con un perfil de seguridad estándar predefinido, y le permite crear perfiles de seguridad personalizados.

Todos los eventos de protección de seguridad se registran dentro del sistema y están disponibles para el resumen ejecutivo y los informes de administración detallados. Una vez distribuidos, las actualizaciones se manejan en forma automática en base a una programación sin la necesidad de intervención del usuario.

Protección anti-virus

Según el perfil de seguridad, **Endpoint Security** quita los archivos infectados o bloquea el acceso a ellos:

- **Escanea el registro del sistema** en busca de entradas sospechosas, archivos de Internet temporales, cookies de rastreo y otros tipos de objetos no deseados.
- **Detecta virus en computadoras** mediante:
  - **Escaneos** : realiza escaneos al acceder y por demanda.
  - **Análisis heurístico** : emula dinámicamente las instrucciones del objeto escaneado dentro de un entorno informático virtual.
  - **Detección genérica** : detecta las instrucciones características de un virus o grupo de virus.
  - **Detección de virus conocido** : busca las cadenas de caracteres características de un virus.
- **Escanea correos electrónicos** : controla los correos electrónicos entrantes y salientes mediante el uso de complementos diseñados para los programas de correo electrónico más frecuentemente usados. Una vez detectados, los virus se borran o se colocan en cuarentena. Algunos clientes de correos electrónicos pueden aceptar mensajes con texto certificando que los correos electrónicos enviados y recibidos se han escaneado en busca de virus. Además, para tener un mayor nivel de seguridad al trabajar con correos electrónicos, se puede fijar un filtro de adjuntos definiendo archivos no deseados o sospechosos.
- **Protección residente en la memoria** : escanea archivos cuando se copian, abren o guardan. Si se descubre un virus, se detiene el acceso al archivo y no se permite que el virus se active. La protección residente en la memoria se carga en la memoria de la computadora al iniciar el sistema y proporciona protección vital para las áreas del sistema de la misma.
- **Escaneos por demanda** : los escaneos pueden ejecutarse por demanda o programarse para su ejecución periódica en los horarios convenientes.
- **Escanea servidores MS Exchange** : escanea los mensajes de correos electrónicos entrantes y salientes y las carpetas de los buzones en los servidores MS Exchange contra las amenazas de virus/spyware/malware y los elimina inmediatamente antes de que los destinatarios de los correos electrónicos del servidor MS Exchange se infecte.

- **Escanea sitios de la Web y las descargas** : escanea sitios de la Web y vínculos de sitios de la Web. También escanea archivos descargados a la computadora. Proporciona una calificación de seguridad para los vínculos devueltos por motores de búsqueda populares.
- **Protección de ID** : previene el robo dirigido a las contraseñas, detalles de cuantas bancarias, números de tarjetas de crédito y otros valores digitales usando un "análisis de comportamiento" para indicar actividades sospechosas en la máquina.

Anti-Spyware

Spyware es un software que reúne información de la computadora sin el conocimiento o consentimiento del usuario. Algunas aplicaciones del spyware pueden también instalarse en forma secreta y a menudo contienen publicidad, ventanas emergentes o tipos distintos de software no deseado. Actualmente, la fuente de infección más común son los sitios Web con contenidos potencialmente peligrosos. Otros métodos de transmisión incluyen los correos electrónicos o la transmisión por gusanos y virus. La protección más importante contra el spyware es usar una **protección residente en la memoria**, como el componente de spyware de **Endpoint Security** de avanzada. La protección residente en la memoria analiza las aplicaciones en segundo plano a medida que se ejecutan. La protección antispyware de **Endpoint Security** detecta spyware, adware, troyanos DLL, registradores de pulsaciones de teclas, malware oculto en flujos de datos, archivos, entradas de spyware en el Registro de Windows y otros tipos de objetos no deseados.

Nota: Consulte Requisitos del sistema para Endpoint Security.

Licencias de Endpoint Security

Cada licencia de puestos de MSE KES permite al cliente instalar y usar un agente de MSE KES de manera continua, así como recibir actualizaciones por un período de suscripción de 365 días consecutivos. La actualización del período de suscripción se ejecuta en forma independiente para cada puesto, y comienza el día de la compra del agente de MSE KES en una máquina y permite que el puesto reciba las actualizaciones de KES lanzadas durante dicho período. Todas las actualizaciones lanzadas durante el período de suscripción también cuentan con licencia de manera continua, siempre y cuando finalice el derecho de recibir nuevas actualizaciones de KES al término del período de suscripción o si este no se renueva.

La emisión de una nueva Licencia del usuario para una máquina con un Termino de suscripción ocasiona que los Términos se fusionen y por consiguiente agrega 365 días al tiempo que caso contrario le quedaría al Término de la suscripción del usuario. Cualquier transferencia de dicho Término fusionado a una nueva máquina ocasionará que todos los días restantes de ambos usuarios anteriores se transfieran.

Se debe obtener la licencia de puestos de KES adecuada para cada máquina o Buzón de Exchange protegido. El cliente sólo puede implementar MSE KES en una máquina que tenga una licencia del VSA válida. Las licencias de MSE KES pueden administrarse de manera central con la interfaz de usuario del sitio web de Kaseya. Las licencias se implementan, y se necesita una licencia para cada buzón que se usa.

Nota: Las licencias de KES se asignan a los ID de grupo en Sistema > **Administrador de licencias** *(http://help.kaseya.com/webhelp/ES/VSA/9010000/index.asp#2924.htm).*

Funciones	Descripción
Tablero *(página 3)*	Proporciona una vista de tablero del estado de todas las máquinas que tienen instalado Endpoint Security.
Estado de Seguridad *(página 10)*	Muestra el estado actual de la seguridad de las ID de máquinas.
Actualización Manual *(página 8)*	Programa actualizaciones de la última versión de los archivos de definición de protección de seguridad.
Programar	Programa los escaneos de protección de seguridad de las

Exploración *(página 10)*	ID de máquinas.
Ver Amenazas *(página 11)*	Lista los archivos que se han colocado en cuarentena debido a una amenaza sospechada o confirmada.
Ver Registros *(página 13)*	Muestra el registro de eventos de protección de seguridad de las ID de máquinas.
Extender/Regresar *(página 14)*	Extiende el conteo de las licencias anuales para ID de máquinas seleccionadas o devuelve las licencias anuales de las ID de máquinas seleccionadas.
Notificar *(página 16)*	Proporciona una notificación automática del vencimiento de las licencias de Endpoint Security.
Instalación *(página 17)*	Instala o remueve la protección de seguridad para las ID de máquinas.
Definir Perfil *(página 22)*	Administra los perfiles de seguridad. Cada perfil de seguridad representa un grupo distinto de opciones de seguridad habilitadas o deshabilitadas.
Asignar Perfil *(página 30)*	Asigna los perfiles de seguridad a las ID de máquinas.
Configuración del registro *(página 30)*	Especifica la cantidad de días para retener los datos del registro de protección de seguridad.
Estado de Exchange *(página 31)*	Muestra el estado de la protección de correo electrónico en los servidores MS Exchange que tienen instalado Endpoint Security.
Definir Conjuntos de Alarma *(página 33)*	Define los conjuntos de condiciones de alerta que se usan para desencadenar las alertas en la página Aplicar conjuntos de alarmas.
Aplicar Conjuntos de Alarma *(página 34)*	Crea alarmas como respuesta a los eventos de protección de seguridad.

Requisitos del módulo Endpoint Security

Kaseya Server

- El módulo Endpoint Security R91 requiere el VSA R91.
- Acceso a `http://download.avg.com`

Requisitos para todas las máquinas administradas

- 256 MB de RAM
- 60 MB de espacio libre en disco
- Microsoft Windows Server 2003, 2003 R2, 2008, 2008 R2, 2012, 2012 R2
- Microsoft Windows XP SP3, Vista, 7, 8, 8.1

Nota: Consulte **Requisitos generales del sistema** *(http://help.kaseya.com/WebHelp/EN/VSA/9010000/reqs/index.asp#home.htm).*

Tablero

Seguridad > Tablero

- Se proporciona información similar en Info Center > Elaboración de informes > Informes > Seguridad.

En la página **Tablero**, se proporciona una vista de tablero del estado de las máquinas que tienen instalado **Endpoint Security**.

- **Estadísticas de Seguridad de Terminales**
- **Estado de Licencia**
- **Recuento de licencias**
- **Máquinas Superiores con Amenazas**
- **Amenazas Superiores Descubiertas**

Nota: La lista de ID de máquina que se muestra depende del filtro ID de máquina/ID de grupo y de los grupos de máquinas que el usuario está autorizado a ver mediante el uso de Sistema > Seguridad de usuarios > Ámbitos.

Estadísticas de Seguridad de Terminales

La sección **Estadística de seguridad de extremos** proporciona varias estadísticas acerca del estado de la seguridad de los extremos y del estado de las definiciones de seguridad.

- <N> Los extremos requieren un reinicio.
- <N> Las versiones de firma son anteriores a '<version>'.
- <N> Los extremos tienen versiones anteriores de **Endpoint Security**.
- <N> No se completó el análisis de los extremos esta semana.
- <N> Actualmente se están analizando los extremos.
- <N> La protección residente no está habilitada en los extremos.

Haga clic en una estadística del hipervínculo para ver un diálogo de opciones que muestra cada miembro que pertenece a dicha estadística.

Estado de Licencia

Un gráfico de torta muestra el porcentaje de máquinas cuyas licencias vencieron o hubiesen vencido en 30, 60, 90 ó 91+ días. Haga clic en una porción del gráfico o en cualquier nivel del gráfico para mostrar una lista de máquinas individuales pertenecientes a dicha porción.

Recuento de licencias

Nota: As of version 9.1 licensing sets the expiration date of the license to one year from the day it is purchased, irrespective of the day it is installed. The expiration dates of existing licenses are not affected by this change.

Se indican los recuentos de licencias para lo siguiente:

- Licencias compradas
- Licencias completamente disponibles (compradas no asignadas, instaladas o vencidas)
- Licencias asignadas (programadas para instalación, pero la instalación aún no está completa)
- Licencias aplicadas (licencia activa aplicada a una máquina)
- Licencias parcialmente disponibles (asignadas antes a una máquina, pero devueltas al grupo antes del vencimiento)
- Licencias asignadas parcialmente (disponibles parcialmente y programadas para la instalación pero todavía sin instalación completa)
- Licencias totales (licencias compradas menos las vencidas)
- Licencias expiradas

Máquinas Superiores con Amenazas

Lista las máquinas con la mayor cantidad de amenazas actuales. También se lista la cantidad de amenazas en la bóveda de virus. Al hacer clic en la ID de máquina con hipervínculo se muestran las amenazas pertenecientes a dicha ID de máquina en la página **Ver amenazas** *(página 11)* .

Amenazas Superiores Descubiertas

El gráfico de torta muestra las amenazas que se encontraron en la mayor parte de las máquinas. Haga clic en una porción del gráfico de torta o en cualquier nivel del gráfico para mostrar una lista de máquinas individuales pertenecientes a dicha porción en la página **Ver amenazas**.

Estado de Seguridad

Seguridad > Estado de seguridad

- Se proporciona información similar en Info Center > Elaboración de informes > Informes > Seguridad *(página 37)*.

En la página **Estado de seguridad**, se muestra el estado de seguridad actual de cada ID de máquina con licencia para usar **Endpoint Security**. La lista de ID de máquina que se muestra depende del filtro ID de máquina/ID de grupo y de los grupos de máquinas que el usuario está autorizado a ver mediante el uso de Sistema > Seguridad de usuarios > Ámbitos. Para que se muestren en esta página, los ID de máquina deben tener el software cliente de **Endpoint Security** instalado en la máquina administrada mediante la página **Instalación** *(página 17)* en Seguridad.

Los indicadores incluyen la protección de la Protección residente, protección de correo, la cantidad de amenazas detectadas no resueltas, la cantidad de amenazas en la bóveda de virus y la protección de seguridad instalada en cada ID de máquina.

Acciones

- **Habilitar Protección residente** : haga clic para habilitar la protección anti-malware de la memoria residente en las ID de máquinas seleccionadas.
- **Deshabilitar Protección residente** : haga clic para deshabilitar la protección anti-malware de la memoria residente en las ID de máquinas seleccionadas.

  Nota: En algunos casos, la protección de seguridad se debe deshabilitar para instalar o configurar software en una máquina administrada.

  Nota: También puede **habilitar o deshabilitar Protección residente por procedimiento de agente** *(página 7)*.

- **Habilitar correo electrónico** : haga clic para habilitar la protección de correos electrónicos en las ID de máquinas seleccionadas.
- **Deshabilitar correo electrónico** : haga clic para deshabilitar la protección de correos electrónicos en las ID de máquinas seleccionadas.
- **Vaciar bóveda de virus** : haga clic para vaciar la bóveda de virus de todas las ID de malware en cuarentena.
- **Reiniciar ahora** : reinicia las ID de máquinas seleccionadas. Algunas actualizaciones de seguridad requieren un reinicio para instalar la actualización. Si hay un reinicio pendiente, se muestra un ícono de reiniciar al lado del número de la versión de la pre-actualización y la máquina sigue protegida.

Información de encabezado

- **Versión actual de firma disponible**: la versión más reciente disponible de la protección de seguridad. Puede actualizar un ID de máquina o más con la **versión actual disponible** en Seguridad > **Actualizaciones manuales** *(página 34)*.
- **Versión actual del instalador**: el número de versión del instalador de AVG que se usa en las instalaciones nuevas.

Columnas de tablas

- **Íconos de registro**: Estos íconos indican el estado de registro del agente de cada máquina administrada. Al desplazar el cursor sobre un ícono de registro, se muestra la ventana de Vista rápida 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
- **(Casilla de verificación Seleccionar todo)**: haga clic en esta casilla de verificación para seleccionar todas las filas en el área de paginación. Si está tildada, haga clic en esta casilla para destildar todas las filas en el área de paginación.
- **Machine.Group ID**: Un nombre de ID de máquina, ID de grupo o ID de organización exclusivo para una máquina del VSA.
- **Nombre de perfil**: el perfil de seguridad asignado al ID de máquina.
- **Estado**: el estado actual de la protección de seguridad para un ID de máquina se indica mediante el conjunto de íconos de estado que se muestran en la columna **Estado**. Los posibles íconos de estado incluyen:


Protección residente conectado


Protección residente desconectado


Protección residente parcial


Habilitación/Deshabilitación pendiente de Protección residente


Escaneo de correo electrónico conectado


Escaneo de correo electrónico desconectado


Escaneo de correo electrónico parcial


Habilitación/Deshabilitación pendiente de escaneo de correo electrónico


Escaneo vínculo conectado


Escaneo vínculo desconectado


Escaneo vínculo parcial


Habilitación/Deshabilitación pendiente de escaneo vínculo


Protección de Web conectado


Protección de Web desconectado


Protección de Web parcial


Habilitación/Deshabilitación pendiente de protección de Web

- **Amenazas**: la cantidad de amenazas no reparadas detectadas en el ID de máquina. Son amenazas actuales que requieren la atención del usuario. Puede hacer clic en el número con hipervínculo de una fila para mostrar estas amenazas en la pestaña **Amenazas actuales** de la página **Ver amenazas** *(página 11)* .
- **Bóveda de virus**: la cantidad de amenazas almacenadas en la bóveda de virus del ID de máquina. Estos elementos están en cuarentena en forma segura y se eliminarán automáticamente si se aplica la configuración de perfil. Puede hacer clic en el número con hipervínculo en cualquier fila para mostrar estas amenazas en la pestaña **Bóveda de virus** en la página **Ver amenazas** *(página 11)*.
- **Versión**: La versión de protección de seguridad que usa actualmente este ID de máquina. Por ejemplo: `8.5.322 270.12.6/2084`
  - `8.5.322`: la versión instalada del programa AVG.
  - `270.12.6/2084`: la versión completa de la *base de datos* de virus. `270.12.6` representa la versión de *definición* y `2084` es la versión de *firma*. De muestra el texto en color rojo si la versión de la *firma* es anterior que las últimas 5 versiones de *firmas* disponibles o si la versión de la *definición* es anterior que las 2 últimas versiones de *definición* disponibles y el agente está activo.

> **Nota:** Si la versión del ID de máquina está desactualizada, puede actualizar los ID de máquina manualmente en Seguridad > **Actualización manual** *(página 8)*.
>
> **Nota:** Algunas actualizaciones de seguridad requieren un reinicio para instalar la actualización. Si hay un reinicio pendiente, se muestra un ícono de reiniciar al lado del número de la versión de la pre-actualización y la máquina sigue protegida.

Habilitar/Deshabilitar Protección residente por procedimiento de agente

Puede habilitar o deshabilitar la **protección residente** con el comando **executeShellCommand()** en un procedimiento de agente. En el **directorio de trabajo** *(http://help.kaseya.com/webhelp/ES/VSA/9010000/index.asp#368.htm)* del agente, ejecute:

```
C:\kworking\kes>KasAVCmd -setFileMonitorEnable 0   ;disables Resident Shield
C:\kworking\kes>KasAVCmd -setFileMonitorEnable 1   ;enables Resident Shield
```

```
Script Name: KES_Enable Resident Shield
Script Description: Enables Resident Shield temporarily (until next scan or
reboot...unless it is enabled by default and is being re-enabled after being
temporarily disabled)
IF True
THEN
   Get Variable
     Parameter 1 : 10
     Parameter 2 :
     Parameter 3 : agenttemp
         OS Type : 0
   Execute File
     Parameter 1 : #agenttemp#\kes\KasAVCmd.exe
     Parameter 2 : -setFileMonitorEnable 1
     Parameter 3 : 3
         OS Type : 0
ELSE
```

```
Script Name: KES_Disable Resident Shield
Script Description: Disables Resident Shield temporarily (until next scan or reboot)
IF True
THEN
   Get Variable
     Parameter 1 : 10
     Parameter 2 :
     Parameter 3 : agenttemp
         OS Type : 0
   Execute File
     Parameter 1 : #agenttemp#\kes\KasAVCmd.exe
     Parameter 2 : -setFileMonitorEnable 0
     Parameter 3 : 3
         OS Type : 0
ELSE
```

Actualización Manual

Seguridad > Actualización manual

En la página **Actualizaciones manuales**, se controla la actualización de los ID de máquina con licencia para usar **Endpoint Security** con la versión más reciente disponible de la protección de seguridad. *Las actualizaciones se programan automáticamente en forma predeterminada.* Puede deshabilitar y volver a habilitar las actualizaciones automáticas por máquina. Esta función, por lo general, solo se utiliza para revisar el estado de actualización de los agentes o para forzar una verificación inmediata de la actualización, si es necesario.

La lista de los ID de máquina que puede seleccionar depende del filtro ID de máquina / ID de grupo y el ámbito que usa. Para que se muestren en esta página, los ID de máquina deben tener el software cliente de **Endpoint Security** instalado en la máquina administrada mediante la página **Instalación** *(página 17)* en Seguridad.

Acciones

- **Actualizar** : haga clic para programar una actualización de definiciones de virus en las ID de máquinas seleccionadas, mediante el uso de las opciones de actualización previamente seleccionadas.
- **Cancelar actualización** : haga clic para borrar la actualización programada.
- **Habilitar actualizaciones automáticas** :habilita las actualizaciones de las definiciones de virus.
- **Deshabilitar actualizaciones automáticas** :deshabilita las actualizaciones de las definiciones de virus. Esto hace que las actualizaciones de las definiciones de virus no hagan más lenta la red durante las horas laborales picos. En una versión futura podrá programar cuándo actualizar las definiciones de virus. Si se deshabilitan las actualizaciones automáticas, un ícono con una cruz roja se muestra en la columna **Hora programada** , incluso si se programa una actualización manual.

Información de encabezado

- **Versión actual disponible**: la versión más reciente disponible de la protección de seguridad. Compruebe la columna de la versión en esta página para determinar si a algún ID de máquina le falta la versión más actualizada de la protección de seguridad o el software cliente de **Endpoint Security** más reciente disponible.
- **Versión actual del cliente de KES**: el software cliente de KES más reciente disponible.

Configuración de programación

- **Inmediato**: active esta casilla de verificación para programar esta tarea de inmediato.
- **Fecha/Hora**: introduzca el año, el mes, el día, la hora y los minutos para programar esta tarea.
- **Escalonar cada**: puede distribuir la carga en la red si escalona esta tarea. Si configura este parámetro en 5 minutos, la tarea en cada ID de máquina se escalona cada 5 minutos. Por ejemplo, máquina 1 ejecuta a las 10:00, máquina 2 ejecuta a las 10:05, máquina 3 ejecuta a las 10:10, ...
- **Omitir si la máquina está desconectada**: si se muestra una marca de verificación y la máquina está desconectada, omita y ejecute el siguiente período y hora programados. Si no se muestra el tilde, realice la tarea tan pronto como la máquina se conecte después de la hora programada.
- **Actualizar desde KServer (reemplazar origen de archivo)**: si está seleccionada, las actualizaciones se descargan de Kaseya Server. Si no está seleccionada, las actualizaciones se descargan con el método especificado en Administración de parches > **Origen de archivo** *(http://help.kaseya.com/webhelp/ES/VSA/9010000/index.asp#366.htm)*.

Columnas de tabla

- **Estado de registro**: Estos íconos indican el estado de registro del agente de cada máquina administrada. Al desplazar el cursor sobre un ícono de registro, se muestra la ventana de Vista rápida 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
- **(Casilla de verificación Seleccionar todo)**: haga clic en esta casilla de verificación para seleccionar todas las filas en el área de paginación. Si está tildada, haga clic en esta casilla para destildar todas las filas en el área de paginación.

- **Machine.Group ID**: Un nombre de ID de máquina, ID de grupo o ID de organización exclusivo para una máquina del VSA.
- **Origen**: si se define un origen de archivo en Administración de parches > Origen de archivo, las actualizaciones se originan en esta ubicación. Caso contrario, las actualizaciones usan las fuentes desde Internet. Si la opción **Descargar de Internet si la máquina no puede conectarse al servidor de archivos** está seleccionada en Administración de parches>Origen de archivo:
  - Durante la instalación del extremo **Endpoint Security** v2.x, si el origen de los archivos está inactivo o las credenciales no son válidas, el instalador se descarga de Kaseya Server y se completa la instalación del extremo.
  - Durante la actualización manual de **Endpoint Security** v2.x, si el origen de los archivos está inactivo o las credenciales no son válidas, la actualización se descarga de Internet.

  En los dos casos anteriores, la página **Ver registros** *(página 13)* muestra un mensaje de error indicando por qué falló la fuente del archivo y que está intentando descargar desde Internet.
- **Última actualización**: Este marca del reloj fechador aparece cuando una ID de máquina se actualizó por última vez. Cuando cambia esta fecha, una nueva actualización está disponible para ser usada.
- **Versión**: La versión de protección de seguridad que usa actualmente este ID de máquina. Por ejemplo: `8.5.322 270.12.6/2084`
  - `8.5.322`: la versión instalada del programa AVG.
  - `270.12.6/2084`: la versión completa de la *base de datos* de virus. `270.12.6` representa la versión de *definición* y `2084` es la versión de *firma*. De muestra el texto en color rojo si la versión de la *firma* es anterior que las últimas 5 versiones de *firmas* disponibles o si la versión de la *definición* es anterior que las 2 últimas versiones de *definición* disponibles y el agente está activo.
  - `[KES 2.1.0.87]`: la versión del software cliente de **Endpoint Security**.
- **Hora programada**: la marca de hora que muestra la siguiente actualización programada, si se programa una en forma manual o automática. Para una máquina seleccionada:
  - Si *las actualizaciones automáticas se habilitan* para una máquina selecciona da y KES detecta una actualización AVG, se muestra una marca del reloj fechador. Cuando se programan múltiples máquinas, las marcas del reloj fechador diferirán porque las actualizaciones automáticas usan una programación escalonada.
  - Si *las actualizaciones automáticas están habilitadas* pero no se detecta actualización AVG, la celda de la tabla estará en blanco, al menos que también se programe una actualización manual.
  - Si *las actualizaciones automáticas están deshabilitadas*, el ícono de la cruz roja se muestra, incluso si está programada una actualización manual.
  - Si *está programada una actualización manual*, se muestra la marca del reloj fechador.

Programar Exploración

Seguridad > Programar análisis

En la página **Programar análisis**, se programan análisis de protección de seguridad de los ID de máquina seleccionados con licencia para usar **Endpoint Security**. La lista de los ID de máquina que puede seleccionar depende del filtro ID de máquina / ID de grupo y el ámbito que usa. Para que se muestren en esta página, los ID de máquina deben tener el software cliente de **Endpoint Security** instalado en la máquina administrada mediante la página **Instalación** *(página 17)* en Seguridad.

Acciones

- **Escanear** : haga clic para programar un escaneo de las ID de máquinas seleccionadas usando las opciones de escaneo previamente seleccionadas.
- **Cancelar** : haga clic para borrar el escaneo programado.

Configuración de programación

- **Inmediato**: active esta casilla de verificación para programar esta tarea de inmediato.
- **Fecha/Hora**: introduzca el año, el mes, el día, la hora y los minutos para programar esta tarea.
- **Escalonar cada**: puede distribuir la carga en la red si escalona esta tarea. Si configura este parámetro en 5 minutos, la tarea en cada ID de máquina se escalona cada 5 minutos. Por ejemplo, máquina 1 ejecuta a las 10:00, máquina 2 ejecuta a las 10:05, máquina 3 ejecuta a las 10:10, ...
- **Omitir si la máquina está desconectada**: si se muestra una marca de verificación ✔ y la máquina está desconectada, omita y ejecute el siguiente período y hora programados. Si no se muestra el tilde, realice la tarea tan pronto como la máquina se conecte después de la hora programada.
- **Cada N períodos**: Tilde la casilla para que esta tarea sea una tarea recurrente. Ingrese la cantidad de períodos a esperar antes de ejecutar esta tarea nuevamente.

Columnas de tabla

- **Estado de registro**: Estos íconos indican el estado de registro del agente de cada máquina administrada. Al desplazar el cursor sobre un ícono de registro, se muestra la ventana de Vista rápida 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
- **(Casilla de verificación Seleccionar todo)**: haga clic en esta casilla de verificación para seleccionar todas las filas en el área de paginación. Si está tildada, haga clic en esta casilla para destildar todas las filas en el área de paginación.
- **Machine.Group ID**: Un nombre de ID de máquina, ID de grupo o ID de organización exclusivo para una máquina del VSA.
- **Último análisis**: esta marca de hora muestra el momento en que se realizó el último análisis. Cuando cambia esta fecha, hay nuevos datos de escaneo disponibles.
- **Siguiente análisis/Programación**: Esta marca de reloj fechador muestra el siguiente escaneo programado. Las marcas de la fecha y hora de vencimiento se muestran en texto en rojo resaltado en amarillo. Un tilde verde ✔ indica que el escaneo es recurrente.

Ver Amenazas

Seguridad > Ver amenazas

- Se proporciona información similar en Info Center > Elaboración de informes > Informes > Seguridad *(página 37)*.

La página **Ver amenazas** muestra las amenazas sobre las que puede accionar. Las amenazas se agrupan por su estado en dos pestañas diferentes:

- **Amenazas actuales** : lista las amenazas descubiertas en máquinas que pueden repararse en forma automática. Cada amenaza no reparada se mantiene son cambios en la máquina, requiriendo la acción del usuario. Eliminar una amenaza en la pestaña **Amenazas actuales** elimina inmediatamente el archivo, sin moverlo a la **Bóveda de virus**.

  Nota: Cuando se analiza una máquina, todas las amenazas actuales se borran y se marcan como resueltas. Si la amenaza continua existiendo, se redescubre y vuelve a agregar a la lista de amenazas actuales.

- **Bóveda de virus** : las amenazas se descubren mediante el escaneo o la protección residente. Reparar la amenaza reemplaza el archivo original por una copia reparada. El archivo original no reparado se mueve a una partición oculta en la unidad del disco duro de la computadora llamada **Bóveda de virus**. En efecto, la **Bóveda de virus** actúa como un tipo de "papelera de reciclaje" para amenazas, permitiéndole recuperarlos antes de eliminarlo permanentemente de las máquinas.

Reparar

Reparar involucra los siguientes pasos:

1. Se ha hecho un intento para borrar el archivo.
2. Si esto falla, se hace el intento de mover el archivo a la **Bóveda de virus**.
3. Si eso falla, se hace el intento de eliminar el archivo.
4. Si eso falla, el archivo sigue sin cambios en la máquina y se lista en la pestaña de **Amenazas actuales** de la página **Ver amenazas** .

Amenazas del servidor MS Exchange

Cualquier malware detectado por la protección de correo electrónico del servidor MS Exchange se elimina inmediatamente del servidor MS Exchange y se muestra *solo* en la pestaña **Bóveda de virus** .

Pestaña Amenazas actuales

Acciones

- **Reparar** : intenta reparar el archivo sin eliminarlo. Las amenazas reparadas se remueven de la pestaña **Amenazas actuales** y se muestran en la pestaña **Bóveda de virus** .
- **Eliminar** : intenta eliminar el archivo. Las amenazas eliminadas se eliminan inmediatamente de la computadora.

  Nota: Si fallan la reparación y la eliminación, es posible que el archivo esté abierto. Cierre cualquier proceso que mantenga el archivo abierto e intente nuevamente eliminarlo.

- **Remover de esta lista** : remueve la amenaza de la página **Ver amenazas** sin realizar otra acción.
- **Cancelar operación pendiente** : cancela cualquier otra acción, si aún no se han completado.
- **Agregar a la lista de exclusión de PUP**: se identifica una amenaza como un posible programa no deseado, o PUP, con una `(P)` junto al nombre de la amenaza en la página **Ver amenazas**. Las amenazas PUP pueden agregarse a la lista de exclusión para el perfil asignado a la máquina en la que se encontraron. Exclusión significa que el archivo ya no se escanea como amenaza potencial en *todas* las máquinas con este perfil asignado. Solo realice esta acción si está seguro que el archivo es seguro de usar. Toda la lista de exclusión de PUP se mantiene en la pestaña Exclusiones de PUP en **Definir perfil** *(página 22)*.

  Nota: Las amenazas que no son PUP no se pueden agregar a la lista de exclusión de PUP.

Pestaña Bóveda de virus

Acciones

- **Restaurar** : restaura el archivo original identificado como una amenaza. Solo realice esta acción si está seguro que el archivo es seguro de usar.
- **Eliminar** : elimina el archivo original identificado como una amenaza desde la **Bóveda de virus**.

> **Nota:** No puede recuperar un archivo eliminado de la **Bóveda de virus**.

- **Remover de esta lista** : remueve la amenaza de la página **Ver amenazas** sin realizar otra acción.
- **Cancelar operación pendiente** : cancela cualquier otra acción, si aún no se han completado.
- **Agregar a la lista de exclusión de PUP**: se identifica una amenaza como un posible programa no deseado, o PUP, con una `(P)` junto al nombre de la amenaza en la página **Ver amenazas**. Las amenazas PUP pueden agregarse a la lista de exclusión para el perfil asignado a la máquina en la que se encontraron. Exclusión significa que el archivo ya no se escanea como amenaza potencial en *todas* las máquinas con este perfil asignado. Solo realice esta acción si está seguro que el archivo es seguro de usar. Toda la lista de exclusión de PUP se mantiene en la pestaña Exclusiones de PUP en **Definir perfil** *(página 22)*.

> **Nota:** Las amenazas que no son PUP no se pueden agregar a la lista de exclusión de PUP.

Aplicar filtro / Reconfigurar filtro

Haga clic en **Aplicar filtro** para filtrar las filas mostradas por el texto ingresado en los campos **Machine.Group**, **Ruta de amenaza** o **Nombre de amenaza**. El filtro de la **Fecha y hora** y la clasificación de la **Acción** ocurren en forma inmediata. Haga clic en **Reconfigurar filtro** para mostrar todas las filas de datos.

Filtrar columnas

Filtre las amenazas usando campos de texto, un rango de fecha y/o listas desplegables. Incluya un comodín con asterisco (*) con el texto que ingresa para coincidir con registros múltiples.

- **Machine.Group** : filtre por el machine ID.group ID de las máquinas administradas que informan amenazas.
- **Ruta de amenaza** : filtre por la ubicación del nombre de la ruta de los archivos en las máquinas administradas con amenazas informadas.
- **Fecha y hora** : filtre por rango de fechas y horas en que las amenazas se detectaron por *última vez*. El filtrado por **Fecha y hora** ocurre en forma inmediata.
- **Nombre de amenaza** : filtre por el nombre de la amenaza, según lo designado por las definiciones de anti-malware usadas para detectar una amenaza.
- **Acción** : filtre por las acciones pendientes o completadas tomadas contra la visualización de los registros de amenazas. Seleccione `All OFF` o `All ON` para habilitar o deshabilitar las acciones. La clasificación de las acciones ocurre en forma inmediata.

Ver Registros

Seguridad > Ver registros

- Se proporciona información similar en Info Center > Elaboración de informes > Informes > Seguridad *(página 37)*.

En la página **Ver registros**, se muestra el registro de eventos de protección de seguridad de cada ID de máquina con licencia para usar **Endpoint Security**. La lista de ID de máquina que se muestra depende del filtro ID de máquina/ID de grupo y de los grupos de máquinas que el usuario está autorizado a ver mediante el uso de Sistema > Seguridad de usuarios > Ámbitos. Para que se muestren en esta página, los ID de máquina deben tener el software cliente de **Endpoint Security** instalado en la máquina administrada mediante la página **Instalación** *(página 17)* en Seguridad.

Haga clic en la machine ID.group ID para mostrar un registro de eventos Cada evento muestra la **Hora**, un **Código**de eventos y en la mayoría de los casos un **Mensaje** que contiene información adicional. Los

códigos de eventos de protección de seguridad describen uno de los siguientes tres tipos de entrada de registro:

- Errores
- Eventos
- Comandos

Aplicar filtro / Reconfigurar filtro

Haga clic en **Aplicar filtro** para filtrar las filas por rango de fecha ingresado en los campos de **Hora** y/o el texto ingresado en el campo de **Mensaje**. Haga clic en **Reconfigurar filtro** para mostrar todas las filas de datos.

Filtrar columnas

Filtre las amenazas usando campos de texto, un rango de fecha y/o listas desplegables. Incluya un comodín con asterisco (*) con el texto que ingresa para coincidir con registros múltiples. Las filas de paginación pueden ordenarse haciendo clic en los vínculos de los encabedos de las columnas.

- **Hora, mín, máx**: filtre por rango de fechas y horas.
- **Código**: filtre por categoría de evento de registro informado. Seleccione `All OFF` o `All ON` para habilitar o deshabilitar todas las categorías.
- **Mensaje**: filtre por mensaje de texto.

Extender/Regresar

Seguridad > Extender/Devolver

La página **Extender/Devolver** extiende el conteo de las licencias anuales para ID de máquinas seleccionadas o devuelve las licencias anuales de las ID de máquinas seleccionadas. Se puede devolver una licencia anual de una ID de máquina y aplicarse a otra ID de máquina. A cada ID de máquina se le pueden asignar múltiples años de protección de seguridad. Las licencias de **Endpoint Security** se asignan a los ID de grupo en Sistema > **Administrador de licencias** *(http://help.kaseya.com/webhelp/ES/VSA/9010000/index.asp#2924.htm)*.

> **Nota:** Consulte **Licencias de Endpoint Security** en el tema **Descripción general de seguridad** *(página 2)*.

La lista de los ID de máquina que puede seleccionar depende del filtro ID de máquina / ID de grupo y el ámbito que usa. Para que se muestren en esta página, los ID de máquina deben tener el software cliente de **Endpoint Security** instalado en la máquina administrada mediante la página **Instalación** *(página 17)* en Seguridad.

Acciones

- **Extender** : extiende el conteo de licencias anuales para las ID de máquinas seleccionadas.
- **Devolver** : devuelve las licencias anuales de las ID de máquinas seleccionadas.
- **Extender automático** : habilita la asignación automática de una nueva licencia el día que vence la licencia anterior para las ID de máquinas seleccionadas. Sólo se asignan licencias completas con **Extensión automática**. Si no existen licencias adicionales, falla la asignación y vence la protección de seguridad para el extremo. Deshabilitado en forma predeterminada.
- **Remover extender automático** : deshabilita extender automático para las ID de máquinas seleccionadas.
- **Recuento de licencias**: se muestra una ventana emergente con los siguientes recuentos de licencias:
  - Licencias compradas

- Licencias completamente disponibles (compradas no asignadas, instaladas o vencidas)
- Licencias asignadas (programadas para instalación, pero la instalación aún no está completa)
- Licencias aplicadas (licencia activa aplicada a una máquina)
- Licencias parcialmente disponibles (asignadas antes a una máquina, pero devueltas al grupo antes del vencimiento)
- Licencias asignadas parcialmente (disponibles parcialmente y programadas para la instalación pero todavía sin instalación completa)
- Licencias totales (licencias compradas menos las vencidas)
- Licencias expiradas

> **Nota:** As of version 9.1 licensing sets the expiration date of the license to one year from the day it is purchased, irrespective of the day it is installed. The expiration dates of existing licenses are not affected by this change.

- **Mostrar sólo las licencias que vencen en 30 días**: limita las licencias que se muestran en el área de paginación a aquellas que vencen dentro de los 30 días.

Columnas de tabla

- **(Estado de registro)**: Estos íconos indican el estado de registro del agente de cada máquina administrada. Al desplazar el cursor sobre un ícono de registro, se muestra la ventana de Vista rápida 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
- **(Casilla de verificación Seleccionar todo)**: haga clic en esta casilla de verificación para seleccionar todas las filas en el área de paginación. Si está tildada, haga clic en esta casilla para destildar todas las filas en el área de paginación.
- **Machine.Group ID**: Un nombre de ID de máquina, ID de grupo o ID de organización exclusivo para una máquina del VSA.
- **Retornable**: el recuento de licencias anuales retornables de un ID de máquina. Un ID de máquina con sólo una licencia anual no puede devolver ninguna licencia anual adicional.
- **Fecha de caducidad**: la fecha en que vence la protección de seguridad de un ID de máquina sobre la base del recuento de licencias anuales que tiene.
- **Extensión automática**: si está seleccionada, se habilita la extensión automática para este ID de máquina.
- **En el límite**: si se usa el recuento máximo de licencias anuales disponibles para un ID de grupo, cada ID de máquina con licencia en dicho ID de grupo muestra `Yes` en la columna **En el límite**. Esto anuncia al usuario que es posible que se requieran más licencias anuales para ese ID de grupo. Las licencias de **Endpoint Security** se asignan a los ID de grupo en Sistema > **Administrador de licencias** *(http://help.kaseya.com/webhelp/ES/VSA/9010000/index.asp#2924.htm)*.

Notificar

Seguridad > Notificar

En la página **Notificar**, se proporciona una notificación automática del vencimiento de las licencias de **Endpoint Security**. Se puede notificar a los clientes, los usuarios del VSA y los usuarios de máquinas una cantidad específica de días antes de que venzan las licencias de **Endpoint Security**. Las licencias de **Endpoint Security** se asignan a los ID de grupo en Sistema > **Administrador de licencias** *(http://help.kaseya.com/webhelp/ES/VSA/9010000/index.asp#2924.htm)*.

Nota: Consulte **Licencias de Endpoint Security** en el tema **Descripción general de seguridad** *(página 2)*.

La lista de los ID de máquina que puede seleccionar depende del filtro ID de máquina / ID de grupo y el ámbito que usa. Para que se muestren en esta página, los ID de máquina deben tener el software cliente de **Endpoint Security** instalado en la máquina administrada mediante la página **Instalación** *(página 17)* en Seguridad.

Acciones

- **Enviar una notificación cuando la licencia vaya a vencer en N días**: introduzca la cantidad de días antes de la fecha de vencimiento de una licencia de **Endpoint Security** para notificar a los clientes y usuarios.
- **Destinatarios de correo electrónico (separar varias direcciones por coma)**: especifique las direcciones de correo electrónico a las que se debe enviar mensajes de notificación. Las direcciones de correos electrónicos múltiples deben separarse por comas.
- **Aplicar**: haga clic para aplicar parámetros a los ID de máquina seleccionados. Confirma que los parámetros se han aplicado correctamente en la lista de ID de máquinas.
- **Borrar**: haga clic para quitar todos los ajustes de parámetros de los ID de máquina seleccionados.

Columnas de tabla

- **(Estado de registro)**: Estos íconos indican el estado de registro del agente de cada máquina administrada. Al desplazar el cursor sobre un ícono de registro, se muestra la ventana de Vista rápida 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
- **Seleccionar todo/Anular selección**: Haga clic en el enlace **Seleccionar Todo** para marcar todas las filas en la pagina. Haga clic en el enlace **Desmarcar Todo** para desmarcar todas las filas en la pagina.
- **Machine.Group ID**: Un nombre de ID de máquina, ID de grupo o ID de organización exclusivo para una máquina del VSA.
- **Días**: muestra la cantidad de días antes de la fecha de vencimiento de la licencia para enviar la notificación.
- **Lista de direcciones de correo electrónico**: indica las direcciones de correo electrónico a las que se envían las notificaciones.
- **Notificar**: si está seleccionada, se advierte a los destinatarios de correo electrónico que la licencia de seguridad del ID de máquina está por vencer. Si está en blanco, no se enviará la notificación.

Instalación: Pestaña de Seguridad

Seguridad > Instalación

En la página **Instalación**, se instala o se quita la protección de seguridad para los ID de máquina seleccionados.

- La lista de ID de máquina que se muestra depende del filtro ID de máquina/ID de grupo y de los grupos de máquinas que el usuario está autorizado a ver mediante el uso de Sistema > Seguridad de usuarios > Ámbitos.
- Se debe deshabilitar el control de acceso de usuarios (UAC) antes de instalar o actualizar clientes de extremo.
- Después de que se instala **Endpoint Security** 2.3 en el VSA, se descargan los instaladores de extremos de AVG.
  - Los nuevos instaladores de extremos de **Endpoint Security** 2.3 se basan en AVG 2012 SP1, pero **Endpoint Security** continúa siendo compatible con los extremos AVG 9 existentes.
  - Los instaladores de extremos se basan en el tipo de estación de trabajo, servidor y CPU: 32 bits o 64 bits. Se selecciona el instalador apropiado cuando se instala en un extremo.
  - El instalador de extremos de servidor contiene componentes de instalación de Exchange.
  - El tiempo de descarga de los instaladores de extremos de AVG puede variar, sobre la base de un paquete de entrega de 500 MB.
  - Es posible que se necesite un reinicio condicional del VSA.
- AVG 2012 no se registra en el Centro de seguridad de Windows.
- Las licencias de **Endpoint Security** se asignan a los ID de grupo en Sistema > **Administrador de licencias** *(http://help.kaseya.com/webhelp/ES/VSA/9010000/index.asp#2924.htm)*.

Reinicio de extremos durante instalaciones y actualizaciones

La instalación de AVG 2012 puede reiniciar el extremo después de la instalación. La actualización de AVG 2012 reinicia el extremo después de la desinstalación del software cliente de **Endpoint Security** anterior y después de la instalación de AVG 2012.

Nota: Se recomienda la instalación de AVG 2012 y la actualización a AVG 2012 fuera el horario laborable para evitar interrumpir al usuario. Existe una opción para preguntar al usuario final si desea proceder con la instalación o actualización antes de continuar con la instalación.

AVG 8 no es compatible

Advertencia: Los extremos de AVG 8 no son compatibles con Endpoint Security 2.3. Se recomienda ampliamente a los usuarios que actualicen los extremos a AVG 9 antes de actualizar a KES 2.3 o que desinstalen los extremos de AVG 8 por completo y los vuelvan a instalar en extremos de AVG 2012 después de la instalación de KES 2.3.

Instrucciones de opciones de instalación

No se recomienda la instalación de las siguientes opciones en los *servidores*.

- Explorador de Correo Electrónico

No se recomiendan las siguientes opciones en los *servidores que tienen Exchange instalado*.

- Escudo Web
- Enlazar Explorador
- Protección de identidad

Tanto para los *servidores* como para las *estaciones de trabajo*, el firewall de AVG no es compatible

con los extremos de AVG 2012, pero sí lo es con los extremos de AVG 9.

Acciones

Esta página ofrece las siguientes acciones:

- **Instalar**: permite instalar **Endpoint Security** en los ID de máquina seleccionados. Consulte **Instalación o actualización de extremos** *(página 20)*.

  Advertencia: Desinstale todos los software antivirus, spyware y malware en la máquina administrada antes de instalar el software cliente de **Endpoint Security**.

- **Actualizar**: permite actualizar clientes de extremo de AVG 9 a AVG 2012. En la columna **Estado de instalación**, se identifican los extremos que pueden recibir una actualización. Consulte **Instalación o actualización de extremos** *(página 20)*.
- **Conectar cliente**: instala *sólo el servicio de cliente de Endpoint Security* en el extremo. Esto le permite lo siguiente:
  - Verificar si existe un motor de AVG compatible en el extremo.
  - Actualizar o reinstalar sólo el servicio de cliente de **Endpoint Security**, sin afectar el componente de AVG. Esto se puede requerir si el servicio de cliente de **Endpoint Security** está desactualizado o se dañó.
- **Quitar**: permite quitar **Endpoint Security** en los ID de máquina seleccionados.
- **Cancelar operación pendiente**: cancela cualquiera de las primeras tres acciones, si aún no se completaron.
- **Editar preguntas al usuario** : edita la pregunta de advertencia mostrada a los usuarios, si es que se muestra la misma. También puede especificar la cantidad de minutos que el usuario tiene permitido posponer la instalación.
- **Opciones de instalación**: establece **opciones de instalación** *(página 21)* de *nivel de módulo* o predeterminadas para instalaciones o actualizaciones.
- **Reiniciar**: reinicia la computadora seleccionada. AVG publica en forma periódica una actualización que requiere reinicio. Se muestra `Reboot Required` en la columna **Versión**.
- **Recuento de licencias**: se muestra una ventana emergente con los siguientes recuentos de licencias:
  - Licencias compradas
  - Licencias completamente disponibles (compradas no asignadas, instaladas o vencidas)
  - Licencias asignadas (programadas para instalación, pero la instalación aún no está completa)
  - Licencias aplicadas (licencia activa aplicada a una máquina)
  - Licencias parcialmente disponibles (asignadas antes a una máquina, pero devueltas al grupo antes del vencimiento)
  - Licencias asignadas parcialmente (disponibles parcialmente y programadas para la instalación pero todavía sin instalación completa)
  - Licencias totales (licencias compradas menos las vencidas)
  - Licencias expiradas

  Nota: As of version 9.1 licensing sets the expiration date of the license to one year from the day it is purchased, irrespective of the day it is installed. The expiration dates of existing licenses are not affected by this change.

Columnas de tabla

- **(Estado de registro)**: Estos íconos indican el estado de registro del agente de cada máquina administrada. Al desplazar el cursor sobre un ícono de registro, se muestra la ventana de Vista rápida 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

- **(Casilla de verificación Seleccionar todo)**: haga clic en esta casilla de verificación para seleccionar todas las filas en el área de paginación. Si está tildada, haga clic en esta casilla para destildar todas las filas en el área de paginación.
- **Machine.Group ID**: Un nombre de ID de máquina, ID de grupo o ID de organización exclusivo para una máquina del VSA.
- **Estado de instalación**: los tipos de mensaje incluyen lo siguiente:
  - (Vacío): el software cliente de **Endpoint Security***no* está instalado en el ID de máquina. No hay requisitos previos que impidan instalar el cliente en esta máquina.
  - `Application Conflict` <product name>: ya hay un producto antivirus instalado en esta máquina y entra en conflicto con la instalación de **Endpoint Security**.
  - `Requires Agent Update`: el software de agente es anterior a 4.7.1. Use la página **Actualizar agente** *(http://help.kaseya.com/webhelp/ES/VSA/9010000/index.asp#549.htm)* en Agente para actualizar este agente.
  - `Install Pending` <date/time>: la instalación se programa para una fecha y una hora específicas. Las marcas de la fecha y hora de vencimiento se muestran en texto en rojo resaltado en amarillo.
  - `Waiting for Service`: el servicio que usa el agente para comunicarse con el motor de AVG inició la instalación. Este mensaje se muestra hasta que se completa la instalación.
  - : se completó la instalación. Puede mostrar las opciones de instalación aplicadas a un ID de máquina al hacer clic en este ícono.
  - `FAILED at <time/date and error message>`: muestra los detalles del error en la instalación, si están disponibles, que informa el software cliente de AVG.
  - `AVG Removed by User` : el usuario de la máquina eliminó el cliente de AVG manualmente.
- **Origen de instalación**: si se define un origen de archivo en Administración de parches > **Origen de archivo** *(http://help.kaseya.com/webhelp/ES/VSA/9010000/index.asp#366.htm)*, las instalaciones se originan en esta ubicación. Caso contrario, las instalaciones usan las fuentes desde Internet. Si la opción **Descargar de Internet si la máquina no puede conectarse al servidor de archivos** está seleccionada en Administración de parches>Origen de archivo:
  - Durante la instalación del extremo **Endpoint Security** v2.x, si el origen de los archivos está inactivo o las credenciales no son válidas, el instalador se descarga de Kaseya Server y se completa la instalación del extremo.
  - Durante la actualización manual de **Endpoint Security** v2.x, si el origen de los archivos está inactivo o las credenciales no son válidas, la actualización se descarga de Internet.

  En los dos casos anteriores, la página **Ver registros** *(página 13)* muestra un mensaje de error indicando por qué falló la fuente del archivo y que está intentando descargar desde Internet.
- **Fecha de instalación**: la fecha en que se instaló el software cliente de **Endpoint Security** en el ID de máquina.
- **Versión**: La versión de protección de seguridad que usa actualmente este ID de máquina. Por ejemplo: `8.5.322 270.12.6/2084`
  - `8.5.322`: la versión instalada del programa AVG.

- `270.12.6/2084`: la versión completa de la *base de datos* de virus. `270.12.6` representa la versión de *definición* y `2084` es la versión de *firma*. De muestra el texto en color rojo si la versión de la *firma* es anterior que las últimas 5 versiones de *firmas* disponibles o si la versión de la *definición* es anterior que las 2 últimas versiones de *definición* disponibles y el agente está activo.
- `[KES 2.1.0.87]`: la versión del software cliente de **Endpoint Security**.

Instalación o actualización de extremos

Seguridad > Instalación > Instalar o actualizar

Establezca las siguientes opciones después de hacer clic en los botones **Instalar** o **Actualizar**. La configuración predeterminada se establece con el botón **Opciones de instalación** *(página 21)*. Después de instalar el cliente de **Endpoint Security** en el ID de máquina, se pueden ver las opciones de instalación aplicadas a dicho ID de máquina al hacer clic en la marca de verificación verde en la columna **Estado de instalación**.

Selección de perfil

- **Seleccionar perfil**: selecciona el perfil para usar durante la instalación.

Opciones de instalador

- **Instalar/Actualizar desde KServer (reemplazar origen de archivo)**: si está seleccionada, las instalaciones se descargan de Kaseya Server. Si no está seleccionada, las instalaciones se descargan con el método especificado en Administración de parches > **Origen de archivo** *(http://help.kaseya.com/webhelp/ES/VSA/9010000/index.asp#366.htm)*.
- **Preguntar al usuario antes de instalar/Forzar instalación sin advertir al usuario**: la instalación requiere un reinicio de la máquina administrada. Si se selecciona **Preguntar al usuario antes de instalar**, el usuario tiene la opción de posponer la instalación durante un determinado número de minutos. De lo contrario **Forzar instalación sin advertir al usuario** provoca que el software sea instalado en el tiempo programado sin advertir al usuario.

> **Nota:** Haga clic en **Editar mensajes de usuario** para especificar la cantidad de minutos que el usuario tiene permitido posponer la instalación.

Programa

- **Inmediato**: haga clic en la casilla de verificación Inmediato para comenzar la instalación no bien se hace clic en Instalar.
- **Fecha/Hora**: introduzca el año, el mes, el día, la hora y los minutos para programar esta tarea.
- **Escalonar cada**: puede distribuir la carga en la red si escalona esta tarea. Si configura este parámetro en 5 minutos, la tarea en cada ID de máquina se escalona cada 5 minutos. Por ejemplo, máquina 1 ejecuta a las 10:00, máquina 2 ejecuta a las 10:05, máquina 3 ejecuta a las 10:10, ...
- **Omitir si la máquina está desconectada**: seleccione esta opción para que esta tarea se realice sólo a la hora programada. Si la máquina está fuera de línea, omitir y ejecutar el siguiente período y hora programados. Destildar para realizar esta tarea tan pronto como la máquina se conecte después de la hora programada.

Componentes

Componentes de estación de trabajo

- **Escaneo de vínculos** : bloquea sitios Web peligrosos y verifica vínculos devueltos por los motores de búsqueda más populares. No instala en exploradores que se ejecutan en SO de servidores de Windows.
  - **Búsqueda de seguridad activa** : escanea el vínculo mostrado en una página Web antes de que usted lo seleccione.
  - **Search-Shield** - identifica la clasificación de seguridad para un vínculo de búsqueda listado en las listas de búsqueda de Google, Yahoo y MSN.
- **Web-Shield** : escanea los archivos descargados y los archivos intercambiados usando la mensajería instantánea.
- **Escaneo de correos electrónicos** : si está tildado, la instalación detecta el cliente de correos electrónicos predeterminado en la máquina y automáticamente instala el complemento de escaneo de correos electrónicos respectivo.
- **Protección de ID** : si está tildado, se habilita la opción Protección de identidad de AVG. Previene el robo dirigido a las contraseñas, detalles de cuantas bancarias, números de tarjetas de crédito y otros valores digitales usando un "análisis de comportamiento" para indicar actividades sospechosas en la máquina.
- **Firewall (No administrado por Kaseya)** : si está tildado, se habilita la opción de firewall de AVG. Bloquea el acceso no autorizado y permite las comunicaciones autorizadas. *El cliente de* **Endpoint Security** *no se puede usar para mantener las listas negras y listas blancas que requiere esta opción.*

Componentes de servidor

- **Complemento del servidor SharePoint**: si está seleccionada, instala la protección de **Endpoint Security** para los documentos del servidor SharePoint.
- **Complemento del servidor Exchange**: si está seleccionada, instala la protección de correo electrónico de **Endpoint Security** en los servidores MS Exchange. Esta configuración se omite cuando se instala el cliente de **Endpoint Security** en una máquina que no tiene servidor MS Exchange.

Instalando

Las excepciones de licencias se indican en el área de mensajes del cuadro de diálogo.

Opciones de instalación

Seguridad > Instalación > Opciones de instalación

Algunas **opciones de instalación** funcionan como opciones predeterminadas que se pueden reemplazar cuando se **instala o actualiza un extremo** *(página 20)*.

Otras **opciones de instalación** funcionan como ajustes *de nivel de módulo* que se aplican generalmente a todas las instalaciones. Los ajustes de nivel de módulo no se pueden reemplazar para una instalación o actualización especifica, pero se aplican a cualquier instalación que se lleve a cabo de ahí en más.

Opciones de Instalación

- **Nombre de usuario** - *nivel de módulo*: si está seleccionada, introduzca un nombre relacionado con esta instalación de **Endpoint Security**.
- **Nombre de la compañía** - *nivel de módulo*: si está seleccionada, introduzca el nombre de la compañía relacionado con esta instalación de **Endpoint Security**.
- **Directorio de destino** - *nivel de módulo*: si está seleccionada, introduzca el directorio de destino. Si está en blanco, se utiliza el directorio de instalación predeterminado.
- **Seleccionar perfil**: selecciona el perfil para usar durante la instalación.

- **Terminar todas las aplicaciones en ejecución que impidan la instalación** - nivel de módulo: si está seleccionada, se detienen todas las aplicaciones en ejecución que puedan impedir una instalación correcta.
- **Deshabilitar Windows Defender** - *nivel de módulo*: la ejecución de Windows Defender degrada significativamente el rendimiento de **Endpoint Security**, y se debe deshabilitar de manera predeterminada con esta opción.
- **Habilitar análisis de directorio de usuario final** - *nivel de módulo*: agrega una opción que se activa al hacer clic con el botón secundario para Windows Explorer, que permite al usuario analizar un archivo individual o un directorio en forma inmediata.

Opciones de procedimiento de agente

- **Procedimiento de agente para ejecutar antes de la instalación** - *nivel de módulo*: selecciona un procedimiento de agente.
- **Procedimiento de agente para ejecutar después de la instalación** - *nivel de módulo*: selecciona un procedimiento de agente.

Componentes

Componentes de estación de trabajo

- **Escaneo de vínculos** : bloquea sitios Web peligrosos y verifica vínculos devueltos por los motores de búsqueda más populares. No instala en exploradores que se ejecutan en SO de servidores de Windows.
  - **Búsqueda de seguridad activa** : escanea el vínculo mostrado en una página Web antes de que usted lo seleccione.
  - **Search-Shield** - identifica la clasificación de seguridad para un vínculo de búsqueda listado en las listas de búsqueda de Google, Yahoo y MSN.
- **Web-Shield** : escanea los archivos descargados y los archivos intercambiados usando la mensajería instantánea.
- **Escaneo de correos electrónicos** : si está tildado, la instalación detecta el cliente de correos electrónicos predeterminado en la máquina y automáticamente instala el complemento de escaneo de correos electrónicos respectivo.
- **Protección de ID** : si está tildado, se habilita la opción Protección de identidad de AVG. Previene el robo dirigido a las contraseñas, detalles de cuantas bancarias, números de tarjetas de crédito y otros valores digitales usando un "análisis de comportamiento" para indicar actividades sospechosas en la máquina.

Componentes de servidor

- **Complemento del servidor SharePoint**: si está seleccionada, instala la protección de **Endpoint Security** para los documentos del servidor SharePoint.
- **Complemento del servidor Exchange**: si está seleccionada, instala la protección de correo electrónico de **Endpoint Security** en los servidores MS Exchange. Esta configuración se omite cuando se instala el cliente de **Endpoint Security** en una máquina que no tiene servidor MS Exchange.

Definir Perfil

Seguridad > Definir perfil

La página **Definir perfil** administra los perfiles de seguridad. Cada perfil de seguridad representa un grupo distinto de opciones de seguridad habilitadas o deshabilitadas. Los cambios en el perfil de seguridad afectan todas las ID de máquinas a las que se le asignó ese perfil de seguridad. Se asigna un perfil de seguridad a los ID de máquina en Seguridad > **Asignar perfil** *(página 30)*. En general, los

tipos de máquinas o redes diferentes requieren perfiles de seguridad distintos. Se suministra un perfil de muestra. No puede cambiar el perfil de muestra, pero puede guardarlo bajo un nuevo nombre y hacer cambios a la copia. Se puede usar el mismo perfil para administrar los extremos de AVG 9 y AVG 2012.

Esta página le suministra las siguientes acciones:

- **Guardar** : guarda los cambios a un perfil de seguridad.
- **Guardar como** : crea un nuevo perfil de seguridad guardándolo mediante el uso de un nombre diferente.
- **Eliminar** : elimina un perfil de seguridad existente.
- **Compartir** : comparte un perfil de seguridad privado. Los demás usuarios no pueden ver los perfiles de seguridad privados. Compartir un perfil de seguridad privado lo convierte en un perfil de seguridad público. Los derechos compartidos se asignan *por objeto*. Existen tres opciones de casilla de compartir. Las primeras dos casillas son *mutuamente exclusivas* y determinan qué derechos compartidos se asignan. Si ninguna de las dos primeras casillas está tildada, el objeto compartido sólo puede ser visto por los usuarios que tienen acceso compartido, pero el objeto no puede ser usado ni editado. Las casillas de la lista **Compartidos** y **No compartidos** y la tercera casilla determinan quién puede *ver* el objeto.
  - **Permitir modificar a otros administradores**: si está tildada, los derechos compartidos para el objeto incluyen poder usarlo, ver los detalles y editarlo.
  - **Otros administradores pueden usarlo pero no pueden verlo ni editarlo**: si está tildada, los derechos compartidos para el objeto sólo permiten usarlo.
  - **Hacer público (puede ser visto por todos los administradores)**: si está seleccionada, asegura que *todos* los usuarios del VSA actuales y futuros puedan *ver* el objeto. Si está en blanco, sólo los roles de usuarios y usuarios seleccionados pueden ver el objeto compartido. Si está en blanco y más tarde se agregan nuevos usuarios o roles de usuarios, debe regresar a este diálogo para permitirles ver el objeto específico.
- **Tomar posesión** : toma la **posesión** *(http://help.kaseya.com/webhelp/ES/VSA/9010000/index.asp#5537.htm)* de cualquier perfil de seguridad público.

Para definir o mantener un perfil de seguridad

1. Seleccione un perfil de seguridad de la lista desplegable **Seleccionar perfil**.
2. Fijar opciones en pestañas de perfiles de seguridad:
   - **General**
   - **Resident Shield**
   - **Explorador de Correo Electrónico**
   - **Exploración Completa**
   - **Exchange**
   - **Excluir Dirs**
   - **Excluir PUPs**
   - **Actualizaciones**
3. Haga clic en el botón **Guardar** o **Guardar como** para guardar el perfil de seguridad.

General

Contraseña de GUI de escritorio de AVG

- **Proteger GUI de escritorio de AVG con contraseña**: introducir una contraseña para forzar al usuario a introducir una contraseña antes de ocultar el escritorio de AVG, el ícono de bandeja y los accesos directos del menú Inicio. Si no está seleccionada, no se configura una contraseña si no introduce una.

Virus Vault

- **Limitar tamaño de bóveda** : si está tildado, limita el tamaño de la bóveda como se especifica usando las siguientes opciones:
  - **Tamaño máximo de la bóveda: <N>% del disco local**: introduzca el porcentaje máximo del espacio en disco para asignar al almacenamiento de las amenazas en cuarentena.
  - **Espacio disponible mínimo para retener en disco local** : ingrese la cantidad mínima de megabytes para signar en el disco con el propósito de almacenar las amenazas en cuarentena.
- **Eliminación de archivo automática** : si está tildado, elimina archivos automáticamente según lo especificado por las opciones siguientes:
  - **Eliminar archivos anteriores a <N> días**: introduzca la cantidad de días para almacenar las amenazas en cuarentena antes de que se eliminen automáticamente.
  - **Cantidad máxima de archivos para almacenar** : ingrese la cantidad máxima de amenazas en cuarentena para almacenar.

Notificaciones de la Bandeja del Sistema

- **Mostrar las notificaciones de la bandeja del sistema** : si está tildado, se pueden habilitar opcionalmente las siguientes notificaciones de la bandeja del sistema. Se muestran todos los mensajes de notificación en la máquina administrada que se encuentra al lado de la bandeja del sistema.
- **Mostrar notificaciones de la bandeja acerca de actualización**: si está seleccionada, se muestra un mensaje de notificación que indica que el software **Endpoint Security** se está actualizando.
- **Mostrar notificaciones de la bandeja acerca de escaneos** : si está tildado, muestra un mensaje de notificación indicando que se está escaneando la máquina.
- **Mostrar notificaciones de bandeja relacionadas con Protección residente (acción automática)** : si está tildado, muestra un mensaje de notificación que indica que la Protección residente ha accionado contra una amenaza.
- **Mostrar notificación de cambio de estado de los componentes**: si está seleccionada, se muestra un mensaje de notificación que indica que se modificó el estado de uno de los componentes de **Endpoint Security**.
- **Mostrar notificaciones relacionadas con el analizador de correo electrónico**: si está seleccionada, se muestra un mensaje de notificación que indica que el analizador de correo electrónico tomó medidas contra una amenaza de correo electrónico.

Menú del Icono de Agente

- **Mostrar la opción para Habilitar/Deshabilitar la Protección residente en el Menú del ícono del agente** : si está tildado:
  - las opciones **Habilitar seguridad** y **Cancelar escaneo** se muestran en el menú de tareas del agente de la máquina administrada.
  - El usuario puede hacer clic en la opción **Habilitar seguridad** del menú del agente para conectar o desconectar la protección.
  - El usuario puede hacer clic en la opción **Cancelar escaneo** en el menú del agente para cancelar un escaneo de protección de seguridad en progreso.

> **Nota:** El usuario también puede habilitar o deshabilitar la protección de seguridad en forma remota en Seguridad > **Estado de seguridad** *(página 5)*.

Resident Shield

La Protección residente es una característica residente en la memoria.

- **Habilitar Protección residente** : si está tildado, se escanean los siguientes tipos de archivos a medida que se copian, abren o guardan. Si está en blanco, no se evalúan otras opciones de la **Protección residente** .

> **Nota:** También puede **habilitar o deshabilitar Protección residente por procedimiento de agente** *(página 7)*.

Tipos de archivos

- **Escanear todos los archivos** : si está seleccionado, se escanean todos los archivos de la máquina administrada.
- **Escanear archivos que pueden infectarse y tipos de documentos seleccionados** : si está seleccionado. especifica las extensiones de los archivos *adicionales* de los programas y documentos para incluir o excluir usando las siguientes opciones:
  - **Excluir del escaneo archivos con las siguientes extensiones** :especifica las extensiones de archivos de programas y documentos para excluir del escaneo. Las extensiones excluidas tienen precedencia sobre las extensiones incluidas. Ingrese cada extensión separada por el carácter punto y coma (;).
  - **Siempre escanear archivos con las siguientes extensiones** :especifica las extensiones de archivos de programas y documentos para incluir en el escaneo. Ingrese cada extensión separada por el carácter punto y coma (;). La Protección residente escanea las siguientes extensiones de archivos sin que usted las especifique: 386; ASP; BAT; BIN; BMP; BOO; CHM; CLA; CLASS; CMD; CNM; COM; CPL; DEV; DLL; DO*; DRV; EML; EXE; GIF; HLP; HT*; INI; JPEG*; JPG; JS*; LNK; MD*; MSG; NWS; OCX; OV*; PCX; PGM; PHP*; PIF; PL*; PNG; POT; PP*; SCR; SHS; SMM; SYS; TIF; VBE; VBS; VBX; VXD; WMF; XL*; XML; ZL*;
  - **Escanear archivos sin una extensión** : si está tildado, el escaneo incluye los archivos sin extensión.

Opciones Adicionales

- **Escanear para cookies de rastreo** : si está tildado, el escaneo incluye las cookies de rastreo del explorador de Internet. Las cookies de rastreo encontradas se eliminan inmediatamente y no se trasladan a la bóveda de virus.
- **Escanear amenazas de spyware y posibles programas no deseados** : si está tildado, el escaneo detecta las aplicaciones ejecutables o bibliotecas DDL que pudieran ser potenciales programas no deseados. Algunos programas, en particular los gratuitos, incluyen adware, y **Endpoint Security** los puede detectar e informar como **posibles programas no deseados**.
- **Escanear archivos al cerrarse** : si está tildado, se escanean los archivos cuando se cierran.
- **Escanear el sector de inicio de los medios removibles** : si está tildado, el escaneo incluye el sector de inicio de los medios removibles.
- **Usar heurísticos** : si está tildado, el escaneo incluye el análisis heurístico. El análisis heurístico realiza una emulación dinámica de las instrucciones del objeto escaneado dentro de un entorno informático virtual.

Explorador de Correo Electrónico

- **Habilitar escaneo de correo electrónico** : si está tildado, se escanean los correos electrónicos entrantes y salientes y los adjuntos en busca de virus. Si está en blanco, no se evalúan otras opciones de la **Protección de correos electrónicos** .

> **Nota:** No se recomienda el **Analizador de correo electrónico** para los *servidores*. Consulte la pestaña **Exchange** a continuación.

Exploración de Correo Electrónico

- **Verificar correo electrónico entrante** : si está tildado, se escanea el correo electrónico entrante.

Certificación: Algunos clientes de correos electrónicos aceptan el agregado de un texto en los mensajes de correos electrónicos que certifican que se han escaneado los mismos en busca de virus.

  - **No certificar correo electrónico** : si está seleccionado, no se certifica el correo electrónico entrante.
  - **Certificar todos los correos electrónicos** : si está seleccionado, se certifican todos los correos electrónicos entrantes.
  - **Solo certificar correo electrónico son adjuntos** : si está seleccionado, solo se certifican los correos electrónicos entrantes con adjuntos.
  - **Certificación de correos electrónicos entrantes** : texto de certificación agregado al correo electrónico entrante.
- **Verificar correo electrónico saliente** : si está tildado, se escanea el correo electrónico saliente.
  - **No certificar correo electrónico** : si está seleccionado, no se certifica el correo electrónico saliente.
  - **Certificar todos los correos electrónicos** : si está seleccionado, se certifican todos los correos electrónicos salientes.
  - **Solo certificar correo electrónico son adjuntos** : si está seleccionado, solo se certifican los correos electrónicos salientes con adjuntos.
  - **Certificación de correos electrónicos salientes** : texto de certificación agregado al correo electrónico saliente.
- **Modificar asunto para mensajes marcados como virus** : agrega un texto prefijo al asunto del mensaje que contiene el virus.

Propiedades de la Exploración

- **Usar heurísticos** : se aplica al mensaje del correo electrónico. Si está tildado, el escaneo incluye el análisis heurístico. El análisis heurístico realiza una emulación dinámica de las instrucciones del objeto escaneado dentro de un entorno informático virtual.
- **Escanear amenazas de spyware y posibles programas no deseados** : si está tildado, el escaneo de correos electrónicos incluye escanear en busca de spyware, adware y posibles programas no deseados.
- **Analizar archivos internos** (RAR, RAR 3.0, ZIP, ARJ, CAB): si está seleccionada, se analizan los archivos de correo electrónico.

Informes de Adjuntos de Correos Electrónicos (como una amenaza)

- **Informar archivos protegidos con contraseña** : si está tildado, informa como amenazas a los adjuntos de los archivos protegidos con contraseñas (zip, rar, etc.) en los correos electrónicos.
- **Informar documentos protegidos con contraseña** : si está tildado, informa como amenazas a los adjuntos de los documentos protegidos con contraseñas en los correos electrónicos.
- **Informar archivos que contienen macro** : si está tildado, informa como amenazas a los archivos que contienen macros adjuntos a los correos electrónicos.
- **Informa las extensiones ocultas** : si está tildado, informa los archivos que usan extensiones ocultas. Algunos virus se ocultan a sí mismos duplicando la extensión del archivo. Por ejemplo, el virus `VBS/Iloveyou` adjunta un archivo, `ILOVEYOU.TXT.VBS`, al correo electrónico. La configuración predeterminada de Windows permite ocultar extensiones conocidas, de manera que el archivo se vea como `ILOVEYOU.TXT`. Cuando lo abre, no se abre un archivo de texto `.TXT`, sino que se ejecuta un archivo de procedimiento `.VBS`.
- **Más adjuntos informados para la bóveda de virus (solo correos electrónicos entrantes)** : si está tildado, los adjuntos de los correos electrónicos informados se mueven a la bóveda de virus. Se muestran en la pestaña **Bóveda de virus** de la página **Ver amenazas** *(página 5)* en vez de en la pestaña **Amenazas actuales**.

Exploración Completa

Explorar Configuraciones

- **Escanear amenazas de spyware y posibles programas no deseados** : si está tildado, el escaneo detecta las aplicaciones ejecutables o bibliotecas DDL que pudieran ser potenciales programas no deseados. Algunos programas, en particular los gratuitos, incluyen adware, y **Endpoint Security** los puede detectar e informar como **posibles programas no deseados**.
- **Escanear para cookies de rastreo** : si está tildado, el escaneo incluye las cookies de rastreo del explorador de Internet. Las cookies de rastreo encontradas se eliminan inmediatamente y no se trasladan a la bóveda de virus.
- **Escanear dentro de archivos** : si está tildado, el escaneo incluye archivos como ZIP y RAR.
- **Usar heurísticos** : si está tildado, el escaneo incluye el análisis heurístico. El análisis heurístico realiza una emulación dinámica de las instrucciones del objeto escaneado dentro de un entorno informático virtual.
- **Escanear entorno del sistema** : si está tildado, se escanean las áreas del sistema antes de iniciar el escaneo completo.
- **Escanear solo archivos que pueden infectarse** : si está tildado, se escanean los archivos "que pueden infectarse" en base a sus contenidos independientemente de las extensiones del archivo. Por ejemplo, se puede renombrar un archivo EXE pero seguir infectado. Los siguientes tipos de archivos se consideran archivos 'que pueden infectarse':
  - **Tipo EXE** : COM; DRV; EXE; OV?; PGM; SYS; BIN; CMD; DEV; 386; SMM; VXD; DLL; OCX; BOO; SCR; ESL; CLA; CLASS; BAT; VBS; VBE; WSH; HTA; HTM; HTML; ?HTML; CHM; INI; HTT; INF; JS; JSE; HLP; SHS; PRC; PDB; PIF; PHP; ZL?; ASP; LNK; EML; NWS; CPL; WMF
  - **Tipo DOC** : DO?; XL?; VBX; RTF; PP?; POT; MDA; MDB; XML; DOC?; DOT?; XLS?; XLT?; XLAM; PPT?; POT?; PPS?; SLD?; PPAM; THMX

Rendimiento

- **Seleccionar prioridad del sistema para escaneo** : define la rapidez en que se ejecuta el escaneo y cuántos recursos del sistema utiliza. Puede fijar el escaneo para que se ejecute lo más rápido posible mientras se alenta considerablemente la computadora, o puede elegir que el escaneo se ejecute usando la menos cantidad de recursos posible mientras prolonga el tiempo de ejecución del escaneo.

Exchange

- **Habilitar AVG para servidor Exchange** : habilite o deshabilite el escaneo de correo electrónico para los servidores MS Exchange asignados.

> **Nota:** Si instala la protección de correo electrónico en uno o más servidores MS Exchange, cree un perfil único para los servidores MS Exchange y sólo aplique este perfil a estos servidores. Las opciones de configuración de la pestaña Exchange en **Definir perfil** sólo se deben habilitar y aplicar a los servidores MS Exchange.

Certificación de correo

- **Habilitar**: si está seleccionada, agrega una nota de certificación a los correos electrónicos analizados en los servidores MS Exchange. Personalice la nota de certificación en el campo de texto.

Rendimiento

- **Ejecutar escaneos en el fondo** : habilite o deshabilite escaneos en el fondo. Los escaneos en el fondo son unas de las características de la interfaz de la aplicación VSAPI 2.0/2.5. Proporciona

escaneos subprocesados de las bases de datos de mensajería de Exchange. Siempre que se encuentre en las carpetas del buzón del usuario un elemento que no se ha escaneado con anterioridad, se envía a AVG para que lo escanee el servidor Exchange 2000/2003. El escaneo y búsqueda de los objetos no examinados se ejecutan en paralelo. Se utiliza un subproceso de baja prioridad para cada base de datos, lo cual garantiza que las otras tareas siempre tengan preferencia, por ejemplo el almacenamiento de los mensajes de correo electrónico en la base de datos de Microsoft Exchange.

- **Escanear proactivamente** : habilite o deshabilite el escaneo proactivo de VSAPI 2.0/2.5. El escaneo proactivo involucra la administración de prioridad dinámica de los elementos en la cola del escaneo. Los elementos de más baja prioridad no se escanean al menos que se hayan escaneado todos los de prioridad más alta. La prioridad de un elemento aumenta si el cliente intenta usarlo, de manera que la precedencia de un elemento cambia dinámicamente de acuerdo a la actividad del usuario.
- **Escanear archivos RTF** : especifique si los archivos RTF deben o no escanearse.
- **Subprocesos escaneados** : el proceso de escaneo se subprocesa predeterminadamente para aumentar el rendimiento general del escaneo por un cierto nivel de paralelismo. La cantidad predeterminada de subprocesos se computa como 2 veces la 'cantidad_ de_procesadores' + 1.
- **Escanear tiempo de espera excedido** : el intervalo continuo máximo, en segundos, para que un subproceso acceda al mensaje que se está escaneando.

Excluir Dirs

Excluir directorios

Advertencia: No excluya directorios, a menos que se sepa que el contenido de estos esté libre de amenazas.

- **Agregar nuevos registros** : agrega directorios excluidos del escaneo. Algunos directorios pueden estar libres de amenazas pero tienen archivos que se interpretan erróneamente como malware.
  - **Nombre de archivo**: introduzca el nombre del directorio.

Exclusión de archivos de Protección residente

Excluir archivos de Protección residente (disponible sólo en Protección residente de AVG2012, se omite en AVG9)

Advertencia: No excluya archivos, a menos que se sepa que el contenido de estos está libre de amenazas.

Use esta pestaña para excluir archivos específicos *manualmente*. Esta lista de exclusión sólo está activa con el análisis activo de la Protección residente.

- **Agregar nuevo registro** : agrega archivos PUP para excluirlos del escaneo. Algunos archivos pueden estar libres de amenazas pero ser erróneamente interpretados como programas potencialmente no deseados (PUP).
  - **Nombre de archivo** : ingrese el nombre del archivo.

Excluir PUPs

Excluir Programas Potencialmente No Deseados

Advertencia: No excluya archivos, a menos que se sepa que el contenido de estos está libre de amenazas.

Use esta pestaña para excluir programas potencialmente no deseados, o PUP *manualmente*. Las amenazas que no son PUP no se pueden agregar a la lista de exclusión de PUP. En la página Ver amenazas, se proporciona un método más rápido para identificar y excluir los PUP.

- **Agregar nuevo registro** : agrega archivos PUP para excluirlos del escaneo. Algunos archivos pueden estar libres de amenazas pero ser erróneamente interpretados como programas potencialmente no deseados (PUP).
  - **Nombre de archivo** : ingrese el nombre del archivo.
  - **Suma de comprobación** : ingrese el valor de la suma de comprobación del archivo. Para determinar el valor de la suma de comprobación, abra **AVG UI** en la máquina que contiene el archivo. Seleccione **Herramientas > Configuración avanzada**. Seleccione la hoja de propiedades de **Excepciones de PUP**. Haga clic en el botón **Agregar excepción**. Seleccione el archivo explorando el directorio local de la máquina. Se mostrará el valor de la suma de comprobación correspondiente. Copie y pegue el valor de la suma de comprobación de **AVG UI** en el cuadro de diálogo **Agregar nuevo registro** de la pestaña **Excluir PUP** en Seguridad > **Definir perfil**.
  - **Tamaño del archivo** : ingrese el tamaño del archivo en bytes. Para determinar el tamaño del archivo, haga clic con el botón derecho del mouse en el archivo en Windows Explorer y compruebe el valor del **Tamaño** en bytes.

Actualizaciones

Use esta pestaña para configurar la manera en que se descargan las actualizaciones de AVG.

Configuración de proxy

Habilita/Deshabilita usando un servidor proxy para descargar las actualizaciones de AVG.

- **No usar proxy** : deshabilita las configuraciones del proxy.
- **Usar proxy** : habilita las configuraciones del proxy.
- **Intentar conexión usando proxy, si falla conectar en forma directa** : habilita las configuraciones del proxy. Si el proxy falla, se conecta en forma directa.

Los ajustes **Manual** y **Automático** se aplican si se selecciona una de las opciones de proxy indicadas más arriba.

- **Manual** : fija las configuraciones del proxy en forma manual.
  - **Servidor** : ingrese un nombre de servidor proxy o una dirección IP válidos.
  - **Puerto** : ingrese un número de puerto.
  - **Usar autenticación de PROXY** : si está tildado, se requiere la autenticación del proxy.
    - ✓ **Nombre de usuario** : si **Usar autenticación de PROXY** está tildado, ingrese un nombre de usuario válido.
    - ✓ **Contraseña** : si **Usar autenticación de PROXY** está tildado, ingrese una contraseña válida.
- **Automático** : fija las configuraciones del proxy en forma automática.
  - **Desde explorador** : seleccione un explorador predeterminado desde el menú desplegable para fijar las configuraciones del proxy.
  - **Desde script** : ingrese la ruta completa de un script que especifique la dirección del servidor proxy.
  - **Detección automática** : intenta obtener las configuraciones directamente desde el servidor proxy.

Actualizar URL

AVG proporciona una URL predeterminada para descargar actualizaciones. Puede preferentemente descargar actualizaciones desde una URL personalizada.

- **Usar URL de actualización personalizada** : seleccione esta opción para descargar preferentemente actualizaciones desde una URL personalizada.
  - **Nombre** : ingrese el nombre de la URL de actualización personalizada.
  - **URL** : ingrese la URL.

Asignar Perfil

Seguridad > Asignar perfil

En la página **Asignar perfil**, se asignan perfiles de seguridad a los ID de máquina con licencia para usar **Endpoint Security**. Los perfiles de seguridad se definen en Seguridad > **Definir perfil** *(página 22)*.

La lista de los ID de máquina que puede seleccionar depende del filtro ID de máquina / ID de grupo y el ámbito que usa. Para que se muestren en esta página, los ID de máquina deben tener el software cliente de **Endpoint Security** instalado en la máquina administrada mediante la página **Instalación** *(página 17)* en Seguridad.

Acciones

- **Aplicar configuración**: haga clic en **Aplicar configuración** para aplicar el perfil de seguridad que se muestra en el cuadro desplegable **Seleccionar perfil** para los ID de máquina seleccionados.
- **Seleccionar perfil**: se selecciona un perfil de seguridad para aplicar a los ID de máquina seleccionados.
- **Sólo mostrar máquinas con el perfil seleccionado**: si está seleccionada, se filtra el área de paginación por perfil de seguridad seleccionado.

Columnas de tabla

- **Estado de registro**: Estos íconos indican el estado de registro del agente de cada máquina administrada. Al desplazar el cursor sobre un ícono de registro, se muestra la ventana de Vista rápida 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
- **(Casilla de verificación Seleccionar todo)**: haga clic en esta casilla de verificación para seleccionar todas las filas en el área de paginación. Si está tildada, haga clic en esta casilla para destildar todas las filas en el área de paginación.
- **Machine.Group ID**: Un nombre de ID de máquina, ID de grupo o ID de organización exclusivo para una máquina del VSA.
- **Nombre de perfil**: muestra el perfil de seguridad asignado a un ID de máquina. Muestra el estado del ID de máquina si existe un problema.

Configuraciones de registro: Pestaña de Seguridad

Seguridad > Configuración del registro

En la página **Configuración del registro**, se especifica la cantidad de días que se mantienen los datos de registro de protección de seguridad para los ID de máquina con licencia para usar **Endpoint Security**. Ciertas máquinas, como los servidores Web, pueden garantizar mantener un historial más largo de los ataques de virus que otros tipos de máquinas.

La lista de los ID de máquina que puede seleccionar depende del filtro ID de máquina / ID de grupo y el ámbito que usa. Para que se muestren en esta página, los ID de máquina deben tener el software cliente de **Endpoint Security** instalado en la máquina administrada mediante la página **Instalación** *(página 17)* en Seguridad.

Acciones

- **Aplicar configuración**: haga clic en **Aplicar configuración** para aplicar la cantidad de días especificados en el campo **Mantener las entradas del registro por <N> días** para los ID de máquina seleccionados.
- **Mantener las entradas del registro por <N> días**: introduzca la cantidad de días que se mantienen los datos de registro de protección de seguridad.

Columnas de tabla

- **Estado de registro**: Estos íconos indican el estado de registro del agente de cada máquina administrada. Al desplazar el cursor sobre un ícono de registro, se muestra la ventana de Vista rápida 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
- **(Casilla de verificación Seleccionar todo)**: haga clic en esta casilla de verificación para seleccionar todas las filas en el área de paginación. Si está tildada, haga clic en esta casilla para destildar todas las filas en el área de paginación.
- **Machine.Group ID**: Un nombre de ID de máquina, ID de grupo o ID de organización exclusivo para una máquina del VSA.
- **Días de registro antes del vencimiento**: muestra la cantidad de días que se mantienen los datos de registro de protección de seguridad para un ID de máquina.

Estado de Exchange

Seguridad > Estado de Exchange

En la página **Estado de Exchange**, se muestra el estado de la protección de correo electrónico en los servidores MS Exchange que tienen instalado **Endpoint Security**. Durante la instalación de **Endpoint Security** en una máquina, si se detecta MS Exchange, se instala automáticamente el complemento para la protección de correo electrónico de MS Exchange. Los servidores con Exchange se pueden excluir del uso de la protección de buzón de Exchange en la página **Definir perfil** *(página 22)*.

Nota: Todo malware que detecte la protección de correo electrónico de servidores MS Exchange se elimina inmediatamente del servidor MS Exchange y se muestra *sólo* en la pestaña **Bóveda de virus** en la página **Ver amenazas** *(página 11)*.

La lista de los ID de máquina que puede seleccionar depende del filtro ID de máquina / ID de grupo y el ámbito que usa. Además, la ID de máquina debe tener instalado el servidor MS Exchange en la máquina.

Buzones protegidos / Licencias de buzones

Muestra la cantidad de buzones protegidos del servidor Exchange y la cantidad de licencias de buzones usadas y disponibles. Las licencias se implementan, y se necesita una licencia para cada buzón que se usa.

> **Nota:** Consulte **Licencias de Endpoint Security** en el tema **Descripción general de seguridad** *(página 2)*.

Acciones

- **Quitar**: desinstala la instalación de Exchange.
- **Cancelar acción pendiente**: cancela la remoción de la protección de Exchange.

Columnas de tabla

- **Estado de registro**: Estos íconos indican el estado de registro del agente de cada máquina administrada. Al desplazar el cursor sobre un ícono de registro, se muestra la ventana de Vista rápida 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
- **(Casilla de verificación Seleccionar todo)**: haga clic en esta casilla de verificación para seleccionar todas las filas en el área de paginación. Si está tildada, haga clic en esta casilla para destildar todas las filas en el área de paginación.
- **Machine.Group ID**: Un nombre de ID de máquina, ID de grupo o ID de organización exclusivo para una máquina del VSA.
- **Estado de instalación**: si está seleccionada, el software cliente de **Endpoint Security** se instala en el ID de máquina. Si el software de agente es anterior a la versión 4.7.1, se muestra el mensaje `Requires Agent Update`. Si no está seleccionada, el software cliente de **Endpoint Security** *no* está instalado en el ID de máquina.
- **Origen de instalación**: si se define un origen de archivo en Administración de parches > **Origen de archivo** *(http://help.kaseya.com/webhelp/ES/VSA/9010000/index.asp#366.htm)*, las instalaciones se originan en esta ubicación. Caso contrario, las instalaciones usan las fuentes desde Internet. Si la opción **Descargar de Internet si la máquina no puede conectarse al servidor de archivos** está seleccionada en Administración de parches>Origen de archivo:
  - Durante la instalación del extremo **Endpoint Security** v2.x, si el origen de los archivos está inactivo o las credenciales no son válidas, el instalador se descarga de Kaseya Server y se completa la instalación del extremo.
  - Durante la actualización manual de **Endpoint Security** v2.x, si el origen de los archivos está inactivo o las credenciales no son válidas, la actualización se descarga de Internet.

  En los dos casos anteriores, la página **Ver registros** *(página 13)* muestra un mensaje de error indicando por qué falló la fuente del archivo y que está intentando descargar desde Internet.
- **Buzones**: la cantidad de cuentas de correo electrónico en el servidor MS Exchange.
- **Fecha de instalación**: la fecha en que se instaló la protección de correo electrónico de servidores MS Exchange en el ID de máquina.

Definir Conjuntos de Alarma

Seguridad > Definir conjuntos de alarmas

En la página **Definir conjuntos de alarmas**, se definen los conjuntos de las condiciones de alarma que se usan para desencadenar las alarmas en la página **Aplicar conjuntos de alarmas** *(página 34)*.

Acciones

- **Guardar** : guarde el grupo de la alarma.
- **Guardar como**: guarde un grupo de alarma en un nombre nuevo.
- **Eliminar** : elimine un grupo de alarma.
- **Compartir** : muestra si usted posee un grupo de alarma seleccionado. Comparta este grupo de alarma con los usuarios, roles de usuarios o para hacerlo público para todos los usuarios. Los derechos compartidos se asignan *por objeto*. Existen tres opciones de casilla de compartir. Las primeras dos casillas son *mutuamente exclusivas* y determinan qué derechos compartidos se asignan. Si ninguna de las dos primeras casillas está tildada, el objeto compartido sólo puede ser visto por los usuarios que tienen acceso compartido, pero el objeto no puede ser usado ni editado. Las casillas de la lista **Compartidos** y **No compartidos** y la tercera casilla determinan quién puede *ver* el objeto.
  - **Permitir modificar a otros administradores**: si está tildada, los derechos compartidos para el objeto incluyen poder usarlo, ver los detalles y editarlo.
  - **Otros administradores pueden usarlo pero no pueden verlo ni editarlo**: si está tildada, los derechos compartidos para el objeto sólo permiten usarlo.
  - **Hacer público (puede ser visto por todos los administradores)**: si está seleccionada, asegura que *todos* los usuarios del VSA actuales y futuros puedan *ver* el objeto. Si está en blanco, sólo los roles de usuarios y usuarios seleccionados pueden ver el objeto compartido. Si está en blanco y más tarde se agregan nuevos usuarios o roles de usuarios, debe regresar a este diálogo para permitirles ver el objeto específico.
- **Tomar posesión** : muestra si usted no *posee* un grupo de alarma público seleccionado. Haga clic para tomar **posesión** *(http://help.kaseya.com/webhelp/ES/VSA/9010000/index.asp#5537.htm)* y hacer cambios en el grupo de alarma.

Para crear un nuevo grupo de alarma

1. Seleccione `<No Alarm Sets Saved>` en la lista desplegable **Seleccionar perfil**. Alternativamente puede seleccionar un grupo de alarma existente y hacer clic en **Guardar como**.
2. Active una o más casillas de verificación de condiciones de alerta.
3. Use la opción **Omitir alarmas adicionales por <N> <períodos>** para especificar la cantidad de minutos para omitir el mismo conjunto de condiciones de alerta. Establezca 0 para desencadenar una alarma cada vez que se produzca una condición de alerta.
4. Haga clic en **Guardar** para guardar el grupo de alarma.

Para eliminar un grupo de alarma

1. Seleccione un grupo de alarma de la lista desplegable **Seleccionar perfil**.
2. Haga clic en **Eliminar** para eliminar el grupo de alarma.

Omitir alarmas adicionales por <N> <períodos>

Especifique la cantidad de períodos que desea se ignore el mismo tipo de alarma luego de activar la primera alarma.

Condiciones de alarma

Active cualquiera de los siguientes tipos de condiciones de alarma para incluirlo en un conjunto de alarmas de **Endpoint Security**.

- **Amenaza detectada y no corregida** : se ha agregado una amenaza a la pestaña **Amenaza actual** de la página **Ver amenazas** *(página 11)* que se haya podido corregir en forma automática.
- **Protección deshabilitado** : se ha deshabilitado la protección de seguridad.
- **Definición actualizada**: se actualizó la protección de seguridad con la última versión de **Endpoint Security**.
- **Escaneo programado completado** : se ha completado el escaneo de protección de seguridad.
- **Reiniciar requerido** : se requiere un reinicio.
- **Protección habilitado** : se ha habilitado la protección de seguridad.
- **Error de servicio**: se detuvo el servicio de **Endpoint Security**.
- **Definición no actualizada en <N> días**: la protección de seguridad no se actualizó para la cantidad de días especificada.
- **Escaneo programado no completado** : no se completó el escaneo de protección de seguridad programado.
- **AVG removido por el usuario** : el usuario de la máquina ha desinstalado el cliente AVG de la máquina administrada.

Aplicar Conjuntos de Alarma

Seguridad > Aplicar conjuntos de alarmas

En la página **Aplicar conjuntos de alarmas**, se crean alertas en respuesta a las condiciones de alerta de protección de seguridad definidas en **Definir conjuntos de alarmas** *(página 33)*. Los conjuntos de alarmas se aplican a los ID de máquina seleccionados con licencia para usar **Endpoint Security**.

La lista de los ID de máquina que puede seleccionar depende del filtro ID de máquina / ID de grupo y el ámbito que usa. Para que se muestren en esta página, los ID de máquina deben tener el software cliente de **Endpoint Security** instalado en la máquina administrada mediante la página **Instalación** *(página 17)* en Seguridad.

La página le suministra cuatro acciones:

- **Aplicar** : aplique un grupo de alarma seleccionado a ID de máquinas seleccionadas.
- **Remover** : remueva un grupo de alarma seleccionado de las ID de máquinas seleccionadas.
- **Remover todo** : remueva todos los grupos de alarmas asignados a las ID de máquinas seleccionadas.

Para Crear una Alerta

1. Active una de estas casillas de verificación para llevar a cabo las acciones correspondientes cuando se encuentra una condición de alerta:
   - Crear **A**larma
   - Crear **T**icket
   - Ejecutar **s**cript
   - Destinatarios de Correo **E**lectrónico
2. Configure los parámetros adicionales de correo electrónico .
3. Seleccione un grupo de alarma.
4. Tilde las ID de máquinas a las cuales aplicar el grupo de alerta.
5. Haga clic en **Aplicar** ara asignar el grupo de alarma a las ID de máquinas seleccionadas.

Para Cancelar una Alerta

1. Seleccionar las casillas de verificación de las ID de máquinas.
2. Haga clic en **Remover** para eliminar los grupos de alarmas asignados desde las ID de máquinas seleccionadas.

Opciones

- **Crear alarma**: si está seleccionada y se encuentra una condición de alerta, se crea una alarma. Las alarmas se muestran en Monitor > Lista de tablero, en Monitor > Resumen de alarmas y en Info Center > Elaboración de informes > Informes > Registros > Registro de alarmas.
- **Crear ticket**: si está seleccionada y se encuentra una condición de alerta, se crea un ticket.
- **Ejecutar script después de alerta**: Si está seleccionada y se encuentra una condición de alerta, se ejecuta un procedimiento de agente. Debe hacer clic en el vínculo **seleccionar procedimiento de agente** para elegir un procedimiento de agente para ejecutar. Opcionalmente, puede instruir al procedimiento de agente para ejecutarse en un rango especificado de ID de máquinas haciendo clic en el vínculo **de la ID de esta máquina**. Estas ID de máquinas especificadas no tienen que coincidir con el ID de máquina que encontró la condición de alerta.
- **Destinatarios de correo electrónico**: si está seleccionada y se encuentra una condición de alerta, se envían correos electrónicos a las direcciones especificadas. El correo electrónico se envía directamente desde el servidor VSA a la dirección especificada en la alerta. Configure la **dirección "De"** en Sistema > Correo electrónico saliente.
- **Seleccionar un conjunto de alarma**: selecciona un conjunto de alarma para aplicar a los ID de máquina seleccionados.

Columnas de tabla

- **(Estado de registro)**: Estos íconos indican el estado de registro del agente de cada máquina administrada. Al desplazar el cursor sobre un ícono de registro, se muestra la ventana de Vista rápida 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
- **(Casilla de verificación Seleccionar todo)**: haga clic en esta casilla de verificación para seleccionar todas las filas en el área de paginación. Si está tildada, haga clic en esta casilla para destildar todas las filas en el área de paginación.
- **Machine.Group ID**: Un nombre de ID de máquina, ID de grupo o ID de organización exclusivo para una máquina del VSA.
- **Conjunto de alarma**: indica los conjuntos de alarma asignados a cada ID de máquina.
- **ATSE**: el código de respuesta ATSE asignado a los ID de máquina o los dispositivos SNMP, según se detalla a continuación.
  - A = Crear **A**larma
  - T = Crear **T**icket
  - S = Ejecutar procedimiento de agente
  - E = **E**nviar correo electrónico a destinatarios
- **Dirección de correo electrónico**: una lista separada por comas de las direcciones de correo electrónico adonde se envían las notificaciones.

Elaboración de informes de seguridad

Los siguientes conjuntos de datos están disponibles para admitir la creación de definiciones y

plantillas de informes personalizadas de **Endpoint Security**. Se encuentran en Info Center > Configurar y diseñar > **Partes de informes**.

- Conjunto de alarmas de KES
- Asignación de conjunto de alarmas de KES
- Registro de eventos de KES
- Estado de Exchange de KES
- Estado de máquina de KES
- Amenazas de KES
- Estadísticas de amenazas de KES

Además, se proporcionan las siguientes definiciones de informes heredados de “formato fijo”.

En esta sección

Resumen ejecutivo - Seguridad de extremos

Resumen Ejecutivo

El informe Resumen ejecutivo en Info Center > Elaboración de informes > Informes, incluye una sección denominada **Últimos N días de seguridad de extremos**. Incluye las siguientes estadísticas.

- Total de amenazas detectadas
- Amenazas Activas Actuales
- Amenazas Actuales en Vaults
- Amenazas Resueltas
- Exploraciones completas
- Actualizaciones realizadas
- Máquinas con KES instalado

El **Puntaje de salud de la red** del **Resumen ejecutivo** incluye la categoría **Puntaje de extremos**. Las amenazas no tratadas son aquellas que se indican en la pestaña **Amenazas actuales** en la página > **Ver amenazas** *(página 11)*, en Seguridad. Las amenazas no tratadas representan posibles problemas del sistema. A la cantidad de amenazas no tratadas generadas por cada máquina en el período de tiempo especificado se les da el puntaje de la siguiente manera:

0 amenazas no tratadas	100%
1 a 4 amenazas no tratadas	75%
5 a 10 amenazas no tratadas	50%
más de 10 amenazas no tratadas	25%

Puede ajustar cuánto afecta cada categoría al **Puntaje de salud de la red** total mediante el ajuste del valor **peso** para cada categoría. Los pesos están comprendidos entre 0 y 100. Fije el peso en cero para desactivar dicha categoría.

Seguridad - Configuración

Info Center > Elaboración de informes > Informes > Seguridad > Configuración

- Se muestra sólo si el módulo complementario Seguridad está instalado.
- Se proporciona información similar en Seguridad > Estado de seguridad *(página 5)*, Ver registros *(página 13)* y Ver amenazas *(página 11)*.

La definición de informe **Seguridad - Configuración** genera informes para los siguientes tipos de datos de seguridad que mantiene el VSA.

- Hora de Instalación
- Instalador
- Versión
- Expiración de la Licencia
- Perfil Asignado
- Detalles del Perfil
- Configuración de Alarmas

Seguridad - Seguridad

Info Center > Elaboración de informes > Informes > Seguridad > Amenazas actuales

- Se muestra sólo si el módulo complementario Seguridad está instalado.
- Se proporciona información similar en Seguridad > Estado de seguridad *(página 5)*, Ver registros *(página 13)* y Ver amenazas *(página 11)*.

La definición de informe **Seguridad - Amenazas Actuales** genera informes para los siguientes tipos de datos de seguridad que mantiene el VSA.

- Resumen
- Resumen Categoría de Amenaza
- Amenazas Actuales

Selección de Tiempo

- **Seleccionar el tipo de rango de tiempo** : filtra por un tipo fijo del rango de fechas.
- **Número de días**: sólo se aplica si se selecciona `Last N Days` como tipo de intervalo de tiempo.
- **DateTime de inicio personalizada**: sólo se aplica si se selecciona `Fixed Range` como tipo de intervalo de tiempo.
- **DateTime de finalización personalizada**: sólo se aplica si se selecciona `Fixed Range` como tipo de intervalo de tiempo.

Seguridad - Amenazas históricas

Info Center > Elaboración de informes > Informes > Seguridad > Amenazas históricas

- Se muestra sólo si el módulo complementario Seguridad está instalado.
- Se proporciona información similar en Seguridad > Estado de seguridad *(página 5)*, Ver registros *(página 13)* y Ver amenazas *(página 11)*.

La definición de informe **Seguridad - Amenazas históricas** genera informes para los siguientes tipos de datos de seguridad que mantiene el VSA.

- Resumen
- Resumen Categoría de Amenaza
- Amenazas Actuales

Selección de Tiempo

- **Seleccionar el tipo de rango de tiempo** : filtra por un tipo fijo del rango de fechas.
- **Número de días**: sólo se aplica si se selecciona `Last N Days` como tipo de intervalo de tiempo.
- **DateTime de inicio personalizada**: sólo se aplica si se selecciona `Fixed Range` como tipo de intervalo de tiempo.
- **DateTime de finalización personalizada**: sólo se aplica si se selecciona `Fixed Range` como tipo de intervalo de tiempo.

Seguridad - Registro KES

Info Center > Elaboración de informes > Informes > Seguridad - Registro KES

- Se muestra sólo si el módulo complementario Seguridad está instalado.
- En Agente > Registros de agente, se muestran las entradas de registro por tipo de registro e ID de máquina.

La definición de informe Registro KES genera un informe de entradas del registro de Endpoint Security por ID de máquina.

Configure la definición de su informe usando los siguientes parámetros:

- **Cantidad de días para el registro de consulta*** : cantidad de días antes de la fecha/hora actual para incluir en el informe.
- **Mostrar entradas que coinciden con la siguiente descripción (usar * para comodines)** : ingrese una cadena para filtrar las entradas según su descripción. Incluya un comodín con asterisco (*) con el texto que ingresa para coincidir con registros múltiples.
- **Ignorar máquinas sin datos :** tilde esta casilla para que se muestren solo las ID de máquina que tengan datos coincidentes con los otros parámetros del filtro.

Índice