System Center

Endpoint Protection para Mac

Manual de instalación y guía del usuario

Microsoft

Contenido

System Center Endpoint Protection

Dada la creciente popularidad de los sistemas operativos basados en Unix, los autores de código malicioso han empezado a desarrollar más amenazas dirigidas a los usuarios de Mac. System Center Endpoint Protection ofrece una protección potente y eficaz contra estas nuevas amenazas. System Center Endpoint Protection cuenta con la capacidad de desviar las amenazas de Windows, por lo que protege a los usuarios de Mac cuando interaccionan con usuarios de Windows, y viceversa. Aunque el código malicioso de Windows no supone una amenaza directa para Mac, pero al desactivar el código malicioso que haya infectado un ordenador Mac, se evita su difusión a otros ordenadores basados en Windows a través de una red local o Internet.

Requisitos del sistema

Para disfrutar de un funcionamiento óptimo de System Center Endpoint Protection, el sistema debería cumplir con los siguientes requisitos de hardware y software:

System Center Endpoint Protection:

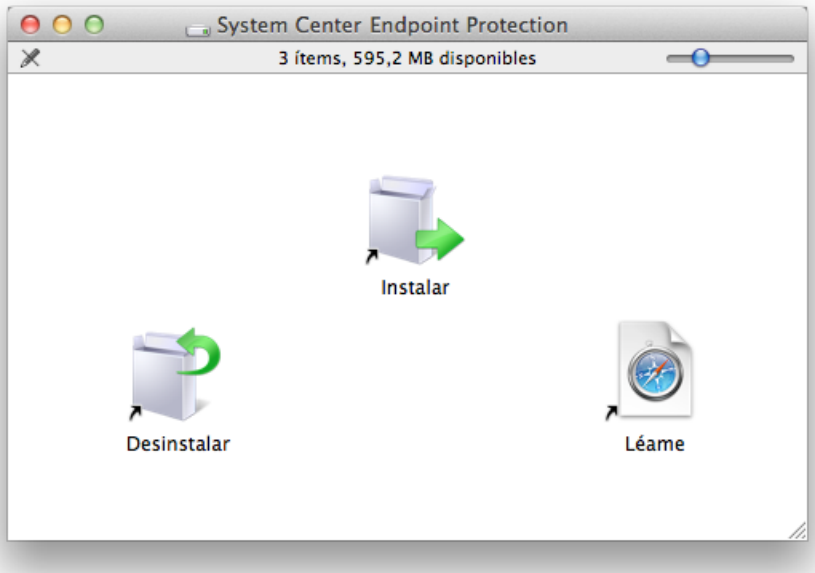
	Requisitos del sistema
Arquitectura de procesador	Intel® de 32 o 64 bits
Sistema operativo	Mac OS X 10.6 o superior
Memoria	512 MB
Espacio libre en disco	100 MB

Instalación

Antes de iniciar el proceso de instalación, cierre todos los programas que estén abiertos en el ordenador. System Center Endpoint Protection contiene componentes que podrían entrar en conflicto con otros programas antivirus que ya estén instalados en el ordenador. Con el fin de evitar posibles problemas, se recomienda encarecidamente que elimine los demás programas antivirus. Se puede instalar System Center Endpoint Protection desde un CD/DVD de instalación o desde el archivo que descargue de nuestro sitio web.

Para iniciar el asistente de instalación, realice una de estas acciones:

- Si va a realizar la instalación desde el CD/DVD, insértelo en el ordenador, ábralo desde el escritorio o la ventana del Finder y haga doble clic en el icono **Instalar**.
- Si va a realizar la instalación desde un archivo descargado, abra el archivo y haga doble clic en el icono **Instalar**.



Ejecute el instalador; el asistente de instalación le proporcionará instrucciones para realizar la configuración básica. Una vez que haya aceptado el acuerdo de licencia de software y leído la declaración de privacidad, podrá elegir uno de estos tipos de instalación:

- Típica 4
- Personalizada 4

Instalación típica

El modo de instalación típica incluye opciones de configuración que son adecuadas para la mayoría de los usuarios. Esta configuración proporciona una seguridad máxima junto con un excelente rendimiento del sistema. La instalación típica es la opción predeterminada y se recomienda cuando no es necesaria una configuración específica.

Después de seleccionar el modo de instalación **Típica**, configure la **Detección de aplicaciones potencialmente indeseables**. Las aplicaciones potencialmente indeseables no tienen por qué ser maliciosas, pero pueden influir negativamente en el comportamiento del sistema operativo. Estas aplicaciones suelen instalarse con otros programas y puede resultar difícil detectarlas durante la instalación. Aunque estas aplicaciones suelen mostrar una notificación durante la instalación, se pueden instalar fácilmente sin su consentimiento.

Después de instalar System Center Endpoint Protection, debe realizar un análisis del ordenador para comprobar si existe código malicioso. En la ventana principal del programa, haga clic en **Análisis del ordenador** y, a continuación, en **Análisis estándar**. Para obtener más información acerca del análisis del ordenador a petición, consulte la sección Análisis del equipo a petición 10.

Instalación personalizada

El modo de instalación personalizada está diseñada para usuarios con experiencia que quieran modificar la configuración avanzada durante el proceso de instalación.

Después de seleccionar el modo de instalación **Personalizada**, se le pedirá que configure el **Servidor Proxy**. Si utiliza un servidor Proxy, puede definir sus parámetros seleccionando la opción **Conexión mediante servidor Proxy**. Introduzca la dirección IP o URL de su servidor Proxy en el campo **Dirección**. En el campo de puerto, especifique el puerto donde el servidor Proxy acepte conexiones

(el 3128, de forma predeterminada). En el caso de que el servidor Proxy requiera autentificación, debe introducir un **nombre de usuario** y una **contraseña** válidos que permitan acceder al servidor Proxy. Si está seguro de que no se utiliza ningún servidor Proxy, seleccione la opción **No se utiliza un servidor Proxy**. Si no está seguro, seleccione **Utilizar configuración del sistema (recomendado)** para utilizar la configuración actual del sistema.

En el próximo paso, puede utilizar la opción **Definir los usuarios privilegiados** para seleccionar a los que podrán editar la configuración del programa. Seleccione los usuarios de usuarios situada a la izquierda y utilice la opción **Agregar** para añadirlos a la lista **Usuarios con privilegios**. Para ver todos los usuarios del sistema, seleccione la opción **Mostrar todos los usuarios**.

El paso siguiente del proceso de instalación consiste en configurar la **Detección de aplicaciones potencialmente indeseables**. Las aplicaciones potencialmente indeseables no tienen por qué ser maliciosas, pero pueden influir negativamente en el comportamiento del sistema operativo. Estas aplicaciones suelen instalarse con otros programas y puede resultar difícil detectarlas durante la instalación. Aunque estas aplicaciones suelen mostrar una notificación durante la instalación, se pueden instalar fácilmente sin su consentimiento.

Después de instalar System Center Endpoint Protection, debe realizar un análisis del ordenador para comprobar si existe código malicioso. En la ventana principal del programa, haga clic en **Análisis del ordenador** y, a continuación, en **Análisis estándar**. Para obtener más información acerca de los análisis a petición, consulte la sección Análisis del ordenador a petición 10.

Desinstalación

Si desea desinstalar System Center Endpoint Protection del ordenador, siga estos pasos:

- Inserte el CD/DVD de instalación de System Center Endpoint Protection en el ordenador, ábralo desde el escritorio o la ventana del Finder y haga doble clic en el icono **Desinstalar**.
- Abra el archivo de desinstalación de System Center Endpoint Protection (*.dmg*) y haga doble clic en el icono **Desinstalar**, o bien
- Inicie **Finder**, abra la carpeta **Aplicaciones** de la unidad de disco duro, pulse Ctrl y haga clic en el icono System Center Endpoint Protection y seleccione la opción **Mostrar contenido del paquete**. Abra la carpeta **Contents > Helpers** y haga doble clic en el icono **Uninstaller**.

Guía para principiantes

En este capítulo se proporciona una descripción general inicial de System Center Endpoint Protection y su configuración básica.

Interfaz de usuario

La ventana principal de System Center Endpoint Protection se divide en dos secciones principales. En la ventana principal, situada a la derecha, se muestra información relativa a la opción seleccionada en el menú principal de la izquierda.

A continuación, se muestra una descripción de las opciones del menú principal:

- **Estado de la protección**: proporciona información acerca del estado de protección de System Center Endpoint Protection. Si está activada la opción **Modo avanzado**, se muestra el submenú **Estadísticas**.
- **Análisis del ordenador**: esta opción le permite configurar e iniciar el análisis del ordenador a petición.
- **Actualización**: muestra información acerca de las actualizaciones de la base de firmas de virus.
- **Configuración**: seleccione esta opción para ajustar el nivel de seguridad del ordenador. Si está activada la opción **Modo avanzado**, se muestra el submenú **Antivirus y antispyware**.
- **Herramientas**: permite acceder a **Archivos de registro**, **Cuarentena** y **Planificador de tareas**. Esta opción solo se muestra en el **Modo avanzado**.
- **Ayuda**: proporciona información acerca del programa y acceso a los archivos de ayuda.

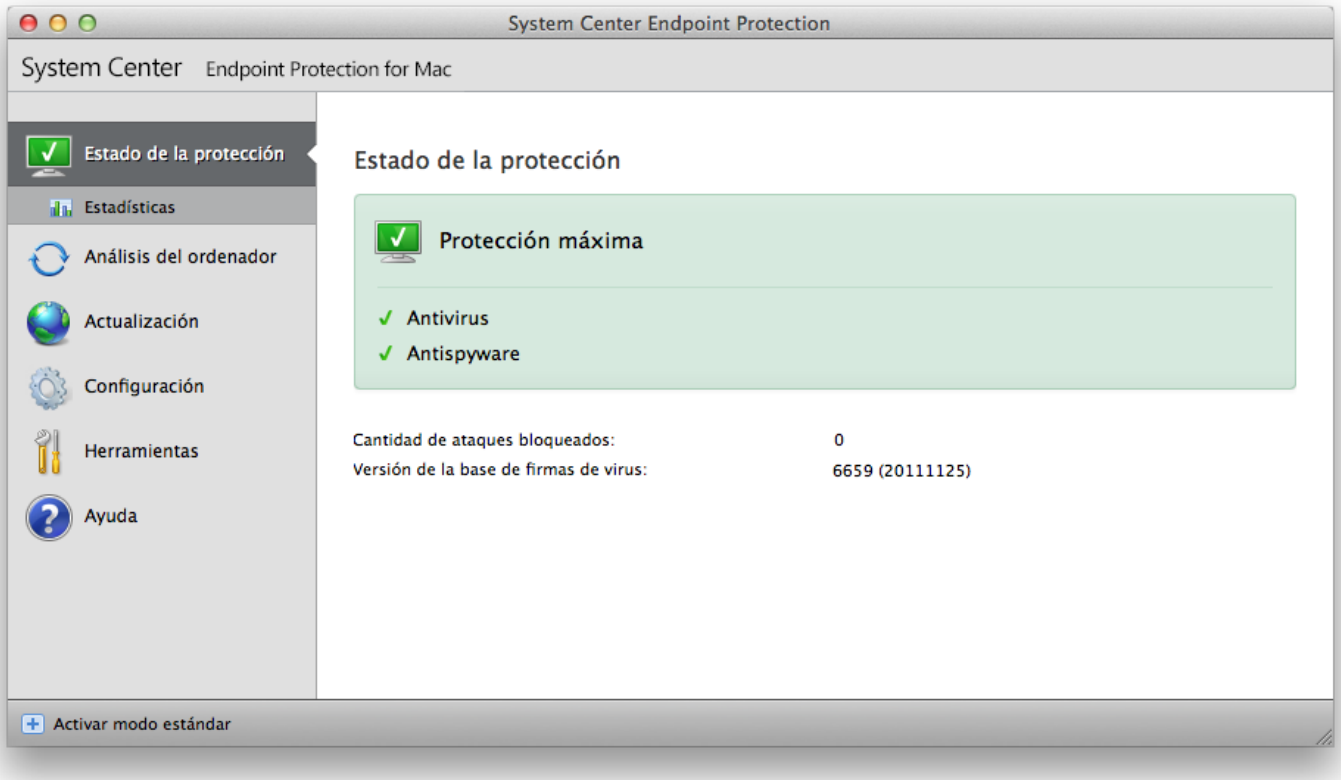
La interfaz de usuario de System Center Endpoint Protection permite a los usuarios alternar entre los modos estándar y avanzado. El 'Modo estándar' permite acceder a las características necesarias para realizar operaciones habituales. No muestra ninguna de las opciones avanzadas. Para cambiar de modo, haga clic en el icono con el signo de suma (**+**) situado junto a **Activar el modo avanzado/Activar modo estándar**, en la esquina inferior izquierda de la ventana principal del programa o pulse cmd + M.

Al cambiar al 'Modo avanzado', la opción **Herramientas** se añade al menú principal. La opción **Herramientas** le permite acceder a los submenús de **Archivos de registro**, **Cuarentena** y **Planificador de tareas**.

NOTA: Todas las demás instrucciones de esta guía se llevarán a cabo en el **Modo avanzado**.

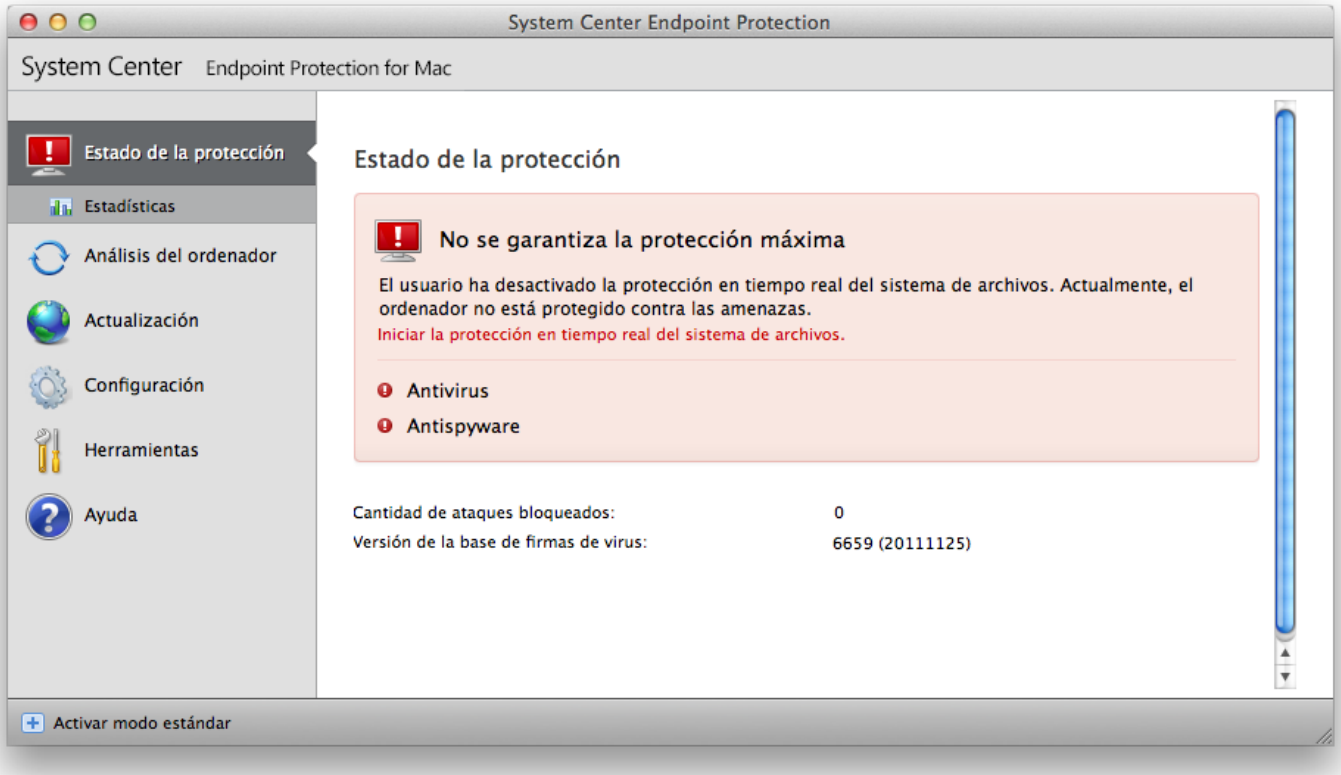
Comprobación del funcionamiento del sistema

Para ver el **Estado de la protección**, haga clic en la primera opción del menú principal. Se mostrará un resumen del estado de funcionamiento de System Center Endpoint Protection en la ventana principal, así como el submenú **Estadísticas**. Selecciónelo para ver información y datos estadísticos más detallados acerca de los análisis realizados en el sistema. La ventana Estadísticas solo está disponible en el modo avanzado.



Qué hacer si el programa no funciona correctamente

Si los módulos activados funcionan correctamente, se les asigna una marca verde. En caso contrario, se muestra un signo de exclamación rojo o un icono de notificación naranja, además de información adicional acerca del módulo en la parte superior de la ventana. También se muestra una sugerencia de solución para reparar el módulo. Para cambiar el estado de los módulos individuales, haga clic en **Configuración** en el menú principal y, a continuación, en el módulo que desee.



Trabajar con System Center Endpoint Protection

Protección antivirus y antispyware

La protección antivirus protege el sistema contra ataques maliciosos mediante la modificación de archivos que presenten amenazas potenciales. Si se detecta una amenaza con código malicioso, el módulo antivirus puede bloquearlo y, a continuación, desinfectarlo, eliminarlo o ponerlo en cuarentena.

Protección del sistema de archivos en tiempo real

La protección del sistema de archivos en tiempo real controla todos los sucesos relacionados con el antivirus en el sistema. Todos los archivos se analizan en busca de códigos maliciosos en el momento de abrirlos, crearlos o ejecutarlos en el ordenador. La protección del sistema de archivos en tiempo real se inicia al arrancar el sistema.

Configuración de la protección en tiempo real

La protección del sistema de archivos en tiempo comprueba todos los tipos de medios y activa un análisis en función de varios sucesos. La protección del sistema de archivos en tiempo real puede diferir entre los archivos recién creados y los ya existentes. En el caso de los archivos recién creados, se puede aplicar un nivel de control más exhaustivo.

La protección en tiempo real comienza de forma predeterminada cuando se inicia el sistema y proporciona un análisis ininterrumpido. En algunos casos especiales (por ejemplo, en caso de conflicto con otro programa de análisis en tiempo real), la protección en tiempo real se puede desactivar. Para desactivarla, haga clic en el icono de System Center Endpoint Protection, situado en la barra de menús (parte superior de la pantalla) y, a continuación, seleccione la opción **Desactivar protección del sistema de archivos en tiempo real**. La protección en tiempo real también se puede desactivar desde la ventana principal del programa (**Configuración** > **Antivirus y antispyware** > **Desactivar**).

Para modificar la configuración avanzada de la protección en tiempo real, seleccione **Configuración** > **Introducir preferencias de aplicación...** > **Protección** > **Protección en tiempo real** y haga clic en el botón **Configuración...**, situado junto a **Opciones avanzadas** (descritas en el apartado Opciones avanzadas de análisis 8).

Analizar (análisis cuando se cumpla la condición)

De forma predeterminada, todos los archivos se analizan cuando se **abren**, **crean** o **ejecutan**. Le recomendamos que mantenga la configuración predeterminada, ya que ofrece el máximo nivel de protección en tiempo real para su ordenador.

Opciones avanzadas de análisis

En esta ventana, puede definir los tipos de objeto que desee que el motor analice y activar/desactivar la opción **Heurística avanzada** , así como modificar la configuración de los archivos comprimidos y el caché de archivos.

No recomendamos cambiar los valores predeterminados de la sección **Configuración predeterminada de archivos comprimidos** a menos que sea necesario para resolver un problema específico, ya que un valor superior de anidamiento de archivos comprimidos podría afectar al rendimiento del sistema.

Puede alternar el análisis con tecnología heurística avanzada para los archivos ejecutados, así como para los archivos creados y modificados por separado. Para ello, haga clic en la casilla de verificación **Heurística avanzada** en todas las secciones de parámetros del motor correspondientes.

Para usar la menor cantidad posible de recursos del sistema cuando se utiliza la protección en tiempo real, puede definir el tamaño del caché de optimización. Este comportamiento se activa cuando se utiliza la opción **Activar la desinfección de la caché de archivos**. Si está desactivada, todos los archivos se analizarán cada vez que se acceda a ellos. Los archivos no se analizarán repetidamente tras su almacenamiento en caché (a no ser que se hayan modificado) hasta que el caché alcance el tamaño especificado. Los archivos se vuelven a analizar inmediatamente después de cada actualización de la base de firmas de virus.

Haga clic en **Activar la desinfección del caché de archivos** para activar/desactivar esta función. Para definir la cantidad de archivos que se almacenarán en caché, basta con introducir el valor deseado en el campo de entrada situado junto a **Tamaño del caché**.

Los demás parámetros del análisis se pueden ajustar en la ventana **Configuración del motor**. Puede definir el tipo de **Objetos** que se deban analizar, con qué **Opciones** y **Nivel de desinfección**, así como las **Extensiones** y los **Límites** de tamaño de archivos para la protección del sistema de archivos en tiempo real. Para acceder a la ventana de configuración del motor, haga clic en el botón **Configuración...** situado junto a **Motor** en la ventana 'Configuración avanzada'. Para obtener más información acerca de los parámetros del motor, consulte la sección Configuración de parámetros del motor 13.

Exclusiones del análisis

En esta sección se explica cómo excluir del análisis determinados archivos y carpetas.

- **Ruta**: ruta de los archivos y carpetas excluidos.
- **Amenaza**: si se muestra el nombre de una amenaza junto a un archivo excluido, significa que el archivo se excluye únicamente para dicha amenaza, pero no por completo. Por lo tanto, si más adelante este archivo se infecta con otro código malicioso, el módulo antivirus lo detectará.
- **Agregar...**: excluye objetos de la detección. Introduzca la ruta de un objeto (también puede utilizar los comodines * y ?) o seleccione la carpeta o archivo en la estructura de árbol.
- **Editar...**: le permite modificar las entradas seleccionadas.
- **Eliminar**: elimina las entradas seleccionadas.
- **Predeterminado**: cancela todas las exclusiones.

Modificación de la configuración de protección en tiempo real

La protección en tiempo real es el componente más importante a la hora de mantener un sistema seguro. Tenga cuidado cuando modifique los parámetros de protección en tiempo real. Le recomendamos que los modifique únicamente en casos concretos, como, por ejemplo, si se produce un conflicto con una aplicación determinada o durante el análisis en tiempo real de otro programa antivirus.

Una vez instalado System Center Endpoint Protection, se optimizará toda la configuración para proporcionar a los usuarios el máximo nivel de seguridad del sistema. Para restaurar la configuración predeterminada, haga clic en el botón **Predeterminado** ubicado en la parte inferior izquierda de la ventana **Protección en tiempo real** (**Configuración** > **Introducir preferencias de aplicación...**). > **Protección** > **Protección en tiempo real**).

Comprobación de la protección en tiempo real

Para verificar que la protección en tiempo real funciona y detecta virus, utilice el archivo de prueba de eicar.com. Se trata de un archivo inofensivo especial detectable por todos los programas antivirus. El archivo fue creado por el instituto EICAR (European Institute for Computer Antivirus Research: 'Instituto Europeo para la Investigación de Antivirus') con el fin de comprobar la funcionalidad de los programas antivirus.

Para comprobar el estado de la protección en tiempo real de forma remota, conéctese al ordenador cliente con **Terminal** y emita el comando siguiente:

```
/Applications/.scep/Contents/MacOS/scep_daemon --status
```

El estado del análisis en tiempo real se mostrará como `RTPStatus=Enabled` o `RTPStatus=Disabled`.

El resultado del comando bash de Terminal también incluye estos estados:

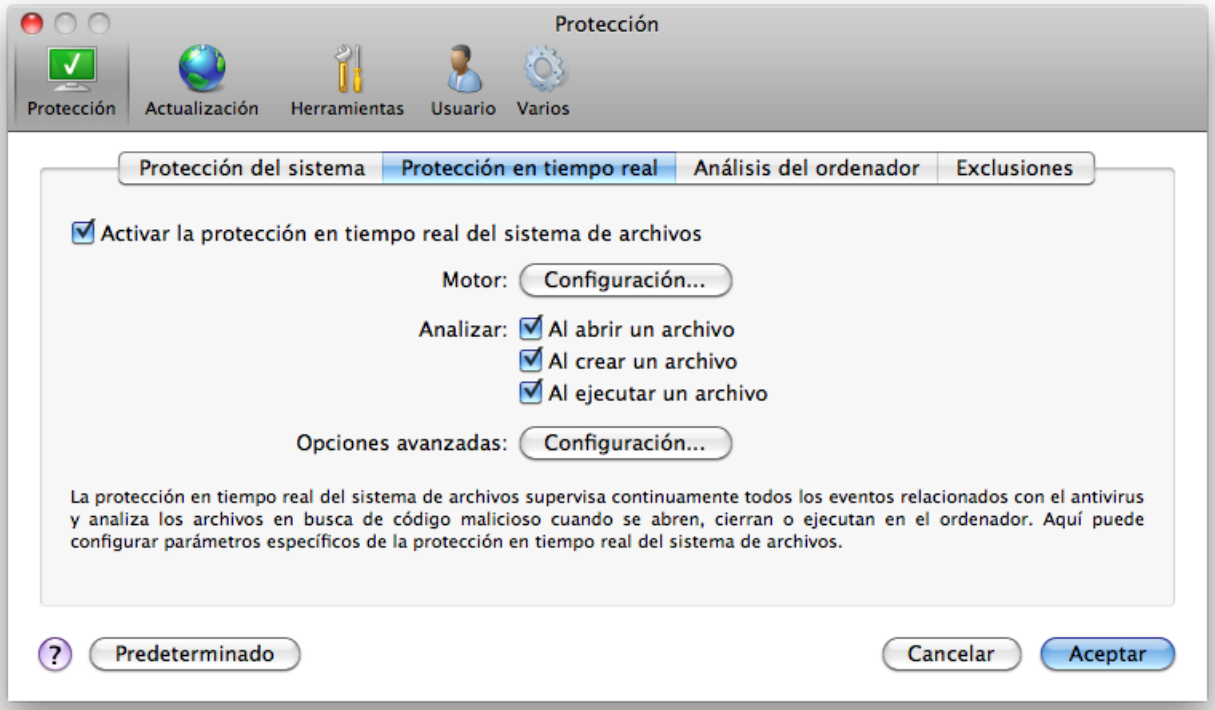
- versión de System Center Endpoint Protection instalada en el ordenador cliente
- fecha y versión de la base de firmas de virus
- ruta al servidor de actualización

NOTA: Solo se recomienda el uso de Terminal a usuarios avanzados.

¿Qué debo hacer si la protección en tiempo real no funciona?

En este capítulo describimos las situaciones en las que pueden surgir problemas a la hora de utilizar la protección en tiempo real y cómo resolverlos.

Protección en tiempo real desactivada
Si un usuario desactivó la protección en tiempo real sin darse cuenta, será necesario reactivarla. Para ello, vaya a **Configuración** > **Antivirus y antispyware** y haga clic en el vínculo **Activar la protección del sistema de archivos en tiempo real**, situado a la derecha de la ventana principal del programa. También puede activar la protección del sistema de archivos en tiempo real en la ventana 'Configuración avanzada', en **Protección** > **Protección en tiempo real**, con la opción **Activar la protección del sistema de archivos en tiempo real**.



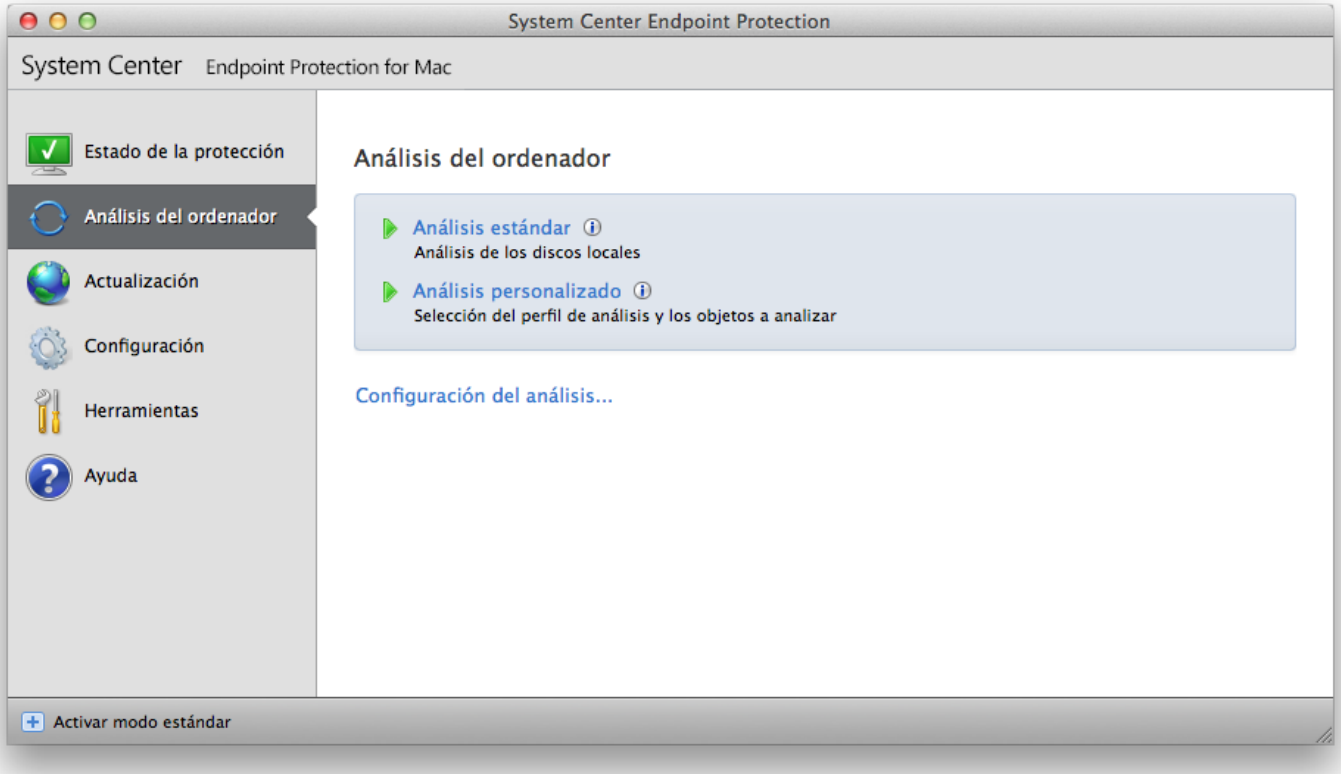
La protección en tiempo real no detecta ni desinfecta las amenazas
Asegúrese de que no tenga instalados otros programas antivirus en el ordenador. Si hay dos protecciones en tiempo real activas a la vez, pueden entrar en conflicto. Le recomendamos que desinstale uno de los programas antivirus del sistema.

La protección en tiempo real no se inicia
Si la protección en tiempo real no se activa al iniciar el sistema, es posible que se deba a que entre en conflicto con otros programas. Si este es el caso, consulte a sus especialistas del servicio de atención al cliente.

Análisis del ordenador a petición

Si sospecha que su equipo está infectado (se comporta de manera anormal), ejecute un **Análisis del ordenador** > **Análisis estándar** para examinar el equipo en busca de infecciones. Para contar con la mayor protección, el ordenador debe analizarse de forma periódica como parte de las medidas de seguridad rutinarias, no únicamente cuando se crea que haya alguna amenaza. Los análisis regulares ayudan a detectar amenazas que no se detectaron durante el análisis en tiempo real, cuando se guardaron en el disco. Esto puede ocurrir si se ha desactivado el análisis en tiempo real en el momento de la infección o si la base de firmas de virus no estaba actualizada.

Le recomendamos que ejecute un análisis a petición una o dos veces al mes como mínimo. El análisis se puede configurar como una tarea programada en **Herramientas** > **Planificador de tareas**.



También puede arrastrar los archivos y carpetas seleccionados desde el escritorio o la ventana del Finder a la pantalla principal de System Center Endpoint Protection, al icono del Dock, al icono de la barra de menú (parte superior de la pantalla) o al icono de la aplicación (ubicado en la carpeta */Aplicaciones*).

Tipo de análisis

Existen dos tipos de análisis del ordenador a petición. **Análisis estándar** analiza el sistema rápidamente, sin necesidad de realizar ninguna configuración adicional de los parámetros de análisis. **Análisis personalizado** le permite seleccionar perfiles de análisis predefinidos y elegir objetos del análisis específicos.

Análisis estándar

El análisis estándar le permite iniciar rápidamente un análisis del ordenador y desinfectar los archivos infectados sin necesidad de que intervenga el usuario. La principal ventaja es su sencillo funcionamiento, sin configuraciones de análisis detalladas. El análisis estándar comprueba todos los archivos de todas las carpetas y desinfecta o elimina automáticamente las amenazas detectadas. El nivel de desinfección se establece de forma automática en el valor predeterminado. Para obtener información más detallada acerca de los tipos de desinfección, consulte el apartado Desinfección 14.

Análisis personalizado

El **Análisis personalizado** es la solución ideal para especificar parámetros de análisis, como, por ejemplo, los objetos y métodos del análisis. El análisis personalizado tiene la ventaja de que permite configurar los parámetros detalladamente. Las diferentes configuraciones se pueden guardar en perfiles de análisis definidos por el usuario, que pueden resultar útiles si el análisis se realiza reiteradamente con los mismos parámetros.

Para seleccionar objetos de análisis, seleccione **Análisis del ordenador** > **Análisis personalizado** y, a continuación, seleccione los **Objetos de análisis** específicos que desee en la estructura de árbol. Los objetos de análisis también se pueden especificar con más precisión al introducir la ruta a la carpeta o los archivos que se deseen incluir en el análisis. Si únicamente quiere analizar el sistema sin realizar acciones de desinfección adicionales, seleccione la opción **Analizar sin desinfectar**. Además, puede hacer clic en **Configuración...** para, de este modo, seleccionar uno de los tres niveles de desinfección. > **Desinfección**.

Los análisis del ordenador en el modo personalizado están recomendados para usuarios avanzados con experiencia previa en la utilización de programas antivirus.

Objetos de análisis

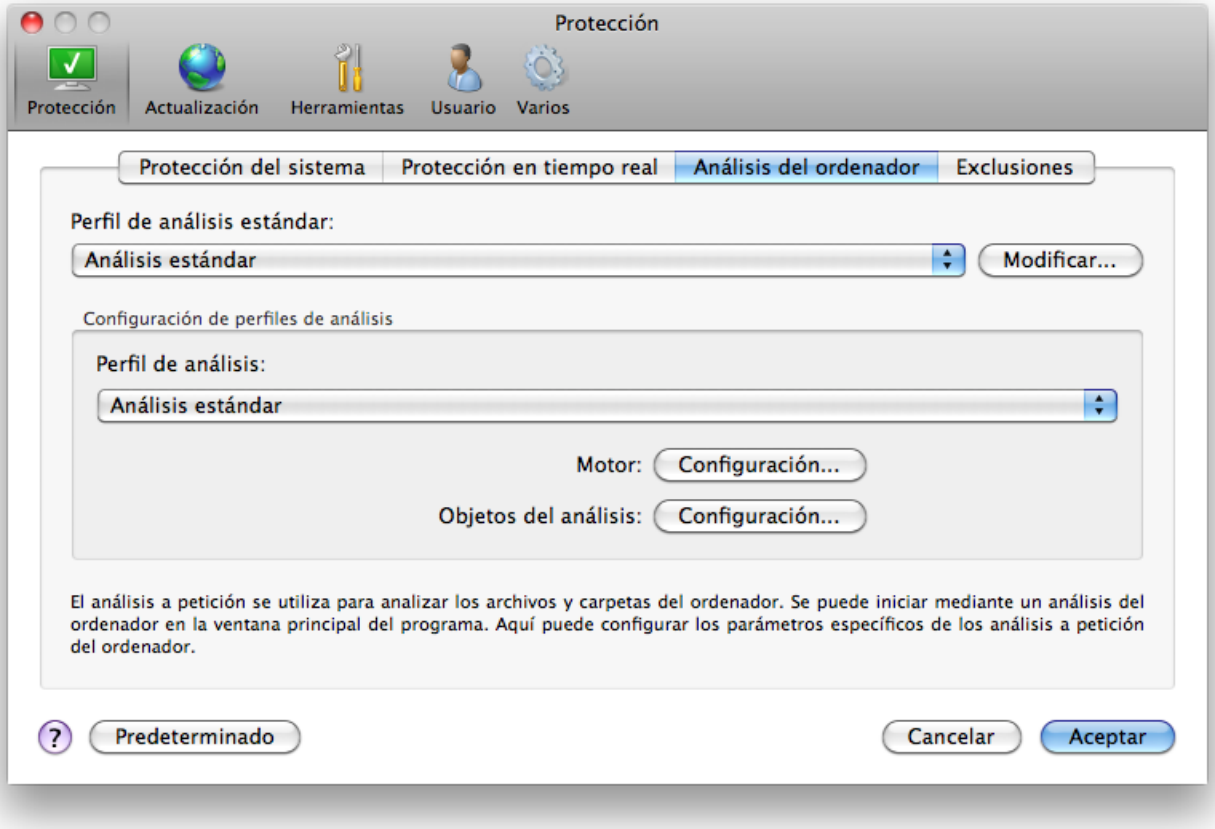
La estructura de árbol de objetos de análisis le permite seleccionar los archivos y carpetas que se analizarán en busca de virus. Las carpetas también se pueden seleccionar según la configuración de un perfil.

Los objetos de análisis se pueden especificar con más precisión al introducir la ruta a la carpeta o los archivos que se deseen incluir en el análisis. Seleccione los objetos en la estructura de árbol que incluya todas las carpetas disponibles en el ordenador.

Perfiles de análisis

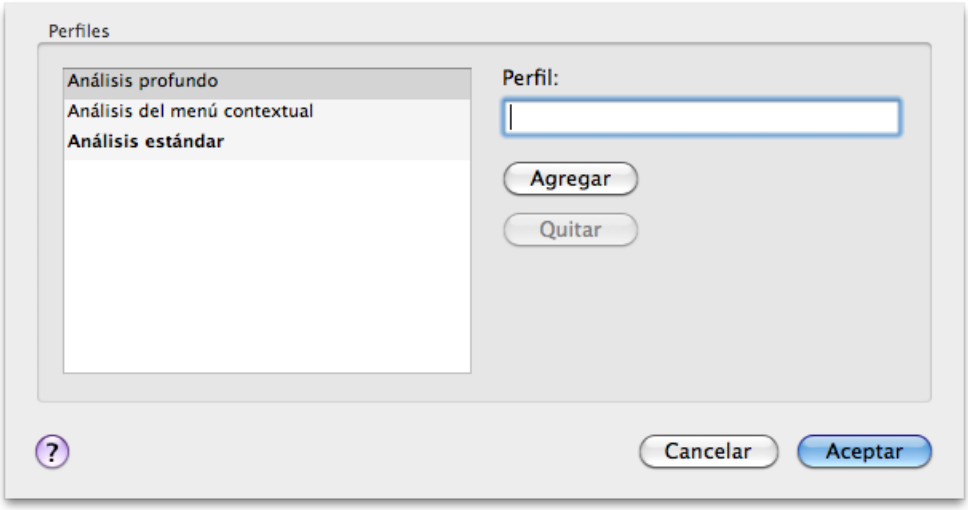
Puede guardar sus perfiles de análisis preferidos para próximas sesiones de análisis. Le recomendamos que cree un perfil diferente (con varios objetos de análisis, métodos de análisis y otros parámetros) para cada uno de los análisis que realice con frecuencia.

Para crear un perfil nuevo, vaya a **Configuración** > **Introducir preferencias de aplicación...** > **Protección** > **Análisis del ordenador** y haga clic en **Editar...**, junto a la lista de perfiles actuales.



Si necesita ayuda para crear un perfil de análisis que se adecúe a sus necesidades, consulte la sección Configuración de parámetros del motor 13 para ver una descripción de los diferentes parámetros de la configuración del análisis.

Ejemplo: supongamos que desea crear su propio perfil de análisis y parte de la configuración del análisis estándar es adecuada; sin embargo, no desea analizar los empaquetadores en tiempo real ni las aplicaciones potencialmente peligrosas y, además, quiere aplicar una desinfección estricta. En la ventana **Lista de perfiles del análisis a petición**, escriba el nombre del perfil, haga clic en el botón **Agregar** y en **Aceptar** para, de este modo, confirmar la operación. A continuación, ajuste los parámetros **Motor** y **Objetos del análisis** en función de sus requisitos.



Configuración de parámetros del motor

La tecnología que utiliza System Center Endpoint Protection es proactiva, lo que significa que también proporciona protección durante la fase inicial de expansión de una nueva amenaza. Utiliza una combinación de diferentes métodos (análisis de código, emulación de código, firmas genéricas y firmas de virus) que funcionan de forma conjunta para mejorar de forma significativa la seguridad del sistema. El motor de análisis es capaz de controlar varios flujos de datos de forma simultánea, de manera que maximiza la eficacia y la velocidad de detección. Además, esta tecnología elimina eficazmente los programas peligrosos (rootkits).

Las opciones de configuración de la tecnología del motor permiten que el usuario especifique distintos parámetros de análisis:

- Los tipos de archivos y extensiones que se deban analizar
- La combinación de diferentes métodos de detección
- Los niveles de desinfección, etc.

Para entrar en la ventana de configuración, haga clic en **Configuración** > **Antivirus y antispyware** > **Configuración avanzada de la protección antivirus y antispyware** y, a continuación, haga clic en el botón **Configuración...**, situado junto a los comodines **Protección del sistema**, **Protección en tiempo real** y **Análisis del ordenador**. Es posible que cada situación de seguridad requiera una configuración diferente. Con esto en mente, los parámetros del motor se pueden configurar de forma individual para los siguientes módulos de protección:

- **Protección del sistema** > Verificación automática de archivos en el inicio
- **Protección en tiempo real** > Protección del sistema de archivos en tiempo real
- **Análisis del ordenador** > Análisis del ordenador a petición

Los parámetros del motor están optimizados específicamente para cada módulo, por lo que su modificación puede afectar al funcionamiento del sistema de forma significativa. Por ejemplo, si cambia la configuración para analizar siempre los empaquetadores en tiempo real o activa la tecnología heurística avanzada en el módulo de protección del sistema de archivos en tiempo real, el sistema podría ralentizarse. Por este motivo, se recomienda que no modifique los parámetros predeterminados del motor de todos los módulos, a excepción de 'Análisis del ordenador'.

Objetos

En la sección **Objetos** se pueden definir los archivos del ordenador que se analizarán en busca de amenazas.

- **Archivos**: analiza todos los tipos de archivos comunes (programas, fotografías, audio, archivos de vídeo, archivos de base de datos, etc.).
- **Enlaces simbólicos**: (solo análisis a petición) analiza un tipo especial de archivos que contengan una cadena de texto que el sistema operativo interprete y siga como una ruta a otro archivo o directorio.
- **Archivos de correo electrónico**: (no disponible en la 'Protección en tiempo real') analiza archivos especiales que contengan mensajes de correo electrónico.
- **Buzones de correo**: (no disponible en la 'Protección en tiempo real') analiza los buzones de usuarios que haya en el sistema. El uso incorrecto de esta opción podría tener como resultado un conflicto con el cliente de correo electrónico.
- **Archivos comprimidos**: (no disponible en la 'Protección en tiempo real') analiza los archivos comprimidos (.rar, .zip, .arj, .tar, etc.).
- **Archivos comprimidos de autoextracción**: (no disponible en la 'Protección en tiempo real') analiza los archivos incluidos en los archivos comprimidos de autoextracción.
- **Empaquetadores en tiempo real**: a diferencia de los archivos comprimidos estándares, los empaquetadores en tiempo real se descomprimen en la memoria, además de los empaquetadores estáticos estándares (UPX, yoda, ASPack, FGS, etc.).

Opciones

En la sección **Opciones**, se pueden seleccionar los métodos utilizados durante un análisis del sistema en busca de amenazas. Están disponibles estas opciones:

- **Heurística**: la tecnología heurística hace referencia a un algoritmo que analiza la actividad (maliciosa) de los programas. Su principal ventaja es la habilidad para detectar nuevo software malicioso que no existía o que no estaba incluido en la lista de virus conocidos (base de firmas de virus).
- **Heurística avanzada**: la tecnología heurística avanzada consiste en un algoritmo heurístico exclusivo optimizado para detectar gusanos informáticos y troyanos escritos en lenguajes de programación de alto nivel. La capacidad de detección del programa es bastante superior gracias a esta tecnología heurística avanzada.
- **Aplicaciones potencialmente indeseables**: estas aplicaciones no tienen por qué ser maliciosas, pero pueden afectar al rendimiento del ordenador de manera negativa. Dichas aplicaciones suelen necesitar que se consienta su instalación. Si se encuentran en su ordenador, el sistema se comportará de manera diferente (en comparación con el estado en el que se encontrase antes de la instalación). Entre los cambios más significativos, destacan las ventanas emergentes no deseadas, la activación y ejecución de procesos ocultos, el aumento del uso de los recursos del sistema, los cambios en los resultados de búsqueda y las aplicaciones que se comunican con servidores remotos.
- **Aplicaciones potencialmente peligrosas**: estas aplicaciones son software comercial y legítimo que podría ser utilizado por atacantes si se instala sin el conocimiento del usuario. En esta clasificación se incluyen programas como, por ejemplo, las herramientas de acceso remoto: de ahí que esta opción esté desactivada de forma predeterminada.

Desinfección

Las opciones de desinfección determinan el comportamiento del análisis durante la desinfección de los archivos infectados. Hay 3 niveles de desinfección:

- **Sin desinfectar**: los archivos infectados no se desinfectan automáticamente. El programa mostrará una ventana de alerta y permitirá que el usuario seleccione una acción.
- **Desinfección estándar**: el programa intentará desinfectar o eliminar los archivos infectados de manera automática. Si no es posible seleccionar la acción correcta de manera automática, el programa ofrecerá una selección de acciones a seguir. La selección de acciones a seguir también aparecerá si no se puede completar una acción predefinida.
- **Desinfección exhaustiva**: el programa desinfectará o eliminará todos los archivos infectados (incluidos los archivos comprimidos). La única excepción la constituyen los archivos del sistema. Si no es posible desinfectarlos, se ofrece al usuario la opción de realizar una acción indicada en una ventana de alerta.

Alerta: en el modo predeterminado (Desinfección estándar), solamente se elimina todo el archivo comprimido si todos los archivos que contenga están infectados. Si el archivo comprimido también contiene archivos legítimos, no se eliminará. Si se detecta un archivo infectado en el modo de 'Desinfección exhaustiva', todo el archivo comprimido se eliminará aunque se encuentren archivos en buen estado.

Extensiones

Las extensiones son una parte del nombre de archivo delimitada por un punto. Estas definen el tipo y el contenido del archivo. En esta sección de la configuración de parámetros del motor se explica cómo definir los tipos de archivos que se deseen excluir del análisis.

De forma predeterminada, se analizan todos los archivos con independencia de cuál sea su extensión. Se puede agregar cualquier extensión a la lista de archivos excluidos del análisis. Con los botones **Agregar** y **Quitar**, puede activar o prohibir el análisis de las extensiones deseadas.

A veces es necesario excluir archivos del análisis, como, por ejemplo, cuando el análisis de ciertos tipos de archivos impide que el programe funcione de forma correcta. Por ejemplo, quizás sea recomendable excluir del análisis las extensiones *.log*, *.cfg* y *.tmp*.

Límites

En la sección **Límites** puede especificar el tamaño máximo de los objetos y niveles de archivos anidados que se analizarán:

- **Tamaño máximo:** define el tamaño máximo de los objetos que se vayan a analizar. El módulo antivirus solamente analizará los objetos cuyo tamaño sea inferior al especificado. Le recomendamos que no cambie el valor predeterminado, ya que no suele haber motivo para hacerlo. Esta opción solo deben cambiarla usuarios avanzados que tengan motivos específicos para excluir del análisis objetos de mayor tamaño.
- **Tiempo máximo de análisis:** define el tiempo máximo asignado para analizar un objeto. Si se introduce aquí un valor definido por el usuario, el módulo antivirus detendrá el análisis de los objetos cuando se haya agotado el tiempo, tanto si ha finalizado el análisis como si no.
- **Nivel máximo de anidamiento:** especifica la profundidad máxima del análisis de archivos comprimidos. Le recomendamos que no cambie el valor predeterminado de 10: en circunstancias normales, no debería haber motivos para hacerlo. Si el análisis finaliza antes de tiempo debido al número de archivos anidados, el archivo comprimido quedará sin analizar.

- **Tamaño máximo del archivo:** esta opción le permite especificar el tamaño máximo de los archivos incluidos en archivos comprimidos (al extraerlos) que se vayan a analizar. Si el análisis finaliza antes de tiempo debido a este límite, el archivo comprimido quedará sin analizar.

Otros

Si la opción 'Optimización inteligente' está activada, se utiliza la configuración más adecuada para garantizar el nivel de análisis más eficaz y, al mismo tiempo, mantener la máxima velocidad de análisis posible. Los diferentes módulos de protección analizan de forma inteligente mediante la utilización de distintos métodos de análisis aplicados a tipos de archivo específicos. La 'Optimización inteligente' no se ha definido de forma estricta en el producto. Nuestro equipo de desarrollo implementa constantemente cambios nuevos que, posteriormente, se integran en System Center Endpoint Protection mediante actualizaciones periódicas. Si la 'Optimización inteligente' está desactivada, solamente se aplica la configuración definida por el usuario en el núcleo del motor del módulo donde se realice el análisis.

Analizar flujo de datos alternativo (solo análisis a petición)
Los flujos de datos alternativos (bifurcaciones de recursos/datos) que utiliza el sistema de archivos son asociaciones de carpetas y archivos que escapan a las técnicas de análisis ordinarias. Muchas amenazas intentan evitar la detección haciéndose pasar por flujos de datos alternativos.

Detección de una amenaza

Las amenazas pueden acceder al sistema desde varios puntos de entrada: páginas web, carpetas compartidas, correo electrónico o dispositivos informáticos extraíbles (USB, discos externos, CD, DVD, disquetes, etc.).

Si el ordenador muestra señales de infección por código malicioso —por ejemplo, se ralentiza, se bloquea con frecuencia, etc.—, le recomendamos que haga lo siguiente:

1. Abra System Center Endpoint Protection y haga clic en **Análisis del ordenador**.
2. Haga clic en **Análisis estándar** (para obtener más información, consulte el apartado Análisis estándar 11).
3. Una vez finalizado el análisis, revise el registro para consultar el número de archivos analizados, infectados y desinfectados.

Si solo desea analizar una parte específica del disco, haga clic en **Análisis personalizado** y seleccione los objetos que desee incluir en el análisis de virus.

A modo de ejemplo general de cómo se gestionan las amenazas en System Center Endpoint Protection, suponga que el supervisor del sistema de archivos en tiempo real, que utiliza el nivel de desinfección predeterminado, detecta una amenaza. El supervisor intentará desinfectar o eliminar el archivo. Si no se dispone de ninguna tarea predefinida para el módulo de protección en tiempo real, una ventana de alerta le pedirá que seleccione una opción. Normalmente, están disponibles las opciones **Desinfectar**, **Eliminar** y **Sin acciones**. No se recomienda seleccionar **Sin acciones**, ya que los archivos infectados quedarían intactos. La única excepción es cuando esté seguro de que el archivo sea inofensivo y se haya detectado por error.

Desinfección y eliminación: inicie la desinfección si un archivo ha sido infectado por un virus que le haya añadido un código malicioso. Si es este el caso, intente desinfectar primero el archivo infectado para devolverlo a su estado original. Si el archivo consta exclusivamente de código malicioso, se eliminará.

Eliminación de amenazas en archivos comprimidos: en el modo de desinfección predeterminado, solamente se eliminará todo el archivo comprimido si todos los archivos que contenga están infectados. En otras palabras, no se eliminan los archivos comprimidos si también contienen archivos no infectados e inofensivos. Sin embargo, tenga cuidado cuando realice un análisis con **Desinfección exhaustiva**, ya que el archivo comprimido se eliminará si contiene, como mínimo, un archivo infectado, sin tener en cuenta el estado de los demás.

Actualización del programa

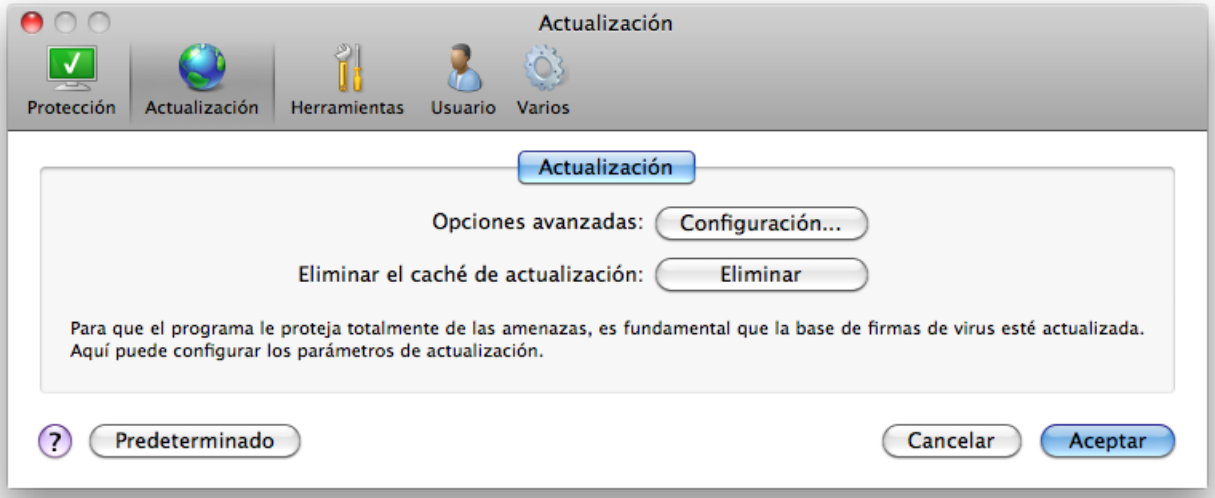
Es necesario actualizar System Center Endpoint Protection de forma periódica para mantener el máximo nivel de seguridad. El módulo de actualización descarga la base de firmas de virus más reciente para, de este modo, garantizar que el programa esté siempre al día.

Haga clic en **Actualización** en el menú principal para comprobar el estado de la actualización, así como la fecha y la hora de la última actualización y si es necesario actualizar el programa. Para comenzar el proceso de actualización manualmente, haga clic en **Actualizar la base de firmas de virus ahora**.

En circunstancias normales, cuando las actualizaciones se descarguen correctamente, se mostrará el mensaje *No es necesario realizar la actualización: la base de firmas de virus instalada está actualizada* en la ventana Actualización.

La ventana Actualización también contiene información acerca de la versión de la base de firmas de virus. Esta indicación numérica es, a la vez, un vínculo activo al sitio web donde se muestran todas las firmas agregadas en la actualización correspondiente.

Configuración de actualizaciones



Para activar el uso del modo de prueba (descarga actualizaciones de prueba), haga clic en el botón **Configuración...** situado junto a **Opciones avanzadas** y seleccione la casilla de verificación **Activar modo de prueba**. Para desactivar las notificaciones de la bandeja del sistema que se muestran tras una actualización correcta, seleccione la casilla de verificación **No mostrar notificación sobre la actualización correcta**.

Para eliminar todos los datos de actualización almacenados temporalmente, haga clic en el botón **Eliminar** situado junto a **Borrar la caché de actualización**. Utilice esta opción si tiene dificultades para realizar la actualización.

Cómo crear tareas de actualización

Las actualizaciones se pueden activar manualmente al hacer clic en **Actualizar la base de firmas de virus ahora** de la ventana principal que se muestra al hacer clic en **Actualización** en el menú principal.

Las actualizaciones también se pueden ejecutar como tareas programadas. Para configurar una tarea programada, haga clic en **Herramientas** > **Planificador de tareas**. Las siguientes tareas están activadas de forma predeterminada en System Center Endpoint Protection:

- **Actualización automática de rutina**
- **Actualización automática después del registro del usuario**

Todas las tareas de actualización se pueden modificar en función de sus necesidades. Además de las tareas de actualización predeterminadas, se pueden crear nuevas tareas de actualización con una configuración definida por el usuario. Para obtener más información acerca de la creación y la configuración de tareas de actualización, consulte la sección Planificador de tareas 18.

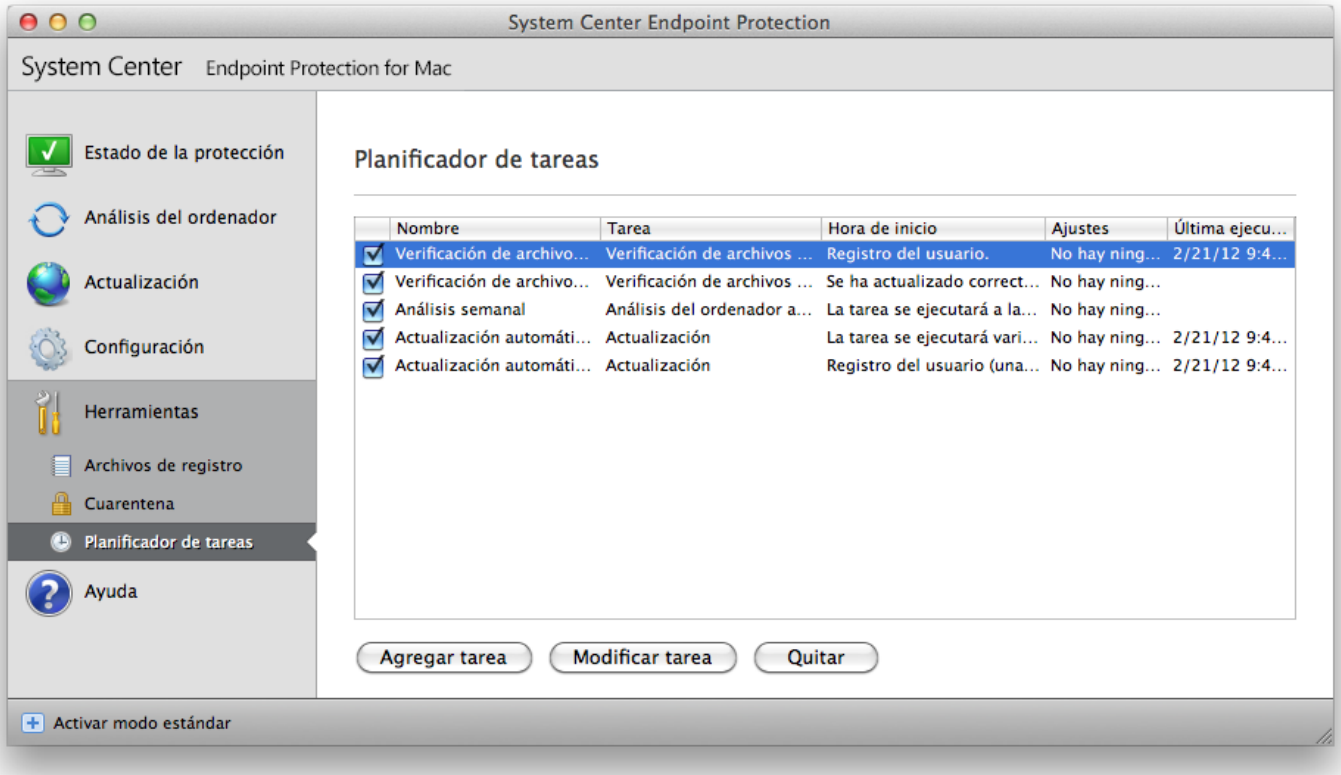
Actualización a una nueva compilación

Utilice la compilación más reciente de System Center Endpoint Protection para disfrutar de la máxima protección posible. Para buscar una versión nueva, haga clic en **Actualizar** en el menú principal de la izquierda. Si está disponible una nueva compilación, se mostrará el mensaje *Está disponible una nueva versión del producto* en la parte inferior de la ventana. Haga clic en **Más información...** para abrir una ventana nueva con el número de versión de la nueva compilación y el registro de cambios.

Haga clic en **Descargar** para descargar la compilación más reciente. Haga clic en **Cerrar** para cerrar la ventana y descargar la actualización en otro momento.

Tareas programadas

El **Planificador de tareas** está disponible si System Center Endpoint Protection tiene activado el 'Modo avanzado'. El 'Planificador de tareas' se puede encontrar en el menú principal de System Center Endpoint Protection, en **Herramientas**. El **Planificador de tareas** contiene una lista de todas las tareas programadas y sus propiedades de configuración, como la fecha, la hora y el perfil de análisis predefinidos que se hayan utilizado.



De forma predeterminada, en el 'Planificador de tareas' se muestran las siguientes tareas programadas:

- Actualización automática de rutina
- Actualización automática después del registro del usuario
- Verificación de archivos en el inicio tras el inicio de sesión del usuario
- Verificación de archivos en el inicio tras actualizar correctamente la base de firmas de virus
- Mantenimiento de registros (después de activar la opción **Mostrar tareas de sistema** en la configuración del planificador de tareas)
- Análisis semanal

Para modificar la configuración de una tarea programada existente (tanto predeterminada como definida por el usuario), pulse Ctrl, haga clic en la tarea que desee modificar y, a continuación, haga clic en **Editar...** o seleccione la tarea y haga clic en el botón **Modificar tarea...**.

Finalidad de la planificación de tareas

El 'Planificador de tareas' administra e inicia las tareas programadas con la configuración y las propiedades predefinidas. La configuración y las propiedades contienen información, como la fecha y la hora, así como los perfiles especificados que se van a utilizar durante la ejecución de la tarea.

Creación de nuevas tareas

Para crear una nueva tarea en el 'Planificador de tareas', haga clic en el botón **Agregar tarea...** o pulse Ctrl, haga clic en el espacio en blanco y seleccione **Agregar...** en el menú contextual. Existen cinco tipos de tareas programadas disponibles:

- **Ejecutar aplicación**
- **Actualización**
- **Mantenimiento de registros**
- **Análisis del ordenador a petición**
- **Verificación de archivos en el inicio del sistema**

Dado que la actualización es una de las tareas programadas más frecuentes, explicaremos cómo se agrega una nueva tarea de actualización.

En el menú desplegable **Tarea programada**, seleccione **Actualización**. Introduzca el nombre de la tarea en el campo **Nombre de la tarea**. Seleccione la frecuencia de la tarea en el menú desplegable **Ejecutar la tarea**. Están disponibles estas opciones: **Definido por el usuario**, **Una vez**, **Reiteradamente**, **Diariamente**, **Semanalmente** y **Cuando se cumpla la condición**. Según la frecuencia seleccionada, se le solicitarán diferentes parámetros de actualización.

Si selecciona **Definido por el usuario**, se le pedirá que especifique la fecha/hora en formato cron (para obtener más detalles, consulte la sección Creación de tareas definidas por el usuario 19).

En el siguiente paso, defina la acción que deba llevarse a cabo si la tarea no se puede realizar o completar a la hora programada. Están disponibles las tres opciones siguientes:

- **Esperar a la próxima hora programada**
- **Ejecutar la tarea lo antes posible**
- **Ejecutar la tarea inmediatamente si el tiempo transcurrido desde la última ejecución supera el intervalo especificado** (el intervalo puede definirse inmediatamente mediante la opción **Intervalo mínimo entre tareas**)

En el paso siguiente, se muestra una ventana de resumen que contiene información acerca de la tarea programada actualmente. Haga clic en el botón **Finalizar**.

La nueva tarea programada se agregará a la lista de tareas programadas actualmente.

De forma predeterminada, el sistema contiene las tareas programadas esenciales para garantizar el correcto funcionamiento del producto. Estas tareas no se deben modificar, por lo que están ocultas de forma predeterminada. Para cambiar esta opción y hacer visibles estas tareas, seleccione **Configuración** > **Introducir preferencias de aplicación...** > **Herramientas** > **Planificador de tareas** y seleccione la opción **Mostrar tareas de sistema**.

Creación de tareas definidas por el usuario

La fecha y la hora de la tarea **Definida por el usuario** se debe introducir en formato cron ampliado por años (una cadena compuesta de 6 campos separados por un espacio en blanco):

```
minuto(0-59) hora(0-23) día del mes(1-31) mes(1-12) año(1970-2099) día de la semana(0-7)(Domingo = 0 o 7)
```

Ejemplo:

```
30 6 22 3 2012 4
```

Caracteres especiales admitidos en las expresiones cron:

- asterisco (`*`): la expresión coincidirá con todos los valores del campo; por ejemplo, un asterisco en el tercer campo (día del mes) significa todos los días
- guión (`-`): define los rangos; por ejemplo, `3-9`
- coma (`,`): separa los elementos de una lista; por ejemplo, `1,3,7,8`
- barra diagonal (`/`): define los incrementos de los rangos; por ejemplo, `3-28/5` en el tercer campo (día del mes) significa tercer día del mes y, luego, cada 5 días.

No se admiten nombres de días (lunes-domingo) ni nombres de meses (enero-diciembre).

NOTA: si define el día del mes y el día de la semana, el comando solo se ejecutará cuando ambos campos coincidan.

Cuarentena

La tarea principal de la cuarentena es almacenar de forma segura los archivos infectados. Los archivos deben ponerse en cuarentena si no es posible desinfectarlos, si no es seguro ni aconsejable eliminarlos o si System Center Endpoint Protection los detecta incorrectamente como infectados.

Puede poner en cuarentena cualquier archivo. Es aconsejable si el comportamiento de un archivo es sospechoso y no lo ha detectado el análisis.

Los archivos almacenados en la carpeta de cuarentena se pueden ver en una tabla que muestra la fecha y la hora en las que se pusieron en cuarentena, la ruta de la ubicación original del archivo infectado, su tamaño en bytes, el motivo (agregado por el usuario, etc.) y el número de amenazas (por ejemplo, si se trata de un archivo que contenga varias amenazas). La carpeta de cuarentena con archivos en cuarentena (*/Library/Application Support/Microsoft/scep/cache/quarantine*) permanece en el sistema aunque System Center Endpoint Protection se desinstale. Los archivos en cuarentena se guardan en un formato cifrado seguro y se pueden restaurar tras la instalación de System Center Endpoint Protection.

Puesta de archivos en cuarentena

System Center Endpoint Protection pone los archivos eliminados en cuarentena automáticamente (si no ha cancelado esta opción en la ventana de alerta). Si lo desea, puede poner en cuarentena cualquier archivo sospechoso de forma manual; para ello, haga clic en el botón **Cuarentena**. El menú contextual también se puede utilizar con este fin: pulse Ctrl, haga clic en el espacio en blanco, seleccione **Cuarentena**, elija el archivo que desee poner en cuarentena y haga clic en el botón **Abrir**.

Restauración de archivos de cuarentena

Los archivos puestos en cuarentena se pueden restaurar a su ubicación original. Utilice el botón **Restaurar** para restaurar dichos archivos. La restauración también está disponible en el menú contextual: pulse Ctrl, haga clic en el archivo en cuestión de la ventana **Cuarentena** y, después, haga clic en **Restaurar**. El menú contextual también ofrece la opción **Restaurar a...**, que le permite restaurar archivos en una ubicación distinta a la original de la cual se eliminaron.

Archivos de registro

Los archivos de registro contienen información relacionada con todos los sucesos importantes del programa y proporcionan información general acerca de las amenazas detectadas. El registro constituye una herramienta esencial en el análisis del sistema, la detección de amenazas y la resolución de problemas. Se lleva a cabo de forma activa en segundo plano, sin necesidad de que intervenga el usuario. La información se registra según la configuración actual del nivel de detalle de los registros. Los mensajes de texto y los registros se pueden ver directamente desde el entorno de System Center Endpoint Protection, donde también se pueden archivar registros.

Puede hacer clic en **Herramientas** > **Archivos de registro** desde el menú principal de System Center Endpoint Protection para, de este modo, acceder a los archivos de registro. Seleccione el tipo de registro que desee en el menú desplegable **Registro**, situado en la parte superior de la ventana. Están disponibles los siguientes registros:

1. **Amenazas detectadas**: utilice esta opción para ver toda la información de los sucesos relacionados con la detección de amenazas.
2. **Sucesos**: esta opción se ha diseñado para que los administradores del sistema y los usuarios puedan solucionar problemas. Todas las acciones importantes que realice System Center Endpoint Protection se registran en los registros de sucesos.
3. **Análisis del ordenador**: en esta ventana se muestran los resultados de todos los análisis completados. Haga doble clic en cualquier entrada para ver los detalles del correspondiente análisis del ordenador a petición.

La información que se muestra en las diferentes secciones se puede copiar directamente en el portapapeles; para ello, seleccione la entrada y haga clic en el botón **Copiar**.

Mantenimiento de registros

Puede acceder a la configuración de registros de System Center Endpoint Protection desde la ventana principal del programa. Haga clic en **Configuración** > **Introducir preferencias de aplicación...** > **Herramientas** > **Archivos de registro**. Puede especificar las siguientes opciones para los archivos de registro:

- **Eliminar los registros antiguos automáticamente**: las entradas de registro anteriores al número de días especificado se eliminarán de forma automática.
- **Optimizar los archivos de registro automáticamente**: los archivos de registro se desfragmentan automáticamente si se supera el porcentaje especificado de registros no utilizados.

Toda la información relevante que se muestra en los mensajes de la interfaz gráfica de usuario, de amenazas y de sucesos se puede almacenar en formato de texto legible, como texto sin formato o CSV (valores separados por comas). Si desea que estos archivos estén disponibles para el procesamiento con herramientas de terceros, seleccione la casilla de verificación situada junto a **Habilitar registro de archivos de texto**.

Para definir la carpeta de destino donde se guardarán los archivos de registro, haga clic en **Configuración** junto a **Configuración avanzada**.

En función de las opciones que seleccione en **Archivos de registro: Editar**: le permite guardar registros con la siguiente información:

- Las amenazas detectadas por Análisis en el inicio, Protección en tiempo real o Análisis del ordenador se guardan en el archivo threatslog.txt.
- Los sucesos como *nombre de usuario y contraseña no válidos* o *no se puede actualizar la base de firmas de virus* se registran en el archivo eventslog.txt.
- Los resultados de todos los análisis completados se guardan en formato scanlog.NÚMERO.txt.

Para configurar los filtros de **Registros predeterminados de análisis del ordenador**, haga clic en el botón **Editar** situado junto a esta opción y seleccione los tipos de registro que desee. Encontrará una explicación más detallada de estos tipos de registro en este capítulo 21.

Filtrado de registros

Registra información acerca de sucesos importantes del sistema. La característica de filtrado de registros permite ver los registros de un tipo específico de suceso.

A continuación se enumeran los tipos de registro más utilizados:

- **Alertas críticas**: errores graves del sistema (por ejemplo, «No se ha podido iniciar la protección del antivirus»).
- **Errores**: mensajes de error, como «*Error al descargar el archivo*», y errores graves.
- **Alertas**: mensajes de alerta.
- **Registros informativos**: mensajes informativos, como los de actualizaciones realizadas con éxito, alertas, etc.
- **Registros de diagnóstico**: información necesaria para ajustar el programa y todos los registros descritos anteriormente.

Interfaz de usuario

Las opciones de configuración de la interfaz de usuario de System Center Endpoint Protection le permiten ajustar el entorno de trabajo según sus necesidades. Se puede acceder a estas opciones de configuración desde **Configuración** > **Introducir preferencias de aplicación...** > **Usuario** > **Interfaz**.

En esta opción, la opción 'Modo avanzado' permite a los usuarios activar dicho modo. Este incluye controles adicionales y opciones de configuración más detalladas para System Center Endpoint Protection.

Para activar la función de pantalla de inicio, seleccione la opción **Mostrar pantalla inicial con la carga del sistema**.

En la sección **Utilizar menú estándar**, puede seleccionar las opciones **En modo estándar/En modo avanzado** para activar el uso del menú estándar en el modo de visualización correspondiente de la ventana principal del programa.

Para activar el uso de las sugerencias, seleccione la opción **Mostrar sugerencias y consejos útiles**. La opción **Mostrar archivos ocultos** le permite ver y seleccionar los archivos ocultos en la configuración de **Objetos de análisis** de un **Análisis del ordenador**.

Alertas y notificaciones

La sección **Alertas y notificaciones** le permite configurar la gestión de las alertas de amenazas y las notificaciones del sistema en System Center Endpoint Protection.

Si desactiva la opción **Mostrar alertas**, se cancelarán todas las ventanas de alertas; esta opción solo es adecuada en situaciones específicas. Para la mayoría de los usuarios, se recomienda mantener la configuración predeterminada (activada).

Si selecciona la opción **Mostrar notificaciones en el escritorio**, las ventanas de alertas que no requieran la interacción del usuario se mostrarán en el escritorio (de forma predeterminada, en la esquina superior derecha de la pantalla). Si desea definir el periodo durante el que se mostrará una notificación, ajuste el valor de **Cerrar automáticamente las notificaciones después de** X **segundos**.

Configuración avanzada de alertas y notificaciones

Mostrar solo notificaciones que requieran la interacción del usuario
Con esta opción, puede activar y desactivar la visualización de mensajes que requieran la intervención del usuario.

Mostrar solo las notificaciones en las que se necesite la intervención del usuario cuando se ejecuten aplicaciones a pantalla completa
Esta opción es útil para hacer presentaciones o realizar otras actividades que requieran la pantalla completa.

Privilegios

La configuración de System Center Endpoint Protection puede ser muy importante para la directiva de seguridad de la empresa. Las modificaciones no autorizadas pueden poner en peligro la estabilidad y la protección del sistema. Por este motivo, es posible seleccionar los usuarios que tendrán permiso para modificar la configuración del programa.

Para especificar los usuarios con privilegios, siga la ruta **Configuración** > **Introducir preferencias de aplicación...** > **Usuario** > **Privilegios**.

Para ofrecer la máxima seguridad para su sistema, es esencial que el programa se haya configurado correctamente. Las modificaciones no autorizadas pueden provocar la pérdida de datos importantes. Para configurar una lista de usuarios con privilegios, selecciónelos en la lista **Usuarios** de la izquierda y haga clic en el botón **Agregar**. Para quitar un usuario, basta con seleccionar su nombre en la lista **Usuarios con privilegios** de la derecha y hacer clic en **Quitar**.

NOTA: Si la lista de usuarios con privilegios está vacía, todos los usuarios del sistema tendrán permiso para modificar la configuración del programa.

Menú contextual

La integración del menú contextual se puede activar en la sección **Configuración** > **Introducir preferencias de aplicación...** > **Usuario** > **Menú contextual** si se activa la casilla de verificación **Integrar en el menú contextual**.

Usuario avanzado

Importar y exportar configuración

La opción de importar y exportar configuraciones de System Center Endpoint Protection está disponible en el modo avanzado de **Configuración**.

Tanto la importación como la exportación utilizan archivos comprimidos para guardar la configuración. La importación y la exportación son útiles para realizar copias de seguridad de la configuración actual de System Center Endpoint Protection y, así, poder utilizarla más adelante. La opción de exportación de configuración también es de utilidad para los usuarios que desean utilizar su configuración preferida de System Center Endpoint Protection en varios sistemas, ya que les permite importar fácilmente el archivo de configuración para transferir los ajustes deseados.

Importar configuración

Importar la configuración es muy fácil. En el menú principal, haga clic en **Configuración** > **Importar y exportar configuración** y, a continuación, seleccione la opción **Importar configuración**. Introduzca el nombre del archivo de configuración o haga clic en el botón **Examinar...** para buscar el archivo de configuración que desee importar.

Exportar configuración

Los pasos para exportar una configuración son muy similares. En el menú principal, haga clic en **Configuración** > **Importar y exportar configuración...**. Seleccione la opción **Exportar configuración** y escriba el nombre del archivo de configuración. Utilice el navegador para seleccionar la ubicación del ordenador donde desee guardar el archivo de configuración.

Configuración del servidor Proxy

La configuración del servidor Proxy se puede establecer en **Varios** > **Servidor Proxy**. Al especificar el servidor Proxy en este nivel, se define la configuración global del servidor Proxy para todas las funciones de System Center Endpoint Protection. Todos los módulos que requieran conexión a Internet utilizarán estos parámetros.

Para especificar la configuración del servidor Proxy en este nivel, seleccione la casilla de verificación **Conexión mediante servidor Proxy** y, a continuación, la dirección IP o la URL del servidor Proxy en el campo **Servidor Proxy**. En el campo de puerto, especifique el puerto donde el servidor Proxy acepte conexiones (el 3128, de forma predeterminada). Si la comunicación con el servidor Proxy requiere autentificación, seleccione la casilla de verificación **El servidor Proxy requiere autentificación** e introduzca un **nombre de usuario** y una **contraseña** válidos en los campos correspondientes.

Bloqueo de medios extraíbles

Las unidades extraíbles (por ejemplo, los CD o las llaves USB) pueden contener código malicioso y poner en peligro su ordenador. Para bloquear las unidades extraíbles, seleccione la casilla de verificación disponible junto a **Activar bloqueo de unidades extraíbles**. Para permitir el acceso a determinados tipos de unidades, anule la selección de las casillas de verificación correspondientes a los tipos de unidades que desea permitir.

Seleccione la casilla de verificación de **Otros** si desea aplicar esta configuración a unidades que no sean CD, DVD, FireWire o USB. En concreto, esta configuración se aplica a cualquier periférico que esté conectado a su ordenador mediante la interfaz Thunderbolt.

Glosario

Tipos de amenazas

Una amenaza es un software malicioso que intenta entrar en el ordenador de un usuario y dañarlo.

Virus

Un virus informático es una amenaza que daña los archivos que haya en el ordenador. Su nombre se debe a los virus biológicos, ya que usan técnicas similares para pasar de un ordenador a otro.

Los virus informáticos atacan sobre todo a archivos ejecutables, scripts y documentos. Para reproducirse, un virus adjunta su «cuerpo» al final de un archivo de destino. En resumen, he aquí cómo funciona un virus informático: después de la ejecución del archivo infectado, el virus se activa (antes de la aplicación original) y realiza la tarea que tenga predefinida. Después, se ejecuta la aplicación original. Un virus no puede infectar un ordenador a menos que un usuario (accidental o deliberadamente) ejecute o abra el programa malicioso.

Los virus informáticos pueden tener diversos fines y niveles de gravedad. Algunos, debido a su capacidad para eliminar archivos del disco duro de forma deliberada, son muy peligrosos. Sin embargo, otros virus no causan daños reales: solo sirven para molestar al usuario y demostrar las capacidades técnicas de sus autores.

Es importante mencionar que los virus (si se comparan con los troyanos o el spyware) son cada vez menos habituales, ya que no son atractivos desde un punto de vista comercial para los autores de software malicioso. Además, el término virus se utiliza incorrectamente con mucha frecuencia para abarcar todo tipo de amenazas. Este término está desapareciendo gradualmente y se está sustituyendo por el término código malicioso, que es más preciso.

Si su ordenador se infecta con un virus, debe restaurar los archivos infectados a su estado original, es decir, desinfectarlos con un programa antivirus.

Ejemplos de virus: *OneHalf*, *Tenga* y *Yankee Doodle*.

Gusanos

Un gusano informático es un programa que contiene código malicioso que ataca a los ordenadores host y se extiende a través de una red. La principal diferencia entre un virus y un gusano es que estos últimos tienen la capacidad de reproducirse y viajar solos: no dependen de archivos host (ni de sectores de inicio). Los gusanos se extienden a través de las direcciones de correo electrónico de la lista de contactos o aprovechan las vulnerabilidades de seguridad de las aplicaciones de red.

Por tanto, los gusanos son mucho más viables que los virus informáticos. Debido a la gran disponibilidad de Internet, se pueden extender por el globo en cuestión de horas desde su lanzamiento y, en algunos casos, incluso en cuestión de minutos. Esta capacidad para reproducirse de forma independiente y rápida los hace más peligrosos que otros tipos de código malicioso.

Un gusano activado en un sistema puede causar una serie de problemas: puede eliminar archivos, degradar el rendimiento del sistema o incluso desactivar algunos programas. Además, su naturaleza le permite servir de «medio de transporte» para otros tipos de amenazas.

Si el ordenador está infectado con un gusano, es recomendable eliminar los archivos infectados, pues podrían contener código malicioso.

Ejemplos de gusanos conocidos: *Lovsan/Blaster*, *Stration/Warezov*, *Bagle* y *Netsky*.

Troyanos

Históricamente, los troyanos informáticos se han definido como una clase de amenaza que intenta presentarse como un programa útil, engañando así a los usuarios para que permitan su ejecución. Hoy en día, los troyanos ya no necesitan ocultarse bajo otra identidad. Su único fin es infiltrarse lo más fácilmente posible y cumplir sus malintencionados objetivos. «Troyano» se ha convertido en un término muy general con el que describir cualquier amenaza que no entre en ninguna clase de amenaza específica.

Dado que se trata de una categoría muy amplia, con frecuencia se divide en muchas subcategorías:

- Descargador: programa malintencionado con capacidad para descargar otras amenazas de Internet.
- Lanzador: tipo de troyano diseñado para lanzar otros tipos de código malicioso en ordenadores vulnerables.
- Puerta trasera: aplicación que se comunica con atacantes remotos y les permite acceder a los sistemas para tomar su control.
- Registrador de pulsaciones: programa que registra todas las teclas pulsadas por el usuario y envía la información a atacantes remotos.

- Marcador: los marcadores son programas diseñados para conectarse con números de tarificación adicional. Es casi imposible que un usuario note que se ha creado una conexión. Los marcadores solo pueden causar daño a los usuarios con módems de marcación, que ya casi no se utilizan.
- Por lo general, los troyanos parecen archivos ejecutables. Si se detecta un troyano en su ordenador, es recomendable que lo elimine, ya que lo más probable es que contenga códigos maliciosos.

Ejemplos de troyanos conocidos: *NetBus*, *Trojandownloader.Small.ZL*, *Slapper*.

Adware

Adware es la forma abreviada de advertising-supported software ('software relacionado con publicidad'). Los programas que muestran material publicitario se incluyen en esta categoría. Por lo general, las aplicaciones de adware abren automáticamente una ventana emergente nueva con anuncios en el navegador de Internet o cambian la página de inicio del mismo. El adware suele instalarse con programas gratuitos, lo que permite que los desarrolladores de esos programas gratuitos cubran los costes de desarrollo de sus aplicaciones (normalmente útiles).

El adware no es peligroso en sí: lo único que molesta a los usuarios es la publicidad. El peligro reside en el hecho de que el adware también puede realizar funciones de seguimiento (como sucede con el spyware).

Si decide utilizar un producto gratuito, preste especial atención al programa de instalación. La mayoría de los instaladores le informarán sobre la instalación de un programa de adware adicional. Por lo general, podrá cancelarlo e instalar el programa sin el adware.

Sin embargo, algunos programas no se instalarán sin el adware o su funcionalidad se verá limitada. Esto significa que el adware puede acceder al sistema de manera «legal» a menudo, pues los usuarios así lo han aceptado. En este caso, es mejor prevenir que curar. Si se detecta un archivo de adware en su ordenador, se recomienda eliminarlo, ya que es muy posible que contenga código malicioso.

Spyware

Esta categoría abarca todas las aplicaciones que envían información privada sin el consentimiento/conocimiento del usuario. El spyware usa funciones de seguimiento para enviar diversos datos estadísticos, como una lista de sitios web visitados, direcciones de correo electrónico de la lista de contactos del usuario o una lista de teclas pulsadas.

Los autores de spyware afirman que el objetivo de estas técnicas es averiguar más sobre las necesidades y los intereses de los usuarios, así como permitir una publicidad mejor gestionada. El problema es que no existe una distinción clara entre aplicaciones útiles y aplicaciones malintencionadas, por lo que nadie puede estar seguro de que la información recuperada se vaya a utilizar correctamente. Los datos que obtienen las aplicaciones spyware pueden contener códigos de seguridad, códigos PIN, números de cuentas bancarias, etc. Con frecuencia, el spyware se instala junto con versiones gratuitas de programas con los que el autor pretende generar ingresos u ofrecer un incentivo para que se compre el software. A menudo, se informa a los usuarios acerca de la presencia de spyware durante la instalación de un programa con el fin de ofrecerles un incentivo para la adquisición de una versión de pago que no contenga dicha aplicación.

Algunos ejemplos de productos gratuitos conocidos que se instalan junto con spyware son las aplicaciones de redes P2P (peer to peer). Spyfalcon o Spy Sheriff (y muchos más) pertenecen a una subcategoría específica de spyware: parecen programas antispyware, pero en realidad son aplicaciones spyware.

Si se detecta un archivo de spyware en su ordenador, se recomienda eliminarlo, ya que es muy posible que contenga código malicioso.

Aplicaciones potencialmente peligrosas

Existen muchos programas legítimos que sirven para simplificar la administración de ordenadores en red. Sin embargo, si caen en las manos equivocadas podrían utilizarse con fines maliciosos. System Center Endpoint Protection proporciona la opción de detectar estas amenazas.

«Aplicaciones potencialmente peligrosas» es la clasificación que se utiliza para el software comercial legítimo. Esta clasificación incluye programas como herramientas de acceso remoto, aplicaciones para detectar contraseñas y registradores de pulsaciones (programas que graban todas las teclas pulsadas por un usuario).

Si detecta la presencia de una aplicación potencialmente peligrosa que esté en ejecución en su ordenador (y no la ha instalado usted), consulte con el administrador de la red o elimine la aplicación.

Aplicaciones potencialmente indeseables

Las aplicaciones potencialmente indeseables no tienen por qué ser maliciosas, pero pueden afectar al rendimiento del ordenador de forma negativa. Dichas aplicaciones suelen necesitar que se consienta su instalación. Si se encuentran en su ordenador, el sistema se comportará de manera diferente (en comparación con el comportamiento previo a la instalación). Los cambios más importantes son:

- Se abren ventanas nuevas que no se habían visto anteriormente
- Se activan y ejecutan procesos ocultos
- Se produce un mayor uso de los recursos del sistema
- Hay cambios en los resultados de búsqueda
- La aplicación se comunica con servidores remotos.