Ayuda de Symantec™ Endpoint Protection para el cliente de Mac - Spanish - Spain

December 2020

De qué manera Symantec Endpoint Protection protege su Mac

Symantec Endpoint Protection combina varias capas de protección para resguardar al equipo de los ataques de virus y spyware, así como de intentos de intrusión.

Tipos de protección describe cada capa de protección.

Table 1: Tipos de protección

Protección	Descripción
Protección antivirus y antispyware	Symantec Endpoint Protection incluye análisis de virus programados, análisis a petición y Auto-Protect, que se ejecuta en segundo plano y supervisa la aparición de virus. Cuando se encuentra un virus, Symantec Endpoint Protection lo elimina. De qué manera la protección antivirus y antispyware protege su Mac
Protección contra amenazas de red	Symantec Endpoint Protection intercepta los datos en la capa de red. Usa firmas para analizar los paquetes o las secuencias de paquetes. Analiza cada paquete individualmente buscando los modelos que corresponden a los ataques de la red o del navegador. La protección contra amenazas de red incluye lo siguiente: • La prevención de intrusiones, que detecta ataques en los componentes del sistema operativo y la capa de aplicación. Cuando Symantec Endpoint Protection detecta una amenaza de red, la bloquea. • El firewall, que permite o bloquea el tráfico de red en función de las políticas y reglas del firewall. (A partir de la versión 14.2.) De qué manera la protección contra amenazas de red protege su Mac
Control de dispositivos	Los administradores de Symantec Endpoint Protection Manager configuran una política de control de dispositivos. Los dispositivos pueden ser bloqueados o desbloqueados con esta política por el nombre de dispositivo, el proveedor de dispositivo, el modelo de dispositivo o el número de serie. En un cliente administrado, se puede ver la configuración del control de dispositivos en la ficha **Avanzado**. El control de dispositivos no está disponible para los clientes no administrados. Acerca del control de dispositivos en el cliente de Symantec Endpoint Protection para Mac
Detección y respuesta de endpoints de	Los administradores de Symantec Endpoint Protection Manager configuran una política de registrador de actividad que proporciona los medios para detectar y exponer actividades sospechosas en la red.

El cliente descarga automáticamente las definiciones de virus, las definiciones IPS y las actualizaciones del producto a su equipo.

Actualización de las definiciones de virus, las definiciones de prevención de intrusiones y el software de cliente

De qué manera la protección antivirus y antispyware protege su Mac

Symantec Endpoint Protection usa definiciones de virus para detectar los virus conocidos durante los análisis programados y los análisis manuales. Auto-Protect usa definiciones de virus para analizar constantemente la actividad del equipo.

Symantec Endpoint Protection notifica que ha detectado un virus u otro riesgo para la seguridad. Un virus u otro riesgo para la seguridad se detecta cuando una de las siguientes situaciones se presenta:

- Auto-Protect encuentra un virus mientras supervisa el equipo.
- Auto-Protect encuentra un virus a partir de un análisis programado o iniciado manualmente.

Con la configuración predeterminada, Symantec Endpoint Protection intenta automáticamente reparar todos los virus que encuentra. Si no puede reparar el archivo; el cliente lo pone en cuarentena de forma segura, de modo que no pueda dañar el equipo. Generalmente, el cliente realiza estas reparaciones sin que usted realice ninguna otra acción. Cuando el equipo encuentra un virus, es posible optar por enviar información sobre él a Symantec.

En algunas circunstancias, el cliente le solicita elegir si desea reparar, eliminar o restaurar un archivo infectado que se encontró. Sus respuestas determinan qué medidas debe tomar el cliente sobre el archivo infectado.

Respuesta de mensajes acerca de detecciones de infecciones y riesgos

Activación o desactivación del envío de información de seguridad a Symantec

De qué manera la protección contra amenazas de red protege su Mac

La protección contra amenazas de red incluye las siguientes tecnologías de protección:

- Prevención de intrusiones
- Firewall

Prevención de intrusiones

La prevención de intrusiones detecta y bloquea automáticamente los ataques de red. La prevención de intrusiones es una capa interna de defensa que protege a los equipos cliente. La prevención de intrusiones a veces se llama sistema de prevención de intrusiones (IPS).

La prevención de intrusiones intercepta datos en la capa de red. Usa firmas para analizar los paquetes o las secuencias de paquetes. Analiza cada paquete individualmente buscando los modelos que corresponden a los ataques de la red o del navegador. La prevención de intrusiones detecta ataques en los componentes del sistema operativo y la capa de aplicación.

La prevención de intrusiones usa firmas para identificar ataques en los equipos cliente. Para los ataques conocidos, la prevención de intrusiones desecha automáticamente los paquetes que coinciden con las firmas.

Firewall

El firewall supervisa el tráfico de red y bloquea el tráfico potencialmente dañino para proteger su Mac. El firewall de Symantec Endpoint Protection no está disponible en el cliente no administrado.

El firewall de Symantec Endpoint Protection supervisa el tráfico en la capa de transporte e Internet. El firewall integrado de Mac supervisa el tráfico en la capa de aplicación superior después de que lo supervisa el firewall de Symantec Endpoint Protection. Por lo tanto, puede habilitar ambos firewalls a la vez para que se ejecuten en paralelo.

El firewall usa los siguientes tipos de reglas para permitir o bloquear el tráfico de red.

- Reglas predeterminadas
- Reglas personalizadas
- Reglas integradas
- Reglas de protección

Estas reglas incluyen la detección de análisis de puertos, la detección de denegación de servicio, protección contra la falsificación de dirección MAC, DHCP inteligente y DNS inteligente. La configuración del firewall está bajo el control total del administrador de Symantec Endpoint Protection Manager. Puede habilitar o deshabilitar el firewall solamente si el administrador permite el control de clientes del usuario mediante el equipo Mac.

Se ha agregado la protección mediante firewall en la versión 14.2.

Administración de la prevención de intrusiones

Administración de la protección mediante firewall para el cliente de Mac

Compatibilidad del sistema operativo con Symantec Endpoint Protection para Mac

Symantec Endpoint Protection para Mac es compatible con las siguientes versiones del sistema operativo:

- macOS 12
- macOS 11 (tanto el procesador Intel como el chip M1)
- macOS de la versión 10.15 a la versión 10.15.7

Para obtener más información sobre la compatibilidad con las versiones anteriores del sistema operativo Mac, consulte Compatibilidad de Mac con el cliente de Endpoint Protection.

Acerca de la autorización de extensiones del sistema de Symantec Endpoint Protection para macOS 10.15 o posterior

Notas de la versión, nuevas correcciones y requisitos del sistema para todas las versiones de Endpoint Protection

Cómo instalar el cliente de Symantec Endpoint Protection para Mac

Es posible instalar directamente un cliente de Symantec Endpoint Protection en un equipo Mac si no se puede (o no se desea) usar la transferencia remota. Los pasos son similares si es un cliente administrado o no administrado.

La única forma de instalar un cliente administrado es con un paquete que se crea en Symantec Endpoint Protection Manager. Es posible convertir un cliente no administrado en un cliente administrado en cualquier momento importando la configuración de comunicación entre el cliente y el servidor en el cliente de Mac.

NOTE

Para preparar el cliente de Symantec Endpoint Protection para Mac para utilizarlo con software de implementación remota de otro fabricante, consulte:

Exportación e implementación de un cliente de Symantec Endpoint Protection mediante Apple Remote Desktop o Casper.

Table 2: Métodos para instalar el cliente de Mac

Si se ha descargado el archivo de instalación.	1. Extraiga el contenido en una carpeta de un equipo Mac y, a continuación, abra la carpeta. 2. Abra `SEP_MAC`. 3. Copie `Symantec Endpoint Protection.dmg` en el escritorio del equipo Mac. 4. Haga doble clic en `Symantec Endpoint Protection.dmg` para montar el archivo como disco virtual. A continuación, instale el cliente de Symantec Endpoint Protection para Mac.
Si dispone de un paquete de instalación de clientes .zip en el Portal de soporte de Broadcom. Para obtener más información, consulte: Portal de soporte de Broadcom	1. Copie el archivo en el escritorio del equipo Mac. El archivo se puede llamar `Symantec Endpoint Protection.zip` o `Symantec_Endpoint_Protection_versión_Mac_Client.zip`, donde versión es la versión del producto. 2. Haga clic con el botón derecho en **Abrir con > Utilidad de archivado** para extraer el contenido del archivo. 3. Abra la carpeta resultante. A continuación, instale el cliente de Symantec Endpoint Protection for Mac.

La imagen o la carpeta resultante del disco virtual contiene el instalador de la aplicación y una carpeta llamada Recursos adicionales. Ambos elementos deben estar presentes en la misma ubicación para una instalación correcta. Si copia el instalador a otra ubicación, se debe además copiar Recursos adicionales.

Para instalar el cliente de Symantec Endpoint Protection para Mac:

1. Haga doble clic en `Instalador de Symantec Endpoint Protection`.
2. Para comenzar la instalación, haga clic en **Instalar**.
3. Para instalar una herramienta auxiliar que se necesita para instalar el cliente de Symantec Endpoint Protection, introduzca el nombre de usuario y la contraseña administrativos de Mac y, a continuación, haga clic en **Instalar herramienta auxiliar**.
4. Después de la instalación, haga clic en **Continuar** para finalizar la configuración del cliente de Symantec Endpoint Protection.
5. Para configurar el cliente de Symantec Endpoint Protection, realice los siguientes pasos:

Autorice la extensión del sistema Symantec Endpoint Protection.	En el cuadro de diálogo **Seguridad y privacidad**, en la ficha **General**, en **Se impidió la carga del software del sistema desde la aplicación Symantec Endpoint Protection**, haga clic en **Permitir**. Si es necesario, haga clic en el icono de bloqueo para realizar los cambios. Es necesario autorizar la extensión del sistema para obtener la funcionalidad completa de Symantec Endpoint Protection. Consulte: Acerca de la autorización de extensiones del sistema de Symantec Endpoint Protection para macOS 10.15 o posterior
Permita el acceso al disco completo.	En el cuadro de diálogo **Seguridad y privacidad**, en la ficha **Privacidad**, asegúrese de que **Extensión del sistema de Symantec** tiene permiso para acceder a los datos y a la configuración administrativa de todos los usuarios en su dispositivo Mac. Si es necesario, haga clic en el icono de bloqueo para realizar los cambios.
Permita cambios en el perfil de red.	Cuando se le solicite **Symantec Endpoint Protection quiere filtrar contenido de redes**, haga clic en **Permitir**.

6. Haga clic en **Completar**.

Acerca de la autorización de extensiones del sistema de Symantec Endpoint Protection para macOS 10.15 o posterior

El requisito de la autorización de las extensiones del sistema es una función de seguridad de macOS 10.15.Es necesario autorizar la extensión del sistema para obtener la funcionalidad completa de Symantec Endpoint Protection.

Para autorizar la extensión del sistema de Symantec Endpoint Protection, durante la configuración del cliente de Symantec Endpoint Protection, en el cuadro de diálogo **Seguridad y privacidad**, en la ficha **General**, en **Se impidió la carga del software del sistema de la aplicación Symantec Endpoint Protection**, haga clic en **Permitir**.

Para obtener más información, consulte:

Instalación del cliente de Symantec Endpoint Protection para Mac

Indicación de la actualización para el cliente de Symantec Endpoint Protection para Mac

Los administradores de Symantec Endpoint Protection Manager pueden asignar un paquete de instalación del cliente para actualizar de forma automática los equipos cliente administrados, con la configuración de instalación del cliente.

Si ha iniciado sesión en Mac, se puede ver una indicación para reiniciar para completar la instalación. Es posible poder retrasar el reinicio según la configuración de la instalación del cliente.

Si no ha iniciado sesión con Mac, la instalación reinicia de forma automática el equipo Mac.

Guía de inicio sobre el cliente de Symantec Endpoint Protection

Al abrir el cliente de Symantec Endpoint Protection, el mensaje **You are Protected** (Está protegido) aparece en la parte superior de la página, a menos que haya un problema que deba resolverse. Haga clic en **Reparar** para resolver cualquier problema.

El cliente de Symantec Endpoint Protection muestra las tareas principales que se pueden realizar.

Table 3: Páginas del cliente de Symantec Endpoint Protection

Opción	Descripción
Seguridad	Muestra el estado de protección del equipo.
Análisis	Permite analizar el equipo. Es posible optar por ejecutar un análisis rápido o un análisis completo. También puede analizar un archivo o carpeta. Ejecución de un análisis manual
LiveUpdate	Ejecuta LiveUpdate para actualizar los archivos de definiciones y del producto para Symantec Endpoint Protection. Actualización inmediata del contenido de Symantec Endpoint Protection
Avanzada	Ofrece más opciones detalladas para las funciones Protección antivirus y antispyware, Protección contra amenazas de red y LiveUpdate.

Administración de la protección de su Mac con Symantec Endpoint Protection

La configuración predeterminada de Symantec Endpoint Protection protege su Mac contra muchos tipos de software malicioso. El cliente controla de forma automática el software malicioso o le permite elegir cómo controlar el software malicioso.

Según la configuración que establece el administrador, es necesario realizar las siguientes tareas para ayudar a mantener la protección.

NOTE
Es posible que el administrador no le haya concedido el control de estas tareas.

Table 4: Protección del equipo

Pasos	Descripción
Paso 1: Comprobar que las opciones Protección antivirus y antispyware, y Protección contra amenazas de red estén habilitadas.	Aparece la página **Seguridad** y muestra una marca de comprobación verde y el mensaje **You are protected** (Está protegido), si las protecciones están activadas. Activación y desactivación de la protección antivirus y antispyware Activación o desactivación de la protección contra amenazas de red
Paso 2: Asegurarse de que el software y las definiciones estén actualizados.	La página **Seguridad** muestra la última hora en la que se actualizaron las definiciones para las funciones Protección antivirus y antispyware, y Protección contra amenazas de red. En **LiveUpdate**, aparece la hora de la última actualización del producto. Para ver el número de versión del software, haga clic en **Ayuda > Acerca de**.
Paso 3: Actualizar el software o las definiciones, si es necesario.	En el cliente de Symantec Endpoint Protection, haga clic en **LiveUpdate** para actualizar el software y las definiciones de inmediato. Actualización de las definiciones de virus, las definiciones de prevención de intrusiones y el software de cliente

Pasos	Descripción
Paso 4: Ejecutar un análisis.	Es posible programar análisis para que se ejecuten regularmente o bien, ejecutar un análisis de inmediato. Configuración de análisis programados Ejecución de un análisis manual

Administración de la configuración de protección antivirus y antispyware

Renovación de la licencia del producto

Es posible ver un mensaje en el icono del cliente de Symantec Endpoint Protection en la barra de menú que indica que la licencia para Symantec Endpoint Protection caducó. El cliente de Symantec Endpoint Protection utiliza una licencia para actualizar lo siguiente:

- El software de cliente
- Los archivos de definiciones de protección para los análisis de virus y spyware, así como la prevención de intrusiones

El cliente puede usar una licencia de prueba o una licencia paga. Si alguna licencia ha caduca, el cliente no actualiza ninguna definición ni el software de cliente.

Para cualquier tipo de licencia, es necesario ponerse en contacto con el administrador para actualizar o renovar la licencia.

Respuesta de mensajes acerca de detecciones de infecciones y riesgos

Habilitación o deshabilitación del control de dispositivos en el cliente de Symantec Endpoint Protection para Mac

Los administradores de Symantec Endpoint Protection Manager pueden configurar los clientes administrados con una política de control de dispositivos. Los dispositivos pueden ser bloqueados o desbloqueados con esta política por el nombre de dispositivo, el proveedor de dispositivo, el modelo de dispositivo o el número de serie.

Puede ver las actividades del control de dispositivos en la página **Avanzado** haciendo clic en **Actividad > Historial de seguridad**.

La configuración en el cliente de Symantec Endpoint Protection para **Control de dispositivos** le deja habilitar o deshabilitar el control de dispositivos. Si se habilita el control de dispositivos, se pueden habilitar o deshabilitar opcionalmente las notificaciones cuando los dispositivos son bloqueados o desbloqueados.

Para cambiar la configuración, es necesario autenticarse con las credenciales del administrador de Mac. Si esta configuración aparece en color gris, el administrador la ha bloqueado para evitar que usted habilite o deshabilite esta función.

No es posible añadir o editar los dispositivos para ser bloqueados o desbloqueados a través de la interfaz del cliente de Symantec Endpoint Protection.

NOTE
La política de control de dispositivos de Symantec Endpoint Protection Manager controla la configuración del control de dispositivos. En el latido siguiente, cualquier cambio que se realice a esta configuración se revierte a lo que dicta la política.

El control de dispositivos no está disponible para los clientes no administrados.

Acerca de Protección de acceso web y en la nube para el cliente de Mac

Protección de acceso web y en la nube automatiza la redirección de tráfico web a Symantec Web Security Service y protege el tráfico web en cada equipo que usa Symantec Endpoint Protection.

El administrador controla la configuración que usa Protección de acceso web y en la nube, que incluye la dirección URL de la configuración de proxy y el certificado raíz opcional de Symantec Web Security Service. Solo el administrador de Symantec Endpoint Protection Manager puede configurar esta opción, que no aparece en la IU del cliente de Symantec Endpoint Protection. Puede ver la URL del archivo de configuración de proxy en el equipo Mac en **Preferencias del sistema > Red**, en **Servidores proxy**. El certificado de servicios en la nube aparece en **Cadena de llaves**.

Los navegadores web Safari, Chrome y Firefox versión 65 y versiones posteriores admiten Protección de acceso web y en la nube. Las versiones anteriores a 14.2 RU1 de Symantec Endpoint Protection solo son compatibles con Safari y Chrome.

NOTE
El método de túnel no se ejecuta en los clientes Mac.

Desinstalación del cliente de Symantec Endpoint Protection for Mac

Desinstale el cliente de Symantec Endpoint Protection para Mac a través del icono de cliente en la barra de menú. La desinstalación del cliente de Symantec Endpoint Protection para Mac requiere credenciales de usuario administrativo.

NOTE
Después de desinstalar el cliente de Symantec Endpoint Protection, se le pedirá reiniciar el equipo cliente para completar la desinstalación. Asegúrese de guardar cualquier trabajo no finalizado o de cerrar todas las aplicaciones abiertas antes de comenzar.

Para desinstalar el cliente de Symantec Endpoint Protection para Mac

1. En el equipo cliente Mac, abra al cliente Symantec Endpoint Protection y a continuación, haga clic en **Symantec Endpoint Protection > Desinstalar Symantec Endpoint Protection**.
2. Haga clic en **Desinstalar** de nuevo para comenzar la desinstalación.
3. Para instalar una herramienta auxiliar que se necesita para instalar el cliente de Symantec Endpoint Protection, introduzca el nombre de usuario y la contraseña administrativos de Mac y, a continuación, haga clic en **Instalar herramienta auxiliar**.
4. En el cuadro de diálogo de la **Symantec Endpoint Protection está intentando modificar una extensión del sistema**, especifique el nombre de usuario y la contraseña administrativos de Mac y, a continuación, haga clic en **Aceptar**.

   Es posible que también se le pida que escriba una contraseña para desinstalar el cliente. Esta contraseña puede ser una contraseña diferente que la contraseña administrativa de su Mac.
5. Una vez que la desinstalación se complete, haga clic en **Reiniciar ahora**.

Si la desinstalación falla, puede tener que usar otro método para desinstalar. Consulte:

Desinstalación de Symantec Endpoint Protection

Actualización de las definiciones de virus, las definiciones de prevención de intrusiones y el software de cliente

Los productos de Symantec dependen de la información actual para proteger su equipo contra amenazas descubiertas recientemente. Symantec pone esta información a disposición de Symantec Endpoint Protection mediante LiveUpdate. LiveUpdate descarga actualizaciones del producto y de definiciones para el equipo mediante la conexión a Internet.

Las actualizaciones de definiciones son los archivos que mantienen actualizados sus productos de Symantec con las últimas tecnologías de protección contra amenazas. LiveUpdate recupera las nuevas firmas de prevención de intrusiones o los archivos de definiciones de virus de un sitio de Internet de Symantec y reemplaza los archivos anteriores.

Las actualizaciones del producto son mejoras al cliente instalado. Las actualizaciones del producto se crean generalmente para ampliar la compatibilidad del sistema operativo o del hardware, para ajustar los problemas de rendimiento o para reparar errores del producto. Las actualizaciones del producto aparecen cuando son necesarias. El cliente recibe actualizaciones del producto directamente de un servidor de LiveUpdate. Las actualizaciones del producto y de definiciones se denominan, en conjunto, actualizaciones de contenido.

Table 5: Maneras de actualizar el contenido en su equipo

Tarea	Descripción
Actualizar el contenido de forma inmediata	Se puede ejecutar LiveUpdate de forma inmediata. Actualización inmediata del contenido de Symantec Endpoint Protection
Actualizar el contenido según una programación	De forma predeterminada, LiveUpdate se ejecuta automáticamente en los intervalos programados. Actualización del contenido de Symantec Endpoint Protection según una programación

Administración de la protección de su Mac con Symantec Endpoint Protection

Actualización inmediata del contenido de Symantec Endpoint Protection

Es posible actualizar los archivos de definiciones y del producto de forma inmediata con LiveUpdate. Es necesario ejecutar LiveUpdate manualmente por los siguientes motivos:

- El software de cliente fue instalado recientemente.
- Ha transcurrido mucho tiempo desde el último análisis.
- Sospecha que el equipo tiene un problema de virus u otro software malicioso.

Para actualizar el contenido de Symantec Endpoint Protection de forma inmediata:

Inicie LiveUpdate de una de las formas siguientes:

- Haga clic con el botón secundario en el icono Symantec Endpoint Protection que se encuentra en la barra de menús y, a continuación, haga clic en **LiveUpdate**.
- Abra el cliente de Symantec Endpoint Protection y, a continuación, haga clic en **LiveUpdate**.

LiveUpdate se conecta con el servidor de LiveUpdate configurado, comprueba si hay actualizaciones disponibles y las descarga e instala automáticamente. Una barra de estado indica el progreso de la descarga.

Actualización del contenido de Symantec Endpoint Protection según una programación

Actualización de las definiciones de virus, las definiciones de prevención de intrusiones y el software de cliente

Actualización del contenido de Symantec Endpoint Protection según una programación

Programaciones en clientes de Mac administrados

De forma predeterminada, los clientes de Mac administrados reciben una programación de Symantec Endpoint Protection Manager que ejecuta LiveUpdate cada cuatro horas. El administrador de Symantec Endpoint Protection Manager controla la programación. Los clientes administrados no pueden eliminar, modificar o ver la programación creada por el administrador o crear una nueva programación.

Programaciones en clientes de Mac no administrados

Es posible crear una programación de modo que LiveUpdate se ejecute automáticamente en intervalos programados. Es conveniente programar la ejecución de LiveUpdate cuando no se use el equipo.

Para actualizar el contenido de Symantec Endpoint Protection según una programación:

1. En el cliente de Symantec Endpoint Protection, en la página **Avanzados**, haga clic en **Configuración** y, a continuación, haga clic en el icono de configuración de **LiveUpdate programado**.

   Aparece la programación actual.

2. Seleccione un intervalo del menú desplegable Programación de LiveUpdate.

   La configuración inicial indica que se debe ejecutar cada **4** horas. También es posible seleccionar las opciones de ejecución **Diaria** o **Semanal** y elegir una hora o un día y una hora, respectivamente.

3. Haga clic en **Aplicar cambios**.

Actualización inmediata del contenido de Symantec Endpoint Protection

Actualización de las definiciones de virus, las definiciones de prevención de intrusiones y el software de cliente

Acerca de cómo establecer la conexión con el servidor de administración mediante un servidor proxy

Es posible que se le solicite permitir que Symantec Endpoint Protection use sus credenciales para conectarse con el servidor de administración mediante un servidor proxy. Recibirá un mensaje donde se le preguntará si desea permitir el acceso a las credenciales al proceso `symdaemon`.

En el mensaje, es necesario hacer clic en **Permitir siempre**. De lo contrario, continuará recibiendo el mismo mensaje cada vez que el cliente se comunique con el servidor de LiveUpdate. Si hace clic en **Denegar**, el cliente no podrá recibir actualizaciones para el software ni las definiciones.

Actualización de las definiciones de virus, las definiciones de prevención de intrusiones y el software de cliente

Administración de la configuración de protección antivirus y antispyware

De forma predeterminada, Symantec Endpoint Protection brinda protección contra virus y riesgos para la seguridad, que incluye las amenazas de red, a partir de que se inicia el equipo. La protección antivirus y antispyware incluye Auto-Protect, que comprueba si existen virus en los programas a medida que se ejecutan. Además, supervisa el equipo en busca de cualquier actividad que pueda indicar la presencia de un virus o un riesgo para la seguridad. La intercepción de Auto-Protect impide que los virus infecten el equipo; por eso, es necesario mantenerlo activado.

Para los clientes administrados, la cantidad de control que tiene sobre esta configuración depende de cómo el administrador configuró el cliente. Además, cualquier cambio que realice a esta configuración puede revertir lo que dicta la política en el siguiente latido.

Administración de la protección antivirus y antispyware describe las tareas que se pueden realizar para administrar la protección antivirus y antispyware en su Mac.

Table 6: Administración de la protección antivirus y antispyware

Pasos	Descripción
Paso 1: Activar o desactivar la protección antivirus y antispyware	Es posible habilitar y deshabilitar fácilmente la protección antivirus y antispyware. Symantec recomienda dejarla activada. Activación y desactivación de la protección antivirus y antispyware
Paso 2: Personalizar la configuración de Auto-Protect	Auto-Protect es una pieza importante de la protección antivirus y antispyware. Es posible configurar estas opciones desde la página **Avanzado**. Cómo establecer la configuración de Auto-Protect y la zona de análisis
Paso 3: Analizar el equipo en busca de virus	Es posible configurar análisis de virus para que se ejecuten de forma programada o de inmediato. Configuración de análisis programados Cómo pausar, posponer y detener los análisis Ejecución de un análisis manual
Paso 4: Responder cuando Symantec Endpoint Protection detecta un virus	Cuando Symantec Endpoint Protection analiza el equipo, puede: • Notificar las acciones que se pueden llevar a cabo. • Informar sobre las acciones de protección que se han tomado. Respuesta de mensajes acerca de detecciones de infecciones y riesgos

Activación y desactivación de la protección antivirus y antispyware

De forma predeterminada, la protección antivirus y antispyware está activada junto con Auto-Protect.

Es posible ejercer un control más preciso sobre Auto-Protect mediante la configuración de opciones específicas.

Si la protección antivirus y antispyware está desactivada, aparece una "x" roja en la página **Estado**, con el mensaje **La protección contra virus y spyware está deshabilitada**. Si se deshabilitó la protección, es necesario habilitarla tan pronto como sea posible.

NOTE
Los análisis programados continúan, independientemente de que la protección antivirus y antispyware esté habilitada o deshabilitada. Es posible que el administrador restrinja el acceso a algunas opciones de configuración de Symantec Endpoint Protection. Es posible que no tenga permitido deshabilitar esta configuración, programar análisis ni personalizar opciones de protección.Es posible que se solicite proporcionar la contraseña del administrador de Mac para modificar algunas de estas opciones de configuración.

Para activar y desactivar la protección antivirus y antispyware:

1. Para activar la protección antivirus y antispyware, en el cliente Symantec Endpoint Protection, en la página **Avanzados**, haga clic en **Protect My Mac** (Proteger mi Mac) y, a continuación, habilite **Automatic Scans** (Análisis automáticos).
2. Para desactivar la protección antivirus y antispyware, en el cliente Symantec Endpoint Protection, en la página **Avanzados**, haga clic en **Protect My Mac** (Proteger mi Mac) y, a continuación, deshabilite **Automatic Scans** (Análisis automáticos).

Cómo establecer la configuración de Auto-Protect y la zona de análisis

Administración de la configuración de protección antivirus y antispyware

Respuesta de mensajes acerca de detecciones de infecciones y riesgos

Cómo establecer la configuración de Auto-Protect y la zona de análisis

En los clientes administrados, si el administrador lo permite, se puede personalizar la forma en que Auto-Protect supervisa los virus y repara los archivos infectados.

La configuración de Auto-Protect aparece como opciones en **Protect My Mac** (Proteger mi Mac). Debe activar **Automatic Scans** (Análisis automáticos) para habilitar Auto-Protect.

La **Configuración de zona de análisis** permite especificar los archivos que se deben incluir en un análisis o que se deben excluir de él.

Para establecer la configuración de Auto-Protect:

1. En el cliente de Symantec Endpoint Protection, en la página **Avanzados**, haga clic en **Protect My Mac** (Proteger mi Mac) y, a continuación, haga clic en el icono de configuración de **Automatic Scans** (Análisis automáticos).
2. Realice cambios en cualquiera de las siguientes opciones:

Poner en cuarentena automáticamente	Es posible elegir si enviar o no a la cuarentena cualquier archivo que no se pueda reparar.
Reparar automáticamente	Es posible elegir que Auto-Protect automáticamente repare cualquier archivo infectado que encuentre.
Analizar	Se puede seleccionar **Discos de datos** y **Todos los demás discos**.
Analizar archivos comprimidos	Es posible elegir que se incluyan los archivos comprimidos en un análisis de Auto-Protect. El análisis incluye el archivo comprimido y los archivos dentro del archivo comprimido.

WARNING
Si no elige **Reparar automáticamente**, no se envía ningún archivo infectado a la cuarentena, aunque se elija **Poner en cuarentena automáticamente**. El software pregunta si desea reparar un archivo infectado. Si no repara el archivo, este queda en el equipo. Si elige **Reparar automáticamente** y no elige **Poner en cuarentena automáticamente**, no se elimina ningún archivo infectado.

3. Haga clic en **Listo**.

Para establecer la configuración de zona de análisis:

1. En el cliente de Symantec Endpoint Protection, en la página **Avanzados**, haga clic en **Protect My Mac** (Proteger mi Mac) y, a continuación, haga clic en el icono de configuración de **Configuración de zona de análisis**.
2. Realice cambios en cualquiera de las siguientes opciones:

Analizar todo	Se analizan todos los archivos y procesos del equipo a medida que se accede a ellos.
Solo analizar	Se incluyen en el análisis solo los archivos o las carpetas que se especifican.

No analizar	Se analizan todos los archivos, excepto los archivos o las carpetas que específicamente se deben excluir del análisis.
Usar valores predeterminados	Mediante esta opción, se analiza todo.

3. Haga clic en **Aceptar**.

De qué manera la protección antivirus y antispyware protege su Mac

Activación y desactivación de la protección antivirus y antispyware

Administración de archivos en cuarentena

Configuración de análisis programados

Symantec Endpoint Protection ejecuta automáticamente un análisis predeterminado si tiene un cliente administrado. Si el administrador lo permite, es posible configurar análisis programados adicionales.

En un cliente no administrado, es necesario ejecutar análisis propios.Symantec recomienda realizar un análisis manual completo tan pronto como sea posible y, luego, configurar un análisis programado regularmente. Es posible pausar o demorar cualquier análisis, incluidos los análisis programados y manuales.

En un cliente administrado, el análisis predeterminado se ejecuta diariamente a las 08:00 p. m., con la opción Reparar automáticamente habilitada.

NOTE
Symantec no recomienda ejecutar un análisis programado más de una vez al día. Al aumentar la frecuencia de los análisis o configurar varios análisis programados se pueden causar problemas de rendimiento.

Ejecución de un análisis manual

Para configurar análisis programados:

1. En el cliente de Symantec Endpoint Protection, en la página **Avanzados**, haga clic en **Protect My Mac** (Proteger mi Mac) y, a continuación, haga clic en el icono de configuración de **Scheduled Scans** (Análisis programados).
2. En el cuadro de diálogo, haga clic en **Agregar análisis programados** o haga clic en un análisis programado actual y después haga clic en **Editar** para ajustar la configuración.
3. En la ficha **Elementos de análisis**, es posible configurar las siguientes opciones:

Unidades	Es posible decidir si se desea analizar **Discos duros** y **Unidades extraíbles**.
Carpetas	Es posible optar por analizar los archivos de **Carpeta particular** (usuario activo), **Aplicaciones** y **Biblioteca**. Si ningún usuario inició sesión en el momento del análisis programado de una carpeta de inicio, el análisis no se ejecuta.
Opciones de análisis	Es posible elegir entre las siguientes opciones: • **Análisis comprimido** • **Reparar automáticamente** • **Poner en cuarentena automáticamente** • **Habilitar análisis durante inactividad**

4. En la ficha **Programación del análisis**, es posible configurar las siguientes opciones:

Programación del análisis	Es posible configurar un análisis para ejecutar en un intervalo específico en horas, diariamente, semanalmente o mensualmente. **Ejecutar según intervalo específico** se selecciona de forma predeterminada al programar un nuevo análisis.
Ejecutar cada	Disponible cuando se selecciona la opción **Ejecutar en un intervalo específico** para la **Programación del análisis**.
Hora de inicio	Disponible cuando se selecciona **Diaria**, **Semanal** o **Mensual** para la programación del análisis. Es posible elegir la hora del día a la que se debe ejecutar el análisis. Se debe elegir una hora que no forme parte del horario habitual de trabajo, ya que los análisis pueden lentificar el rendimiento del equipo.
Activado	Disponible cuando se selecciona **Semanal** o **Mensual** para la programación del análisis. Es posible elegir el día de la semana o el mes en el que se debe ejecutar el análisis. Recomendamos que elija una hora que no forme parte del horario habitual de trabajo, ya que los análisis pueden lentificar el rendimiento del equipo.

5. En la ficha **Afinación**, puede ajustar el modo en que se optimiza el rendimiento del análisis.
6. Haga clic en **Aceptar**.
7. Haga clic en **Listo**.

Cómo pausar, posponer y detener los análisis

Administración de la protección de su Mac con Symantec Endpoint Protection

Respuesta de mensajes acerca de detecciones de infecciones y riesgos

Activación o desactivación del envío de información de seguridad a Symantec

Ejecución de un análisis manual

Es posible que sea necesario analizar manualmente algunos archivos. Por ejemplo, es posible que sea necesario analizar los archivos que se guardaron en el equipo antes de instalar Symantec Endpoint Protection. O bien, es posible decidir analizar algunos archivos que hayan sido excluidos de un análisis programado.

NOTE
Es posible pausar o demorar cualquier análisis, incluidos los análisis programados y manuales.

Para ejecutar un análisis manual:

En el cliente de Symantec Endpoint Protection, en la página **Análisis**, realice una de las siguientes acciones:

- Para iniciar un análisis rápido, haga clic en **Quick Scan** (Análisis rápido) y, a continuación, haga clic en **Start a Quick Scan** (Iniciar un análisis rápido).
- Para iniciar un análisis completo, haga clic en **Full Scan** (Análisis completo) y, a continuación, haga clic en **Start a Full Scan** (Iniciar un análisis completo).
- Para analizar un archivo o una carpeta, haga clic en **File Scan** (Análisis de archivos) y, a continuación, haga clic en **Selecciona un archivo**.Se abre el buscador y es posible optar por **Mostrar archivos ocultos** y **Analizar archivos comprimidos**. También es posible optar por habilitar **Reparar automáticamente** y **Poner en cuarentena automáticamente**.

Cómo pausar, posponer y detener los análisis

Configuración de análisis programados

Activación o desactivación del envío de información de seguridad a Symantec

Cómo pausar, posponer y detener los análisis

La función de pausa permite detener un análisis y reanudarlo en otro momento que elija. También es posible detener y cancelar un análisis en cualquier momento. No es necesario tener privilegios de administrador para usar estas funciones.

Cuando que un análisis se reanuda, se inicia desde donde se detuvo.

> **NOTE**
> Si interrumpe momentáneamente un análisis al mismo tiempo que el cliente analiza un archivo comprimido, el cliente puede tardar varios minutos para responder a la solicitud de interrupción.

Si se habilita la posposición, se puede también posponer un análisis, pero solamente antes de que el análisis comience. No es posible posponer un análisis en curso.

Para pausar o detener un análisis programado en ejecución:

1. En el cuadro de diálogo de progreso del análisis, haga clic en **Pausar**.
2. En el cuadro de diálogo de progreso del análisis, haga clic en **Reanudar** para continuar con el análisis o haga clic en **Detener** para detenerlo. Es posible también hacer clic en **Finalizado** para cerrar la ventana.

Para pausar o detener un análisis manual:

1. En el cuadro de diálogo de progreso del análisis, haga clic en **Pausar** para pausar el análisis.
2. Haga clic en **Cancelar** para detener un análisis manual en ejecución o haga clic en **Reanudar** para continuar el análisis.

Para posponer un análisis que está a punto de comenzar:

1. En la ventana que aparece, haga clic en el menú desplegable para seleccionar un valor para posponer. Es posible posponer por tan poco como 15 minutos o por un día.
2. Haga clic en **Aceptar** para posponer el análisis.

   No debe realizar ninguna acción si desea que el análisis se ejecute como estaba previsto.

Configuración de análisis programados

Ejecución de un análisis manual

Respuesta de mensajes acerca de detecciones de infecciones y riesgos

Es posible comprobar si el equipo está infectado y realizar algunas tareas adicionales si desea más seguridad o mayor rendimiento.

El administrador puede administrar el cliente o se puede ejecutar un cliente no administrado. Las tareas de protección que es posible realizar dependen de qué tanto control ejerza el administrador sobre el cliente.

Si Symantec Endpoint Protection encuentra un virus o un riesgo para la seguridad, es posible que le soliciten realizar alguna acción respecto del riesgo. Según la configuración que elija su administrador, es posible que le informen la acción que el cliente realizó automáticamente.

Table 7: Respuesta de mensajes acerca de infecciones

Contenido del mensaje	Acción requerida
Se reparó el archivo infectado	Ninguno
Solicita su aprobación para reparar el archivo infectado	Apruebe la reparación. Esta opción depende de las preferencias de Auto-Protect. Administración de la configuración de protección antivirus y antispyware Si la opción para reparar automáticamente los archivos infectados no está seleccionada, es necesario reparar el archivo de forma manual. Reparación de archivos infectados
No es posible reparar el archivo infectado	Administre la infección en Cuarentena. Administración de archivos en cuarentena

De qué manera la protección antivirus y antispyware protege su Mac

Reparación de archivos infectados

Si no se repara ni se coloca en cuarentena automáticamente un archivo infectado, es posible reparar el archivo desde la lista de resultados del análisis. Es posible reparar manualmente los archivos del disco duro del equipo o de una unidad extraíble.

Para reparar archivos infectados:

1. En la lista de resultados del análisis, seleccione el archivo que desea reparar y, luego, haga clic en **Reparar**.

   También es posible hacer clic con el botón derecho en cualquier archivo del menú **Finder** o **Buscar** de Mac.
2. Repita estos pasos, según sea necesario.
3. Ejecute otro análisis para buscar otros archivos infectados.
4. Compruebe los archivos reparados para asegurarse de que funcionen correctamente.

Administración de la configuración de protección antivirus y antispyware

Administración de archivos en cuarentena

Administrar los archivos en cuarentena

De forma predeterminada, si el cliente detecta un virus en un archivo, intenta eliminar el virus. Si no es posible eliminar el virus, el archivo se coloca en la cuarentena del equipo. Si Symantec Endpoint Protection detecta un riesgo para la seguridad en un archivo, primero, coloca el archivo en la cuarentena. Luego, repara los efectos secundarios del riesgo.

Cuando se actualizan las definiciones de virus, el cliente comprueba automáticamente la cuarentena. Es posible volver a analizar los elementos de la cuarentena. Es posible que las definiciones más recientes puedan limpiar o reparar los archivos que están en cuarentena.

Para administrar archivos en cuarentena:

1. En el cliente de Symantec Endpoint Protection, en la página **Avanzado**, haga clic en **Actividad > Historial de seguridad > Cuarentena**.
2. Seleccione el archivo que desea administrar y, luego, elija la opción correspondiente:

Reparar	Elija esta opción para tratar de reparar un archivo en cuarentena. Asegúrese de que las definiciones de virus sean más recientes que la fecha en la cual el archivo se puso en cuarentena.
Eliminar	Elija esta opción para eliminar de la cuarentena los archivos que ya no sean necesarios.

Restaurar	Si es seguro que el archivo no contiene un virus, es posible restaurarlo en la ubicación original del equipo. Esta opción no analiza el archivo ni intenta repararlo.

Respuesta de mensajes acerca de detecciones de infecciones y riesgos

Activación o desactivación del envío de información de seguridad a Symantec

Symantec Endpoint Protection puede enviar información seudonimizada sobre las amenazas detectadas a Symantec. Symantec usa esta información para proteger a los equipos cliente contra amenazas nuevas, dirigidas y mutantes. Cualquier dato que se envía mejora la capacidad de Symantec de responder las amenazas y de personalizar la protección para su equipo.

Los datos que recopila de telemetría de Symantec pueden incluir elementos seudónimos que no son directamente identificables. Symantec no necesita ni pretende utilizar los datos de telemetría para identificar a ningún usuario individual.

De forma predeterminada, el equipo cliente envía la información sobre detecciones a Symantec. Es posible desactivar los envíos, aunque Symantec recomienda dejar activada esta configuración.

Esta opción solo envía información sobre las detecciones de virus.

NOTE
Symantec recomienda dejar esta opción activada.

Para activar o desactivar el envío de información seudonimizada de seguridad a Symantec:

En el cliente de Symantec Endpoint Protection, en la página **Avanzados**, haga clic en **Product Settings** (Configuración del producto) y, a continuación, active o desactive **Security Info Submission** (Envío de información de seguridad).

Configuración de análisis programados

Ejecución de un análisis manual

Administrar la prevención de intrusiones

La configuración predeterminada para la prevención de intrusiones protege al cliente de Mac. Sin embargo, si desea administrar su propia protección, es posible administrar la prevención de intrusiones como parte de la protección contra amenazas de red.

Table 8: Administrar la prevención de intrusiones

Pasos	Descripción
Paso 1: Aprender sobre la prevención de intrusiones.	Aprenda cómo la prevención de intrusiones detecta y bloquea ataques de red. De qué manera la protección contra amenazas de red protege su Mac
Paso 2: Descargar las firmas IPS más actuales.	De forma predeterminada, las firmas más actuales se descargan al cliente. Sin embargo, es posible que desee descargar las firmas de forma inmediata. Actualización inmediata del contenido de Symantec Endpoint Protection
Paso 3: Habilitar o deshabilitar la prevención de intrusiones.	Es posible que sea necesario deshabilitar la prevención de intrusiones para solucionar problemas o si los equipos cliente detectan una cantidad excesiva de falsos positivos. Generalmente, no debería deshabilitar la prevención de intrusiones. Activación o desactivación de la protección contra amenazas de red
Paso 4: Habilitar las notificaciones de prevención de intrusiones.	Es posible configurar notificaciones para que aparezcan cuando Symantec Endpoint Protection detecta un ataque. Activación o desactivación de las notificaciones de protección contra amenazas de red

Administración de la protección mediante firewall para el cliente de Mac

El firewall de Symantec Endpoint Protection para Mac ofrece una protección mediante firewall que se integra completamente con Symantec Endpoint Protection, que incluye eventos, políticas y comandos. El firewall de Symantec Endpoint Protection solo está disponible en clientes administrados.

NOTE
El firewall de Symantec Endpoint Protection for Mac no se integra con el firewall integrado del sistema operativo. En cambio, se ejecuta en paralelo. El firewall de sistema operativo inspecciona en la capa de aplicación, mientras que el firewall de Symantec Endpoint Protection inspecciona en niveles más bajos (IP y transporte).El firewall de Symantec Endpoint Protection para Mac no ofrece reglas de bloqueo de punto a punto, aunque se pueden crear estas reglas en parte mediante reglas de firewall personalizadas.

Table 9: Administrar la protección mediante firewall

Pasos	Descripción
Paso 1: Obtenga más información sobre la protección mediante firewall	Sepa cómo la protección mediante firewall supervisa el tráfico y protege contra vectores de ataque comunes. De qué manera la protección contra amenazas de red protege su Mac
Paso 2: Habilitar o deshabilitar el firewall.	Es posible que deba deshabilitar el firewall para solucionar problemas, por ejemplo, si se bloquea el tráfico que espera que sea admitido. Normalmente, no es necesario deshabilitar el firewall. Activación o desactivación de la protección contra amenazas de red

Activación o desactivación de la protección contra amenazas de red

Típicamente, cuando desactiva los componentes de la protección contra amenazas de red en su equipo, este es menos seguro. Sin embargo, es posible que desee desactivar la prevención de intrusiones para evitar falsos positivos o que desee desactivar el firewall para solucionar problemas de tráfico bloqueado. La prevención de intrusiones y el firewall son parte de la protección contra amenazas de red.

Para los clientes administrados, la cantidad de control que tiene sobre esta configuración depende de cómo el administrador configuró el cliente. Además, cualquier cambio que realice a esta configuración puede revertir lo que dicta la política en el siguiente latido.

Para los clientes no administrados, el firewall no está disponible.

Para activar o desactivar la protección contra amenazas de red:

1. En el cliente de Symantec Endpoint Protection, en la página **Avanzados**, haga clic en **Protección contra amenazas de red**.
2. Para habilitar o deshabilitar la prevención de intrusiones, haga clic en **Prevención de intrusiones**.
3. Para habilitar o deshabilitar el firewall, active o desactive el **Firewall**.
4. Para habilitar o deshabilitar las notificaciones de prevención de intrusiones y firewall, haga clic en el icono de configuración de **Protección contra vulnerabilidades** y, a continuación, en el cuadro de diálogo, seleccione o anule la selección de **Mostrar notificaciones de protección contra vulnerabilidades**.
5. Haga clic en **Listo**.

Si desactiva estos componentes, debe activarlos nuevamente tan pronto como sea posible para asegurarse de que su equipo tenga la mejor protección.

Administración de la prevención de intrusiones

Administración de la protección mediante firewall para el cliente de Mac


Symantec
A Division of Broadcom