Notas de la versión de Symantec™ Endpoint Protection 14.3 RU3 - Spanish - Spain

Updated: September 17, 2021

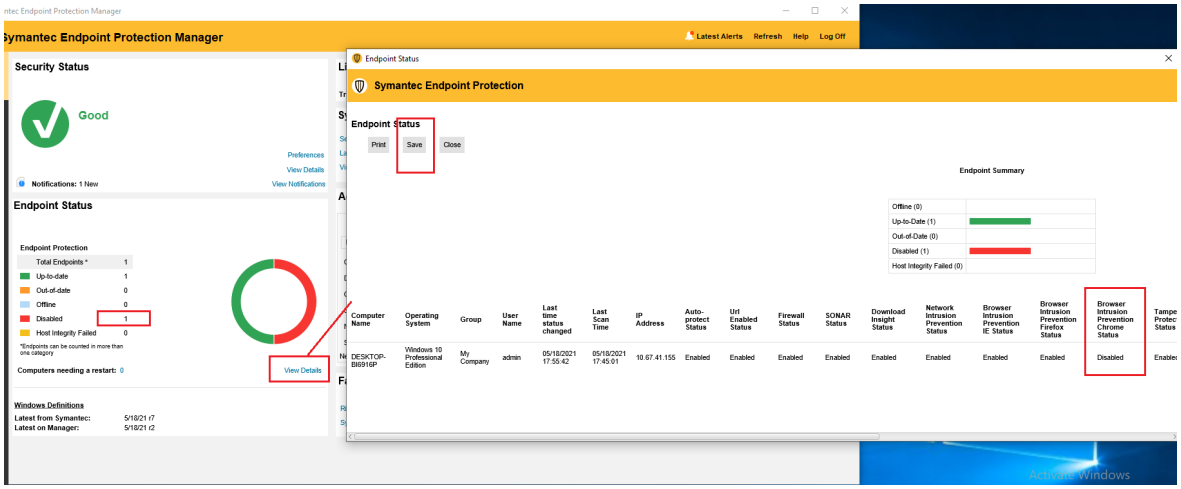
Table of Contents

Novedades en Symantec Endpoint Protection 14.3 RU3

En esta sección se describen las nuevas funciones de esta versión.

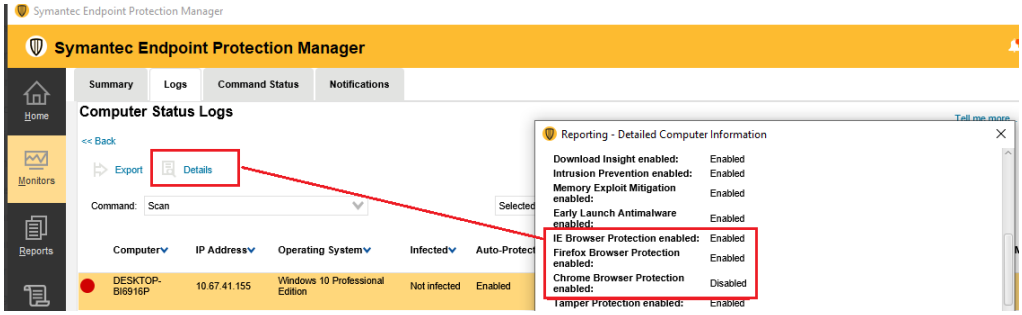
Funciones de protección

- Protección mejorada contra herramientas "living off the land". Para obtener más información, consulte: Cómo Symantec Endpoint Protection protege contra las amenazas de ransomware y las tácticas "living off the land"
- Protección mejorada contra amenazas conocidas de ransomware, como REvil, con tecnologías de inspección expandida para amenazas emergentes. Se detecta el comportamiento sospechoso común a ataques dirigidos y se bloquean los archivos y los procesos antes de que se ejecute el cifrado.
- Protección mejorada contra amenazas en Linux usando el aprendizaje automático y el análisis en la nube. Para aprovechar esta funcionalidad, en la **Política de protección antivirus y antispyware**, haga clic en **Configuración de Linux** > **Opciones de análisis global**.
- Symantec ahora puede liberar de forma más rápida nuevas funciones de detección con Auto-Protect.
- Generación de informes mejorada de la extensión del navegador para identificar los equipos con la protección deshabilitada o con contenido sin actualizar en Symantec Endpoint Protection Manager:
  - La página **Clientes** > ficha **Clientes** > vista **Tecnología de protección** muestra si las extensiones del navegador están habilitadas o deshabilitadas.Seleccione el cliente y haga clic en **Editar propiedades** > ficha **Clientes**. Los campos **Estado habilitado del navegador IE**, **Estado habilitado del navegador FF** y **Estado habilitado del navegador Chrome** muestran el estado **Habilitado**, **Deshabilitado** o **No se informa**. Las **Definiciones de extensiones del navegador** muestran el número de versión de las definiciones.
  - En la página **Inicio**, en **Estado del endpoint**, seleccione los clientes que tienen el estado **Deshabilitado** y haga clic en **Detalles**. En el informe, consulte las extensiones del navegador que están habilitadas o deshabilitadas.



  - Generación de informes mejorada de los clientes con la extensión del navegador deshabilitada. En la página **Inicio**, en **Informes favoritos**, el informe **Estado semanal de Symantec Endpoint Protection** muestra qué clientes tienen las extensiones que están habilitadas o deshabilitadas.
  - El informe rápido **Versiones de contenido de protección** muestra cuándo se han actualizado por última vez las definiciones de la extensión del navegador Chrome. Haga clic en **Informes** > **Informes rápidos** > tipo de informe **Estado del equipo** > informe **Versiones de contenido de protección** y, a continuación, haga clic en **Crear informe**. Haga clic en el informe **Resumen del estado de seguridad** para ver cuántos clientes tienen las extensiones del navegador deshabilitadas o con mal funcionamiento.
  - El registro Estado del equipo muestra las columnas **Protección del navegador IE habilitada**, **Protección del navegador Firefox habilitada** y **Protección del navegador Chrome habilitada**. En la página **Supervisión**,

haga clic en **Registros** > registro **Estado del equipo** > **Ver registro**. En la ficha **Registros**, haga clic en **Detalles** para ver el número de revisión para **Definiciones de extensiones del navegador**. Utilice esta información para asegurarse de que el contenido de la extensión del navegador se descargue al cliente.



– El registro del sistema del cliente muestra un evento cada vez que la extensión del navegador Chrome se habilita, se deshabilita, se instala, se desinstala o se elimina.

Integración de extensiones del navegador con Symantec Endpoint Protection para proteger contra sitios web maliciosos

Actualizaciones de Symantec Endpoint Protection Manager

- Symantec Endpoint Protection Manager ahora es compatible con Windows Server 2022.
- Mayor flexibilidad sobre las actualizaciones del cliente de Windows usando la política de actualización del cliente con la configuración del reconocimiento de ubicación. La política también permite que la actualización se produzca cualquier día de la semana, que se distribuya en varios días y que se vuelva a intentar si no se ha iniciado según lo programado.

  Actualización del software de cliente con la política de actualización del cliente

  Descarga del contenido de LiveUpdate a Symantec Endpoint Protection Manager
- Si el cliente detecta que tiene contenido que no está actualizado, los clientes de Windows proporcionan protección continua comprobando la presencia de actualizaciones en un intervalo regular. Si faltan las definiciones, el cliente registra un evento una vez cada 30 minutos. Los clientes de una versión heredada intentan realizar la reparación un número configurado de veces antes de detenerse al final del día y registrar un error.Se controla esta configuración con la Política de protección antivirus y antispyware > **Varios** > ficha **Notificaciones** > opción **Intentos de reparación antes de que aparezca una advertencia en Symantec Endpoint Protection**.
- Se han actualizado o agregado los siguientes componentes de otros fabricantes: AjaxSwing, Apache HTTP Server, libcurl, libxml2, OpenJDK, OpenSSL y PHP.

Actualizaciones del cliente y de la plataforma

Cliente de Windows:

- El cliente de Windows se admite en Windows Server 2022 y Windows 10 Embedded.La versión 14.3 RU3 se ha probado y es compatible con todas las versiones previas al lanzamiento de Windows 11 y Windows 11 Embeded.
- Si un dominio de Symantec Endpoint Protection Manager está inscrito en la nube, aparece una página de solución de problemas con los nombres de las políticas que administra la consola en la nube. Para acceder a esta página, haga clic en **Ayuda** > **Solución de problemas** > **Administración híbrida**.
- **Registro de depuración**: Cuando se habilita el archivo `debug.log` del cliente en el panel **Ayuda** > **Solución de problemas** > **Debug Logs** (Registros de depuración), también se habilita el archivo `cve.log` .No es necesario reiniciar el cliente ni ejecutar los comandos siguientes para que los cambios realizados en el registro de depuración surtan efecto: `smc -stop` o `smc -start` .Los registros de depuración del cliente ayudan a solucionar problemas de comunicación de cliente a Symantec Endpoint Protection Manager y problemas de funcionalidad del cliente. Se encuentran los registros de comunicación (`cve.log` y `cve-actions.log`) en **C:\ProgramData\Symantec \Symantec Endpoint Protection\CurrentVersion\Data\Logs**.

Opciones avanzadas del registro de depuración en SymDiag para clientes de Endpoint Protection
Configuración del registro del módulo de comunicación de Endpoint Protection en la versión 14.2 y versiones posteriores

Cliente de Mac:

NOTE
El lanzamiento del cliente de Symantec Endpoint Protection para Mac 14.3 RU3 está planificado para octubre de 2021.

- Compatibilidad agregada para macOS 12.
- El tamaño del instalador del cliente de Mac se ha reducido a 100 MB.
- El número de alarmas **En riesgo** se ha reducido y optimizado.
- Para mejorar el rendimiento, ya no pueden ejecutarse varios análisis simultáneamente. Si un análisis está en ejecución, los otros análisis se pondrán en cola.
- A partir de la versión 14.3 RU3, el instalador del cliente de Mac no permite instalar una versión anterior del cliente.

Agente de Linux:

- La herramienta de línea de comandos del Agente de Linux (sav) se ha mejorado con opciones para mostrar versiones, ejecutar LiveUpdate, e iniciar y detener un análisis.Para obtener más información, consulte:
  Administración del Agente de Linux usando la herramienta de línea de comandos (sav)
- Linux ahora admite TCP para los equipos administrados por SEPM.
- Correcciones de defectos.
- Se ha eliminado la advertencia para la opción **Usar los servidores de Symantec cuando los servidores privados no están disponibles** en la página **Clientes** > ficha **Clientes** > **Comunicaciones externas**. Ya no se admiten clientes de la versión 12.1.5.

Cambios en la documentación

- Las API de Symantec Endpoint Protection Manager están en un archivo PDF en la siguiente ubicación:
  ENDPOINT SECURITY REST API DOCUMENTATION

Para obtener más información, consulte:

Novedades en todas las versiones de Symantec Endpoint Protection

Problemas conocidos y soluciones alternativas para Symantec Endpoint Protection (SEP)

Los problemas en esta sección se aplican a esta versión de Symantec Endpoint Protection.

NOTE

La columna Incidencia muestra el número de versión cuando aparece la incidencia. Por ejemplo, [14.3 RU1] significa que el problema se aplica a la versión 14.3 RU1 y versiones posteriores.Cuando se corrigen estos problemas, aparecen en las notas de correcciones. Consulte:

Versiones, requisitos del sistema, fechas de versión, notas y correcciones para Symantec Endpoint Protection y Endpoint Security

Problemas de actualización

Table 1: Problemas conocidos de la actualización

Problema	Descripción y solución
El siguiente mensaje de error aparece: "Symantec Endpoint Protection versión 14.3 RU2 para Win64bit es el paquete más reciente. No se puede eliminar." [14.3 RU2]	No se puede eliminar el paquete de instalación de clientes cuando los paquetes de varias compilaciones aparecen en Symantec Endpoint Protection Manager. A partir de la versión 14.3 RU2, LiveUpdate puede descargar varios paquetes de instalación de clientes con un número de compilación diferente, que aparecen en la página **Administrador** > **Paquetes de instalación** > **Paquete de instalación de clientes**. [SEP-72531]
Se produce un error en la actualización automática si se usa la opción **Upgrade to English if currently installed language is unsupported** (Actualizar a inglés si el idioma instalado actualmente no es compatible) de la versión 14.3 RU2 para actualizar clientes con un idioma no admitido a inglés. [14.3 RU2]	Este problema ocurre para los clientes que se actualizaron manualmente de un idioma admitido a un idioma no admitido en la versión 14.3 RU1 MP1 y versiones anteriores como, por ejemplo, al actualizar un cliente checo a un cliente japonés en un sistema operativo japonés. A continuación, se usa la opción **Upgrade to English if currently installed language is unsupported** (Actualizar a inglés si el idioma instalado actualmente no es compatible) para actualizar el idioma no admitido al inglés en la versión 14.3 RU2. [SEP-72490] Este problema se produce porque el idioma del cliente usa el idioma del sistema operativo admitido (en este caso, japonés). La actualización automática espera usar el idioma admitido y no el inglés. Para solucionar este problema, intente realizar la actualización automática de nuevo y desactive la opción **Upgrade to English if currently installed language is unsupported** (Actualizar a inglés si el idioma instalado actualmente no es compatible).
Al exportar un paquete de instalación de clientes de Symantec Endpoint Protection Manager (SEPM) 14.3 RU2, aparece el siguiente mensaje de advertencia: "El paquete de instalación del cliente no tiene contenido". [14.3 RU2]	Este problema se produce cuando se interrumpe la comunicación entre Symantec Endpoint Protection Manager y la consola que se usa para exportar el paquete.Consulte: Aviso "El paquete de instalación del cliente no tiene contenido" al exportar un paquete de instalación desde Endpoint Protection Manager
Aparece un error al importar los paquetes de instalación de clientes más recientes en una versión anterior de Symantec Endpoint Protection Manager. [14.3 RU2]	Los clientes de Symantec Endpoint Protection 14.3 RU2 no pueden administrarse desde la versión 14.3 RU1 MP1 o anterior de Symantec Endpoint Protection Manager. [SEP-72292]

Problema	Descripción y solución
Después de actualizar Symantec Endpoint Protection Manager a la versión 14.3 RU2, php-cgi.exe se bloquea con un error en el visor de eventos [14.3 RU2]	Este problema ocurre con la versión 17.4.1.1 de Microsoft ODBC Driver para SQL Server. [SEP-70385] Para solucionar este problema de forma temporal, descargue e instale la versión 17.7.2 de Microsoft ODBC Driver para SQL Server en Windows: https://docs.microsoft.com/en-us/sql/connect/odbc/windows/release-notes-odbc-sql-server-windows?view=sql-server-ver15 Para obtener más información, consulte: php-cgi.exe crash occurs on Endpoint Protection Manager after upgrading to 14.3 RU2
Después de actualizar a Symantec Endpoint Protection Manager 14.3 RU2, es posible que aparezcan las notificaciones de "Se ha cambiado el nombre del equipo cliente" [14.3 RU2]	Después de actualizar desde una versión anterior de Symantec Endpoint Protection Manager a la versión 14.3 RU2, es posible que los administradores empiecen a recibir las notificaciones de "Se ha cambiado el nombre del equipo cliente". Este problema solo se aplica a los clientes Mac.Consulte: "The client computer has been renamed" notifications may appear after upgrading to Symantec Endpoint Protection Manager 14.3 RU2
Una instancia de Symantec Endpoint Protection Manager en una red oscura descarga el contenido antiguo del Sistema de detección de intrusiones de clientes (CIDS) a los nuevos clientes porque LiveUpdate no se ejecuta durante una actualización [14.3 RU1]	Cuando una instancia de Symantec Endpoint Protection Manager 14.3 RU1 no puede acceder a Internet o a un servidor del administrador de LiveUpdate (LUA), mantiene el contenido antiguo e incompatible en la memoria caché. Este contenido antiguo normalmente se entrega a los nuevos clientes.Para actualizar el contenido en la memoria caché del servidor de administración, descargue manualmente las definiciones de virus certificadas y los archivos .jdb de CIDS. [SEP-69125] Para asegurarse de que los nuevos clientes no obtengan contenido antiguo, instale manualmente un archivo .jdb de CIDS en SEPM antes de instalar nuevos clientes o de actualizar los clientes anteriores.Consulte: Descarga de los archivos .jdb para actualizar las definiciones de Endpoint Protection Manager
No se puede iniciar sesión en Symantec Endpoint Protection Manager (SEPM) cuando la tarjeta de interfaz de red está deshabilitada [14.3 RU1]	Si después de instalar Symantec Endpoint Protection Manager, no se puede iniciar sesión en la consola y aparece el siguiente mensaje de error: `Error inesperado del servidor` Este problema puede ocurrir si la tarjeta de interfaz de red del equipo estaba deshabilitada cuando se instaló SEPM, lo que impide que el certificado del servidor se genere. [SEP-67040] Para descubrir si SEPM se ha instalado con una tarjeta de interfaz de red deshabilitada, mire el certificado del servidor.Consulte: Error inesperado del servidor en el inicio de sesión de SEPM si se ha instalado en un servidor sin una NIC habilitada
Cuando se desinstala SEPM y se usa la opción para eliminar la base de datos predeterminada y dejar la instancia de SQL Server Express, aparece el siguiente error: "`Se ha producido un error al intentar conectarse al servidor de la base de datos` " [14.3 RU1]	Si desinstala Symantec Endpoint Protection Manager y selecciona la opción **Eliminar solo la base de datos y dejar la instancia de SQL Server Express instalada con SEPM**, es posible que vea el siguiente error: `Se produjo un error al intentar establecer la conexión con servidor de bases de datos` .Este problema ocurre después de agregar las credenciales para el administrador de base de datos del usuario predeterminado y puede estar relacionado con los privilegios de usuario. [SEP-68670] Para solucionar este problema, realice la desinstalación ejecutando el archivo setup.exe de SEPM y haciendo clic en **Eliminar solo la base de datos y dejar la instancia de SQL Server Express instalada con SEPM** durante la desinstalación.

Problema	Descripción y solución
Se produce un error en la actualización de SQL Server de la versión 2017 a la versión 2019 con el modo FIPS habilitado [14.3]	Puede que vea el error: "Se ha producido el error siguiente. Se ha producido un error al instalar la función de extensibilidad con el mensaje de error: Error al crear AppContainer con mensaje de error NINGUNO, estado. Esta implementación no forma parte de los algoritmos criptográficos validados por FIPS de la plataforma de Windows." Esto ocurre si se dispone de una instancia de Symantec Endpoint Protection Manager 14.3 habilitada con FIPS y se actualiza desde Microsoft SQL Server 2017 a 2019.[SEP-61473] Para solucionar este problema, deshabilite FIPS a nivel del sistema operativo: 1. En `C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Administrative Tools`, haga clic en **Directiva de seguridad local** > **Directivas locales** > **Opciones de seguridad** y deshabilite **Criptografía de sistema: usar algoritmos que cumplan FIPS para cifrado, firma y operaciones hash** 2. Actualice desde SQL Server versión 2017 a la versión 2019. 3. Después de actualizar SQL Server correctamente, vuelva a habilitar FIPS. Para obtener más información, consulte: Se produce un error al actualizar SQL de la versión 2017 a la versión 2019 con el modo FIPS habilitado
Los nombres personalizados pueden impedir que la política de firewall se actualice durante una actualización a 14.2 o una versión posterior	Para realizar una actualización a Symantec Endpoint Protection 14.2 o posterior, las políticas de firewall no pueden incorporar los cambios para IPv6 si se cambiaron algunos nombres predeterminados. Los nombres predeterminados incluyen los nombres de las políticas predeterminadas y nombres de reglas predeterminadas. Si las reglas no pueden actualizarse durante la actualización, las opciones de IPv6 no aparecen. No se verá afectada ninguna política o regla nueva que cree después de la actualización. Si es posible, revierta cualquier nombre modificado al nombre predeterminado. De lo contrario, asegúrese de que las reglas personalizadas que agregó a una política predeterminada no bloqueen la comunicación IPv6 de ninguna manera. Asegúrese de lo mismo para cualquier política o regla nueva que agregue.

Problemas de Symantec Endpoint Protection Manager

Table 2: Problemas conocidos de Symantec Endpoint Protection Manager

Problema	Descripción y solución
Endpoint Protection (SEP) 14.2 RU1 MP1 y los clientes anteriores no respetan la configuración de la **Programación de actualización** en una política de actualización del cliente [14.3 RU3]	Para obtener más información, consulte: Endpoint Protection 14.3 RU1 MP1 and older clients not following Client Upgrade Policy [SEP-72814]
Algunos eventos de EDR no aparecen en el cliente [14.3 RU1]	El cliente de Symantec Endpoint Protection debe ejecutar Windows 10 (compilación 14393 o posterior) para recopilar eventos de Symantec EDR Event Tracing para Windows (ETW). [SEP-67175]

Problema	Descripción y solución
La función Redirección de tráfico de red (Protección de acceso web y en la nube) tiene algunas limitaciones [14.3 RU1]	• Symantec Web Security Service se incluye en IPv4 y no en IPv6. [SEP-68700] • El método de redireccionamiento del túnel: – Solo se ejecuta en Windows 10 x64 versión 1703 y posteriores (canal de mantenimiento semestral). Este método no es compatible con otros sistemas operativos de Windows ni con el cliente de Mac. [SEP-67927] – No es compatible con los dispositivos Windows 10 de 64 bits compatibles con HVCI. [SEP-67648] – Redirige el tráfico saliente desde el cliente Symantec Endpoint Protection hasta el WSS antes de que lo evalúe el firewall del cliente o las reglas de reputación de la dirección URL. En su lugar, el tráfico se evalúa con respecto al firewall de WSS y a las reglas de URL. Por ejemplo, si una regla del firewall del cliente de SEP bloquea google.com y una regla de WSS admite google.com, el cliente permite que los usuarios puedan acceder a google.com.El firewall de Symantec Endpoint Protection sigue procesando el tráfico local de entrada al cliente. [SEP-67488] – El portal cautivo de WSS no está disponible para el método de túnel y el cliente omite las credenciales de desafío.En una versión futura, la autenticación de SAML en el agente de WSS reemplazará al portal cautivo y estará disponible en el cliente de Symantec Endpoint Protection. – Si un equipo cliente se conecta a WSS usando el método de túnel y aloja las máquinas virtuales, cada usuario invitado necesitará instalar el certificado SSL proporcionado en el portal de WSS. – El tráfico de la red local, como el directorio de inicio o la autenticación de Active Directory, no se redirige. – No es compatible con la VPN de Microsoft DirectAccess. El método de túnel actualmente se considera una función de lanzamiento de usuario pionero.
Entradas de registro del cliente duplicadas después de la actualización de 14.2.x a 14.3 MP1 y posteriores [14.3 RU1]	Actualización de los clientes de Symantec Endpoint Protection de 14.2.x a 14.3 MP1 y posteriores crea entradas de inscripción de agentes duplicadas para estos clientes en la página **Clientes** de Symantec Endpoint Protection Manager. No hay ningún impacto funcional y se pueden seguir usando las nuevas entradas para los clientes de 14.3 RU1. Symantec Endpoint Protection Manager eliminará las entradas de agente anteriores.
Permitir direcciones URL en Symantec Endpoint Security si se utiliza la opción de administración híbrida, los servidores proxy o un firewall perimetral [14.3]	Gracias a la adquisición de Symantec Enterprise Security por parte de Broadcom, las direcciones URL de la comunicación de cliente a la nube han cambiado en la versión 14.2.2.1. [CDM-42467] Se deben actualizar los clientes a la versión de compilación 14.2.5569.2100 o posterior en la siguiente situación • Utilice Symantec Endpoint Security para administrar los clientes y políticas cuando los dominios locales de Symantec Endpoint Protection Manager estén inscritos en la consola en la nube. • Utilice servidores proxy. Se permiten las direcciones URL en agentes administrados completamente en la nube o en agentes híbridos, lo que hace que también se admitan en el servidor proxy y/o el firewall perimetral. Consulte: • Direcciones URL que permiten que SEP y SES se conecten a los servidores de Symantec • Actualización de los Agentes de Symantec administrados en la nube a la versión 14.2 RU2 MP1 o posterior

Problema	Descripción y solución
La consola remota de Symantec Endpoint Protection Manager ya no es compatible con la plataforma Windows de 32 bits [versión 14.3]	En la versión 14.3 y posteriores, no se puede iniciar sesión en la consola remota de Symantec Endpoint Protection Manager si se ejecuta una versión de 32 bits de Windows. Oracle Java SE Runtime Environment ya no es compatible con las versiones de 32 bits de Microsoft Windows.[SEP-61106] Si aparece el mensaje siguiente, inicie sesión en Symantec Endpoint Protection Manager de forma local: "Esta versión de C:\Users\Administrator\Downloads\Symantec Endpoint Protection Manager Console\bin\javaw.exe no es compatible con la versión de Windows que se está ejecutando. Compruebe la información del sistema del equipo y, a continuación, póngase en contacto con el editor de software."
Aparece el error "Error al instalar Microsoft Visual C++ Runtime" al instalar Symantec Endpoint Protection Manager [versión 14.3]	Es posible que aparezca el siguiente error al instalar Symantec Endpoint Protection Manager en Windows 2012 R2: "Error al instalar Microsoft Visual C++ Runtime" [SEP-60396] Para solucionar este problema, active Windows e instale las actualizaciones de Windows. Windows Update instala el redistribuible de Visual C++ 2017, que es un requisito previo para la instalación de Symantec Endpoint Protection Manager 14.3 en Windows 2012 R2.
Actualización para habilitar TLS 1.1 y TLS 1.2 como protocolos seguros predeterminados en WinHTTP en Windows [versión 14.3]	Después de actualizar o instalar una instancia de Symantec Endpoint Protection Manager versión 14.3 que está inscrita en la consola de la nube, el servidor de administración ya no carga correctamente los registros en la nube. En el archivo uploader.log, es posible que aparezca el siguiente error: `<SEVERE> WinHttpSendRequest: 12175: A security error occurred` Este problema se debe a que falta una actualización de Microsoft que proporciona compatibilidad para TLS 1.1 y 1.2. Para solucionar el problema, instale la siguiente actualización de Microsoft: KB3140245. Para obtener más información, consulte: Actualización para habilitar TLS 1.1 y TLS 1.2 como protocolos seguros predeterminados en WinHTTP en Windows
El mensaje "Implementación en curso" sigue apareciendo en Symantec Endpoint Protection Manager después de que el cliente reciba una política actualizada para Endpoint Threat Defense for AD [versión 14.2 RU1 MP1 y posteriores]	Esto es lo esperado. Las políticas de Endpoint Threat Defense for AD 3.3 solo se admiten en el cliente a partir de la versión 14.2 RU1 MP1. Se aplica una política para Symantec Endpoint Threat Defense for Active Directory 3.3 a un grupo. Este grupo contiene algunos clientes que ejecutan Symantec Endpoint Protection 14.2 RU1 o una versión anterior. Estos clientes reciben y aplican la política según lo esperado, pero el estado en Symantec Endpoint Protection Manager continúa mostrando el mensaje Implementación en curso.

Problemas de clientes de Windows, Mac y Linux

Table 3: Problemas conocidos de clientes de Windows, Mac y Linux

Problema	Descripción y solución
Error inesperado del servidor al iniciar sesión en Endpoint Protection Manager y los clientes ya no se comunican después de cambiar la hora del sistema [14.3 RU3]	Si se establece el reloj del sistema en una fecha u hora que transcurre en el pasado, se puede producir el siguiente error: • Después de iniciar sesión en Symantec Endpoint Protection Manager, aparece un error inesperado del servidor. • Los clientes no se comunican con SEPM, que informa sobre un error 503. [SEP-74510] Para solucionar este problema: • Reinicie manualmente los servicios de SEPM. • Espere hasta que la fecha y hora del sistema pasen la hora original del sistema antes de establecerla de nuevo.
El registro de la Protección de acceso web y en la nube de Endpoint Protection 14.3 RU3 informa sobre el sistema operativo Windows 10 en Windows 11 [14.3 RU3]	Cuando el usuario del cliente ve el registro de la Protección de acceso web y en la nube del cliente de SEP, el registro muestra el sistema operativo como Windows 10 cuando el cliente está instalado en un dispositivo con Windows 11.En la consola del cliente, haga clic en **Protección de acceso web y en la nube** > **Opciones** > **Ver registros**.
El navegador Microsoft Edge y el navegador Google Chrome no pueden iniciarse después de aplicar la técnica de mitigación para **validar la integridad de la dependencia de la imagen** al sistema operativo Windows 10 u 11. [14.3 RU3]	Una de las técnicas de mitigación que Microsoft Edge usa para proteger el sistema operativo Windows es la técnica para **validar la integridad de la dependencia de la imagen**.Para los equipos con Windows 10 u 11 que ejecutan las versiones 14.2 RU2 MP1 o posteriores de los clientes de Symantec Endpoint Protection, si esta opción está habilitada, no se iniciarán los navegadores web Microsoft Edge y Google Chrome. [SEP-75086] Para asegurarse de que se inicie Microsoft Edge, deshabilite la **técnica para validar la integridad de la dependencia de la imagen**. Para obtener más información sobre las técnicas de mitigación para Microsoft Edge, consulte: Customize exploit protection Consulte también: Microsoft Edge and Google Chrome do not open if "Validate image dependence integrity" mitigation technique is applied and SEP 14.2 RU2 MP1 or later is installed
Se debe reiniciar el cliente de Windows sin reinicio para obtener los últimos eventos de EDR [14.3 RU3]	Para que los eventos de ETW adicionales estén disponibles en la versión 14.3 RU3, se debe reiniciar el cliente de Symantec Endpoint Protection. Se debe reiniciar el cliente en las situaciones siguientes: [SEP-73327] • Si EDR está habilitado y se actualiza el cliente a RU3. • Si la versión 14.3 RU3 ya está instalada y se habilita o deshabilita EDR. Se debe reiniciar el cliente para habilitar o deshabilitar los eventos agregados recientemente. Consulte: A restart may be required to begin seeing some ETW events with EDR and SEP 14.3 RU3
Se produce un error al inicializar el motor de análisis después de la actualización del cliente de Linux. [14.3 RU3]	Se produce un error al inicializar el motor de análisis después de actualizar el cliente de Symantec Endpoint Protection para Linux a la versión 14.3 RU3. **Solución temporal:** 1. Actualice LiveUpdate Server con el contenido más reciente que puede tener SEF 1.7.6. 2. Desinstale el cliente de Linux de la versión 14.3 RU3 que exhibe el error de inicialización del motor de análisis. 3. Reinstale el cliente de Linux de la versión 14.3 RU3.
El daemon `auditd` se habilitará después de la instalación del cliente de Linux. [14.3 RU3]	El cliente de Symantec Endpoint Protection para el instalador de Linux habilita el daemon `auditd` después de la instalación del agente, incluso si se ha deshabilitado el daemon `auditd` antes de la instalación.
Para recopilar la información forense de la red (EDR), el paquete `netstat` es necesario en el cliente de Linux. [14.3 RU3]	Si el paquete `netstat` falta en el cliente de Linux, la información forense se recopila para el resto de los tipos de eventos a excepción de los eventos de red.

Problema	Descripción y solución
Problemas de conexión posibles en los dispositivos Mac. [14.3 RU2]	• Después de actualizar el agente de Mac usando la actualización automática y reiniciar el dispositivo, es posible que se produzca un error en el agente al conectarse a la red. **Solución temporal**: Vuelva a ejecutar el paquete de instalación del agente. • Después de estar en modo de espera, es posible que un dispositivo Mac pueda perder la conexión de red con el siguiente error: "Se ha interrumpido la conexión. Se ha detectado un cambio en la red". **Soluciones temporales:** – Si usa una estación de acoplamiento, renueve las direcciones IP manualmente en **Preferencias del sistema > Red**. – Desconecte la estación de acoplamiento del dispositivo Mac durante unos segundos y vuelva a conectarla.
Rosetta puede bloquear la instalación del agente de Mac en dispositivos con Apple Silicon (M1) con el siguiente error: "Esta versión del agente de Symantec para Mac no es compatible con el chip de Apple M1". [14.3 RU2]	Para obtener más información, consulte: Artículo de la base de conocimiento 222282
Es posible que se produzca un error en la descarga e instalación del agente de Mac usando el vínculo web que se ha generado en Symantec Endpoint Protection Manager. [14.3 RU2]	Si un administrador invita a los usuarios a instalar el agente de Mac 14.3 RU2 usando la opción **Correo electrónico y vínculos web** en Symantec Endpoint Protection Manager y los usuarios descargan el paquete usando este vínculo en el navegador Safari, se puede producir un error en la instalación del agente de Mac con el siguiente error: "No se puede abrir la aplicación del instalador de Symantec Endpoint Protection" **Soluciones temporales:** • Después de descargar el archivo, vaya a la carpeta **Descargas**, ejecute el comando siguiente y, a continuación, ejecute la instalación de nuevo: `chmod +x ./Symantec\ Endpoint\ Protection/Symantec\ Endpoint\ Protection\ Installer.app/Contents/MacOS/Symantec\ Endpoint\ Protection\ Installer` • Abra **Preferences** en el navegador Safari y, en la ficha **General**, anule la selección de la opción **Open "safe" files after downloading**.A continuación, descargue el paquete del instalador y ejecute la instalación.
Si se actualiza automáticamente un cliente con un idioma no admitido al inglés, el cliente continúa mostrando la configuración de la fecha para las definiciones en inglés [14.3 RU1 y versiones posteriores]	Para solucionar este problema, desinstale el cliente de una versión anterior e instale manualmente un nuevo paquete de instalación del cliente en inglés. Además, se espera una corrección para los clientes que se actualizan automáticamente. [SEP-72481]
La instancia de Symantec WSS Agent independiente bloquea la instalación del cliente de Symantec Endpoint Protection si se instala SEP en el mismo equipo que WSS Agent	El componente de redirección de tráfico de red (NTR) usa los mismos archivos que la instancia de Symantec WSS Agent independiente (WSSA). NTR se instala de forma predeterminada en Symantec Endpoint Protection y en la consola en la nube de Symantec Endpoint Security.Si la función de NTR está instalada en un endpoint, no se puede instalar WSSA. Del mismo modo, si WSSA está instalado, la función de NTR no se instala. Se puede eliminar la función de redirección de tráfico de red de los endpoints existentes sin tener que desinstalar el cliente completo utilizando uno de los siguientes métodos: • En Symantec Endpoint Protection Manager, cree un Conjunto de funciones de instalación de clientes que no incluya la redirección de tráfico de red y aplíquelo a los endpoints.Consulte: Adición o eliminación de funciones en los clientes existentes de Endpoint Protection • La siguiente opción de la línea de comandos usa el archivo de instalación del cliente para eliminar NTR: `setup.exe /s /v" REMOVE=NTR /qn"`

Problema	Descripción y solución
El paquete de instalación de la actualización que se usa para la instalación limpia instala el conjunto de funciones predeterminadas. [14.3 RU1 MP1 y versiones anteriores]	Si se crea un paquete de instalación de la actualización con la opción **Conservar funciones existentes del cliente al actualizar** seleccionada y se usa este paquete para llevar a cabo una instalación limpia, se instalará el conjunto de funciones predeterminadas en el dispositivo cliente. Si se desea instalar un conjunto de funciones personalizadas, se deberá crear un paquete de instalación aparte para la instalación limpia.
La ruta de actualización no admitida crea dispositivos duplicados en la consola en la nube. [14.3 RU1]	La actualización de macOS de la versión 10.15 a la versión 11.0 antes de actualizar el Agente de Symantec para Mac de la versión 14.2/14.3 a la versión 14.3 RU1 crea dispositivos duplicados en la consola en la nube. Para evitar duplicados, se debe actualizar el cliente antes de actualizar el sistema operativo (es decir, primero actualizar el Agente de Symantec para Mac de la versión 14.2/14.3 a la versión 14.3 RU1 y, a continuación, actualizar macOS de la versión 10.15 a la versión 11.0).
Mensajes incorrectos en el registro del instalador del Agente de Symantec para Linux. [14.3 RU1]	En algunos casos, el instalador del agente registra mensajes incorrectos relacionados con una versión del controlador no coincidente o un reinicio necesario. Estos mensajes no afectan a la funcionalidad del agente.
En un dispositivo SuSe Linux, zypper elimina los paquetes de cliente de SEP Linux al eliminar el paquete 'at'. [14.3 RU1]	En un dispositivo SuSe Linux, el comando 'zypper remove at' elimina los paquetes de cliente de SEP Linux, ya que el paquete 'at' se agrega como un paquete dependiente obligatorio y los comandos zypper intentan eliminar automáticamente los paquetes de cliente de SEP 'sdcss-kmod' y 'sdcss-sepagent' como paquetes con dependencias no utilizadas. **Solución temporal**: para eliminar el paquete 'at', ejecute el siguiente comando: rpm -e --nodeps at
Incidencia de actualización en macOS 10.15 y posteriores [14.3 MP1]	En macOS 10.15 y versiones posteriores, la función **Instalar Symantec Endpoint Protection en equipos remotos** del asistente de implementación del cliente no puede actualizar el cliente de Symantec Endpoint Protection de versiones anteriores a la versión 14.3 MP1. **Solución temporal**: utilice la **actualización automática de Symantec Endpoint Protection Manager** para realizar la actualización de cliente de Symantec Endpoint Protection en macOS 10.15 y versiones posteriores.
La instalación del cliente de Windows de Symantec Endpoint Protection 14.3 puede producir un error a menos que se instale en primer lugar la compatibilidad de SHA-2 [versión 14.3]	Si se ejecutan versiones de sistemas operativos heredados (Windows 7 RTM o SP1, Windows Server 2008 R2, R2 SP1 o R2 SP2), se debe tener instalado el soporte de firma de código de SHA-2 en los dispositivos para instalar las actualizaciones de Windows publicadas en Julio del 2019 o posteriormente. Sin el soporte de SHA-2, a veces se produce un error en la instalación del cliente de Windows. Se puede producir un error en la instalación si se instalan clientes por primera vez o si se actualizan automáticamente desde una versión anterior.[SEP-61175/61403] Para obtener el soporte de firma de código de SHA-2 de Microsoft, consulte: • 2019 SHA-2 Code Signing Support requirement for Windows and WSUS • El cliente de Windows de Symantec Endpoint Protection 14.3 puede producir un error a menos que se instale la compatibilidad de SHA-2
El cliente de Windows de Symantec Endpoint Protection no se ejecuta cuando se instala en Windows 10 1803 con UWF habilitado [versión 14.3]	Si el cliente de Symantec Endpoint Protection se ejecuta en el sistema operativo Windows 10 RS4 1803 de 32 bits cuando se habilita Unified Write Filter (UWF) y protege la unidad en la que está instalado el cliente de Windows, el cliente no se ejecutará correctamente. Este sistema operativo de Windows contiene un defecto de UWF que impide que el cliente de Windows se ejecute. Para solucionar este problema: • Actualice a otra versión del sistema operativo que no contenga el defecto. • Deshabilite UWF.Consulte: Endpoint Protection is malfunctioning when installed on Windows 10 1803 with UWF enabled

Problema	Descripción y solución
Los clientes de Mac que habilitan la redirección de tráfico de WSS no respetan la configuración del proxy personalizada para LiveUpdate [versión 14.2 RU1 MP1 y posterior]	Se han configurado los clientes de Mac administrados para que Symantec Endpoint Protection 14.2 RU1 MP1 o posterior use la configuración del proxy personalizada para LiveUpdate a través de la configuración de comunicaciones externas. Después de habilitar la redirección de tráfico de WSS (WTR) para los clientes de Mac mediante la política de Symantec Endpoint Protection Manager, sin embargo, se encuentra que el tráfico de LiveUpdate ya no respeta la configuración del proxy personalizada. Por el contrario, LiveUpdate intenta una conexión directa. Para solucionar este problema, use solamente la configuración del proxy personalizada para LiveUpdate cuando la redirección de tráfico de WSS esté deshabilitada.
Microsoft Edge inesperadamente permite descargas de PDF con protección habilitada [versión 14.2 RU1 MP1 y posterior]	Con la protección de aplicaciones habilitada en el cliente de Symantec Endpoint Protection, inesperadamente se pueden descargar archivos PDF si se usa el navegador Microsoft Edge. La prevención de descarga de archivos PDF funciona como se esperaba con otros navegadores. Se ha planificado una corrección para este problema en una versión futura.

Para las incidencias resueltas, consulte:

- Nuevas correcciones y componentes para Symantec Endpoint Protection 14.3 RU3
- Nuevas correcciones y componentes para Symantec Endpoint Protection 14.3 RU1 MP1
- Nuevas correcciones y componentes para Symantec Endpoint Protection 14.3 RU1
- Nuevas correcciones y componentes para Symantec Endpoint Protection 14.3 MP1
- Nuevas correcciones y componentes para Symantec Endpoint Protection 14.3

Documentación

Se puede encontrar la documentación en el portal de Symantec Security Tech Docs de Broadcom.

Para encontrar la documentación de Endpoint Protection, haga clic en la ficha **Symantec Security Software** y, a continuación, haga clic en **Endpoint Security and Management** > **Endpoint Protection**.

Para encontrar un archivo PDF, las notas de la versión o el esquema de la base de datos de Symantec Endpoint Protection Manager, vaya a la página Documentos relacionados. En el futuro, Broadcom agregará los archivos PDF heredados y los archivos PDF traducidos.

Requisitos del sistema para Symantec Endpoint Protection (SEP) 14.3 RU3

Generalmente, los requisitos del sistema para los siguientes son los mismos que los de los sistemas operativos en los cuales se admiten.

> **NOTE**
> Es posible que una versión anterior de Symantec Endpoint Protection Manager no pueda administrar correctamente un cliente con una versión posterior. Es posible que se produzcan incidencias con las actualizaciones de contenido y con la administración de clientes.Por ejemplo, Symantec Endpoint Protection Manager 14.0.1 o anterior no puede proporcionar correctamente un cliente de la versión 14.2 con sus monikers específicos de la versión. Symantec Endpoint Protection Manager para versiones anteriores a la versión 14 MP2 no puede proporcionar correctamente versiones de cliente posteriores a la versión 14.0.1 con sus monikers específicos de la versión.

En las tablas siguientes se describen los requisitos de software y hardware para Symantec Endpoint Protection.

Table 4: Requisitos de sistema de software para Symantec Endpoint Protection Manager (SEPM)

Componente	Requisitos
Sistema operativo	• Windows Server 2008 R2 • Windows Server 2012 • Windows Server 2012 R2 • Windows Server 2016 • Windows Server 2019 • Windows Server 2022 (a partir de la versión 14.3 RU3) **Note:** No se admiten sistemas operativos de equipos de escritorio. **Note:** Windows Server Core Edition no es compatible con la versión 14.2x ni versiones anteriores.
Navegador web	Los siguientes navegadores admiten el acceso de la consola web a Symantec Endpoint Protection Manager y la visualización de la Ayuda de Symantec Endpoint Protection Manager: • Navegador Microsoft Edge basado en Chromium (14.3 y versiones posteriores) • Microsoft Edge **Note:** Windows 10 de 32 bits no admite el acceso a la consola web en el navegador Edge. • Microsoft Internet Explorer 11 (14.2.x y versiones anteriores) • Mozilla Firefox 5.x hasta la versión 83 • Google Chrome 87

Componente	Requisitos
Base de datos	Symantec Endpoint Protection Manager incluye una base de datos predeterminada: • Microsoft SQL Server Express 2014 (para Windows Server 2008 R2) • Microsoft SQL Server Express 2017 • Base de datos de Sybase incrustada (14.3 MP.x y versiones anteriores únicamente) En su lugar, es posible optar por usar una base de datos de una de las siguientes versiones de Microsoft SQL Server: • SQL Server 2008 SP4 • SQL Server 2008 R2, SP3 • SQL Server 2012 RTM - SP4 • SQL Server 2014 RTM - SP3 • SQL Server 2016 SP1, SP2 • SQL Server 2017 RTM • SQL Server 2019 RTM (14.3 y versiones posteriores) **Note:** Se admiten las bases de datos de SQL Server que se alojan en Amazon RDS. (14.0.1 MP2 y versiones posteriores). **Note:** Si Symantec Endpoint Protection usa una base de datos de SQL Server y su entorno usa solamente TLS 1.2, asegúrese de que SQL Server admita TLS 1.2. Es posible que deba aplicar un parche de SQL Server. Esta recomendación se aplica a SQL Server 2008, 2012 y 2014.Consulte: **Note:** Compatibilidad con TLS 1.2 para Microsoft SQL Server
Otros requisitos del entorno	• En redes puramente IPv6, la pila de IPv4 debe estar instalada y deshabilitada. Si se desinstala la pila de IPv4, Symantec Endpoint Protection Manager no funciona. • Paquete Microsoft Visual C++ 2017 Redistributable (x64/x86) **Note:** Tenga en cuenta que la versión necesaria de Visual C++ se instala automáticamente durante la instalación de Symantec Endpoint Protection Manager.

Table 5: Requisitos de sistema de hardware para Symantec Endpoint Protection Manager

Componente	Requisitos
Procesador	Intel Pentium Dual-Core o equivalente, como mínimo; se recomiendan 8 núcleos como mínimo **Note:** Los procesadores Intel Itanium IA-64 no se admiten.
RAM física	2 GB de RAM disponible como mínimo; se recomiendan 8 GB o más. **Note:** Es posible que el servidor de Symantec Endpoint Protection Manager requiera más memoria RAM según los requisitos de memoria RAM de otras aplicaciones que ya estén instaladas.Por ejemplo, si Microsoft SQL Server está instalado en el servidor de Symantec Endpoint Protection Manager, el servidor debe tener un mínimo de 8 GB disponibles.
Pantalla	1024x768 o superior
Disco duro al instalar en la unidad del sistema	Con una base de datos local de SQL Server: • 40 GB como mínimo (se recomiendan 200 GB) para el servidor de administración y la base de datos Con una base de datos remota de SQL Server: • 40 GB como mínimo (se recomiendan 100 GB) para el servidor de administración • Espacio en disco disponible adicional en el servidor remoto para la base de datos

Componente	Requisitos
Disco duro al instalar en una unidad alternativa	Con una base de datos local de SQL Server: • La unidad del sistema requiere 15 GB disponibles como mínimo (se recomiendan 100 GB) • La unidad de instalación requiere 25 GB disponibles como mínimo (se recomiendan 100 GB) Con una base de datos remota de SQL Server: • La unidad del sistema requiere 15 GB disponibles como mínimo (se recomiendan 100 GB) • La unidad de instalación requiere 25 GB disponibles como mínimo (se recomiendan 100 GB) • Espacio en disco disponible adicional en el servidor remoto para la base de datos
Otros	Una tarjeta de interfaz de red habilitada

Si usa una base de datos de SQL Server, es posible que se necesite más espacio libre en disco disponible. La cantidad y la ubicación del espacio adicional dependen de qué unidad SQL Server se use, de los requisitos de mantenimiento de la base de datos y de otras configuraciones de la base de datos.

Table 6: Requisitos de sistema de software del cliente de Symantec Endpoint Protection para Windows

Componente	Requisitos
Sistema operativo (escritorio)	• Windows 7 (32 bits y 64 bits, RTM y SP1) • Windows Embedded 7 Standard, POSReady y Enterprise (32 y 64 bits) • Windows 8 (32 bits y 64 bits) • Windows Embedded 8 Standard (32 y 64 bits) • Windows 8.1 (32 y 64 bits), incluyendo Windows To Go • Windows 8.1 Update for April 2014 (32 y 64 bits) • Windows 8.1 Update for August 2014 (32 y 64 bits) • Windows Embedded 8.1 Pro, Industry Pro e Industry Enterprise (32 y 64 bits) • Windows 10 (versión 1507) (32 y 64 bits), incluyendo Windows 10 Enterprise 2015 LTSB • Windows 10 Update November Update (versión 1511) (32 y 64 bits) • Windows 10 Anniversary Update (versión 1607) (32 y 64 bits), incluyendo Windows 10 Enterprise 2016 LTSB • Windows 10 Creators Update (versión 1703) (32 y 64 bits) • Windows 10 Fall Creators Update (versión 1709) (32 y 64 bits) • Windows 10 April 2018 Update (versión 1803) (32 y 64 bits) • Windows 10 October 2018 Update (versión 1809) (32 y 64 bits), incluido Windows 10 Enterprise 2019 LTSC. • Windows 10 May 2019 Update (versión 1903) (32 y 64 bits) • Windows 10 November 2019 Update (versión 1909) (32 y 64 bits) (a partir de la versión 14.2 RU1 y posterior) • Windows 10 20H1 (Windows 10 versión 2004) (14.3 y versiones posteriores) • Windows 10 20H2 (Windows 10 versión 2009) (14.3 y versiones posteriores) • Windows 10 21H1 (a partir de la versión 14.3 RU1) • Se ha probado la versión 14.3 RU3 y es compatible con todas las versiones anteriores a la versión de Windows 11 (a partir de 14.3 RU3)
Sistema operativo (servidor)	• Windows Server 2008 R2 • Windows Small Business Server 2011 • Windows Server 2012 • Windows Server 2012 R2 • Windows Server 2012 R2 update for April 2014 • Windows Server 2012 R2 update for August 2014 • Windows Server 2016 • Windows Server 2019 • Windows Server, versión 1803 (Server Core) (versión 14.2 y posterior) • Windows Server, versión 1809 (Server Core) • Windows Server, versión 1903 (Server Core) (a partir de la versión 14.2 RU1) • Windows Server, versión 1909 (Server Core) (a partir de la versión 14.2 RU1 y posterior) • Windows Server, versión 2004 • Windows Server, versión 20H2 (14.3 RU1) • Windows Server 2022 (a partir de la versión 14.3 RU3) Para obtener una lista de los sistemas operativos admitidos para las versiones anteriores, consulte lo siguiente: • Compatibilidad de Windows con el cliente de Endpoint Protection • Compatibilidad de Endpoint Protection con las actualizaciones de Windows 10 y Windows Server 2016/Server 2019

Componente	Requisitos
Prevención contra intrusiones de navegador	La compatibilidad de Prevención contra intrusiones de navegador se basa en la versión del motor del sistema de detección de intrusiones de clientes (CIDS).Consulte: Consulte Navegadores compatibles para Prevención contra intrusiones de navegador en Endpoint Protection.

Table 7: Requisitos de sistema de hardware par el cliente de Symantec Endpoint Protection para Windows

Componente	Requisitos
Procesador (para equipos físicos)	• Procesador de 32 bits: Intel Pentium 4 de 2 GHz o equivalente como mínimo (Intel Pentium 4 o equivalente recomendado) • Procesador de 64 bits: Pentium 4 de 2 GHz con soporte de x86-64 o un mínimo equivalente **Note:** Los procesadores Itanium no se admiten.
Procesador (para equipos virtuales)	Un zócalo virtual y un núcleo por zócalo de 1 GHz como mínimo (se recomienda un zócalo virtual y dos núcleos por zócalo de 2 GHz) **Note:** La reserva de recursos del hipervisor debe estar habilitada.
RAM física	1 GB (2 GB recomendado) o más si lo requiere el sistema operativo
Pantalla	800x600 o superior
Disco duro	Los requisitos de espacio libre en disco dependen del tipo de cliente que instala, del disco en que lo instala y de dónde reside el archivo de datos del programa. La carpeta de datos del programa generalmente está en la unidad del sistema, en la ubicación predeterminada C:\ProgramData. Siempre se requiere espacio libre en disco en la unidad del sistema, sin importar qué unidad de instalación elige. **Note:** Los requisitos de espacio se basan en los sistemas de archivos NTFS. También se requiere espacio adicional para las actualizaciones de contenido y los registros.

Table 8: Requisitos del sistema para el disco duro disponible de Symantec Endpoint Protection para Windows cuando se instala en la unidad del sistema

Tipo de cliente	Requisitos
Estándar	Con la carpeta de datos del programa situada en la unidad del sistema: • 395 MB* Con la carpeta de datos del programa situada en una unidad alternativa: • Unidad del sistema: 180 MB • Unidad de instalación alternativa: 350 MB
Integrada/VDI	Con la carpeta de datos del programa situada en la unidad del sistema: • 245 MB* Con la carpeta de datos del programa situada en una unidad alternativa: • Unidad del sistema: 180 MB • Unidad de instalación alternativa: 200 MB
Red oscura	Con la carpeta de datos del programa situada en la unidad del sistema: • 545 MB* Con la carpeta de datos del programa situada en una unidad alternativa: • Unidad del sistema: 180 MB • Unidad de instalación alternativa: 500 MB

*Se necesitan 135 MB adicionales durante la instalación.

Table 9: Requisitos del sistema de disco duro disponible cuando el cliente de Symantec Endpoint Protection para Windows se instala en una unidad alternativa

Tipo de cliente	Requisitos
Estándar	Con la carpeta de datos del programa situada en la unidad del sistema: • Unidad del sistema: 380 MB • Unidad de instalación alternativa: 15 MB* Con la carpeta de datos del programa situada en una unidad alternativa:** • Unidad del sistema: 30 MB • Unidad de datos del programa: 350 MB • Unidad de instalación alternativa: 150 MB
Integrada/VDI	Con la carpeta de datos del programa situada en la unidad del sistema: • Unidad del sistema: 230 MB • Unidad de instalación alternativa: 15 MB* Con la carpeta de datos del programa situada en una unidad alternativa:** • Unidad del sistema: 30 MB • Unidad de datos del programa: 200 MB • Unidad de instalación alternativa: 150 MB
Red oscura	Con la carpeta de datos del programa situada en la unidad del sistema: • Unidad del sistema: 530 MB • Unidad de instalación alternativa: 15 MB* Con la carpeta de datos del programa situada en una unidad alternativa:** • Unidad del sistema: 30 MB • Unidad de datos del programa: 500 MB • Unidad de instalación alternativa: 150 MB

*Se necesitan 135 MB adicionales durante la instalación.

** Si la carpeta de datos del programa es la misma que en la unidad de instalación alternativa, añada 15 MB a la unidad de datos del programa para su total. Sin embargo, el instalador aún necesita los 150 MB disponibles en la unidad de instalación alternativa durante la instalación.

Table 10: Requisitos del sistema del cliente de Symantec Endpoint Protection para Windows Embedded

Componente	Requisitos
Procesador	1 GHz Intel Pentium
RAM física	256 MB **Note:** Este valor corresponde a una instalación del cliente integrado de Symantec Endpoint Protection. Si también implementa funciones adicionales de una solución integrada, como EDR, necesitará más memoria RAM física.
Disco duro	El cliente integrado/VDI de Symantec Endpoint Protection requiere el siguiente espacio libre en disco disponible: • Instalado en la unidad del sistema: 245 MB • Instalado en una unidad alternativa: 230 MB en la unidad del sistema y 15 MB en la unidad alternativa Se necesitan 135 MB adicionales durante la instalación. Estas figuras asumen que la carpeta de datos del programa está en la unidad del sistema. Para obtener más información detallada o los requisitos de otros tipos de cliente, consulte el cliente de Symantec Endpoint Protection para obtener los requisitos del sistema Windows.

Componente	Requisitos
Sistema operativo Windows Embedded	• Windows Embedded Standard 7 (de 32 y 64 bits) • Windows Embedded POSReady 7 (de 32 y 64 bits) • Windows Embedded Enterprise 7 (de 32 y 64 bits) • Windows Embedded 8 Standard (32 y 64 bits) • Windows Embedded 8.1 Industry Pro (32 y 64 bits) • Windows Embedded 8.1 Industry Enterprise (32 y 64 bits) • Windows Embedded 8.1 Pro (32 y 64 bits) • Windows Embedded 10 (a partir de la versión 14.3 RU3) • Se ha probado la versión 14.3 RU3 y es compatible con todas las versiones previas al lanzamiento de Windows 11 Embedded (a partir de 14.3 RU3).
Componentes mínimos necesarios	• Administrador de filtro (FltMgr.sys) • Ayudante de los datos de rendimiento (pdh.dll) • Servicio de Windows Installer
Plantillas	• Compatibilidad de la aplicación (opción predeterminada) • Signos digitales • Automatización industrial • IE, Media Player, RDP • Decodificador de televisor • Cliente delgado La plantilla de configuración mínima no se admite. El filtro de escritura mejorado (EWF) y el filtro de escritura unificado (UWF) no se admiten. El filtro de escritura recomendado es el filtro de escritura basado en archivos (FBWF) instalado con el filtro del registro.

Table 11: Requisitos de sistema del cliente de Symantec Endpoint Protection para Mac

Componente	Requisitos
Procesador/chip	Intel Core 2 Duo de 64 bits o posterior Chip M1 de Apple (a partir de la versión 14.3 RU2)
RAM física	2 GB de RAM
Disco duro	1 GB de espacio libre en el disco duro disponible para la instalación
Pantalla	800x600
Sistema operativo	• macOS de la versión 10.15 a la versión 10.15.7 • macOS 11 (Big Sur) Para obtener una lista de los sistemas operativos admitidos para las versiones anteriores, consulte lo siguiente: Compatibilidad de Mac con el cliente de Endpoint Protection

Table 12: Requisitos de sistema del cliente de Symantec Endpoint Protection para Linux

Componente	Requisitos
Hardware	• Intel Pentium 4 (2 GHz) o un procesador posterior • 1 GB de RAM libre (se recomiendan 4 GB de RAM) • 2 GB de espacio libre en disco si `/var`, `/opt` y `/tmp` comparten el mismo sistema de archivos o volumen • 500 MB de espacio libre en disco en cada `/var`, `/opt` y `/tmp` si están en volúmenes diferentes
Sistemas operativos	Sistemas operativos compatibles a partir de la versión 14.3 RU1: • Amazon Linux 2 • CentOS 6, 7 y 8 • Debian 9, 10 (14.3 RU2 y versiones posteriores) • Oracle Enterprise Linux 6, 7 y 8 • Red Hat Enterprise Linux 6, 7 y 8 • SuSE Linux Enterprise Server 12.x, 15.x • Ubuntu 14.04 LTS, 16.04 LTS, 18.04 LTS, 20.04 LTS Para obtener más información y para obtener listas de versiones secundarias admitidas del SO Linux, consulte: Kernels admitidos del Agente de Symantec para Linux Sistemas operativos compatibles con la versión 14.3 MP1 y anteriores: • Amazon Linux • CentOS 6U3 - 6U9, 7 - 7U7, 8; 32 bits y 64 bits • Debian 6.0.5 Squeeze, Debian 8 Jessie; 32 y 64 bits • Fedora 16, 17; de 32 y 64 bits • Oracle Linux (OEL) 6U2, 6U4, 6U5, 6U8; 7, 7U1, 7U2, 7U3, 7U4 • Red Hat Enterprise Linux Server (RHEL) 6U2 - 6U9, 7 - 7U8, 8-8U2 • SUSE Linux Enterprise Server (SLES) 11 SP1 a 11 SP4, 32 y 64 bits; 12, 12 SP1 a 12 SP3 de 64 bits • SUSE Linux Enterprise Desktop (SLED) 11 SP1 a 11 SP4 de 32 bits y 64 bits; 12 SP3 de 64 de bits • Ubuntu 12.04, 14.04, 16.04, 18.04 (a partir de la versión 14.3); 32 bits y 64 bits Para obtener una lista de los kernels del sistema operativo admitidos para las versiones anteriores, consulte: Lista de distribuciones y kernels de Linux con controladores/módulos de Auto-Protect previamente compilados para Symantec Endpoint Protection para Linux 14.x
Otros requisitos del entorno (14.3 RU1 y versiones posteriores)	• OpenSSL 1.0.2k-fips o versiones posteriores

Componente	Requisitos

Otros requisitos medioambientales (14.3 MP1 y versiones anteriores)	• Glibc
	No se admiten sistemas operativos que ejecuten una versión de Glibc anterior a la versión 2.6.
	• net-tools o iproute2
	Symantec Endpoint Protection usa una de estas dos herramientas, dependiendo de cuál está instalada en el equipo.
	• Herramientas de desarrollador
	El proceso de compilación automática y compilación manual para el módulo kernel de Auto-Protect requieren que se instalen ciertas herramientas de desarrollador. Estas herramientas de desarrollador incluyen gcc y los archivos de origen y encabezado del kernel. Para obtener detalles sobre qué instalar y cómo instalarlo para las versiones específicas de Linux, consulte:
	Compilación manual de los módulos del kernel Auto-Protect para Endpoint Protection para Linux
	• Paquetes dependientes basados en i686 en equipos de 64 bits
	Muchos de los archivos ejecutables del cliente Linux son programas de 32 bits. Para equipos de 64 bits, es necesario instalar los paquetes dependientes basados en i686 antes de instalar el cliente de Linux.
	Si aún no ha instalado los paquetes dependientes basados en i686, puede instalarlos con la línea de comandos. Esta instalación requiere los privilegios del superusuario, que los comandos siguientes demuestran con `sudo`:
	– Para las distribuciones basadas en Red Hat: `sudo yum install glibc.i686 libgcc.i686 libX11.i686 libnsl.i686`
	– Para las distribuciones basadas en Debian: `sudo apt-get install ia32-libs`
	– Para distribuciones basadas en Ubuntu:
	`sudo dpkg --add-architecture i386`
	`sudo apt-get update`
	`sudo apt-get install gcc-multilib libx11-6:i386`

Entornos gráficos de equipo de escritorio	Es posible usar los entornos de equipo de escritorio gráficos siguientes para ver el cliente de Symantec Endpoint Protection para Linux: • KDE • Gnome • Unidad El Agente de Symantec para Linux 14.3 RU1 no tiene una interfaz gráfica de usuario.

Más información

Versiones de lanzamiento, notas, nuevas reparaciones y requisitos del sistema para Endpoint Security y todas las versiones de Endpoint Protection

Rutas de actualización admitidas y no admitidas para la versión más reciente de Symantec Endpoint Protection 14.x

Por lo general, todas las versiones que aparecen antes que la versión más reciente de Symantec Endpoint Protection en la lista son compatibles. Sin embargo, debería confirmarlo consultando las notas de la versión de la versión específica.Consulte:

Versiones de lanzamiento, notas, nuevas reparaciones y requisitos del sistema para Endpoint Security y todas las versiones de Endpoint Protection

Rutas de actualización compatibles

- Symantec Endpoint Protection Manager versión 12.1.6 MP10 y versiones posteriores con las actualizaciones de la base de datos integrada instaladas sin problemas en la base de datos de Microsoft SQL Server Express, versión 14.3 RU1 MP1. Se bloquean las actualizaciones de 12.1.6 MP9 y anteriores en la versión 14.3 RU1 MP1.
- Symantec Endpoint Protection Manager 14.x actualiza a la perfección la versión 12.1.x, excepto en los casos en los que se ha eliminado la compatibilidad como, por ejemplo: Windows Server 2003, sistemas operativos de escritorio y sistemas operativos de 32 bits, así como algunas versiones de SQL Server.
- El cliente de Symantec Endpoint Protection 14.x actualiza a la perfección todas las versiones anteriores del cliente 12.1 instaladas en sistemas operativos compatibles.Consulte:

Consideraciones sobre la migración de Symantec Endpoint Protection 14

Symantec Endpoint Protection Manager y cliente Windows

Las siguientes versiones del cliente de Symantec Endpoint Protection Manager y Symantec Endpoint Protection para Windows se pueden actualizar directamente a la versión actual:

- 11.x y Small Business Edition 12.0 (solo para clientes de Symantec Endpoint Protection, para sistemas operativos compatibles)
- 12.1.x, hasta 12.1.6 MP10
- 14, 14 MP1, 14 MP2
- 14 RU1, 14 RU1 MP1, 14 RU1 MP2
- 14.2, 14.2 MP1
- 14.2 RU1, 14.2 RU1 MP1
- 14.2 RU2, 14.2 RU2 MP1
- 14.3, 14.3 MP1
- 14.3 RU1, 14.3 RU1 MP1, 14.3 RU2

Cliente de Mac

Las siguientes versiones del cliente de Symantec Endpoint Protection para Mac se pueden actualizar directamente a la versión actual:

- 12.1.4 - 12.1.6 MP9
  El cliente de Mac no se actualizó para la versión 12.1.6 MP10.
- 14, 14 MP1, 14 MP2
- 14 RU1, 14 RU1 MP1, 14 RU1 MP2

El cliente de Symantec Endpoint Protection for Mac no se actualizó a 14.0.1 MP2.
- 14.2, 14.2 MP1
- 14.2 RU1, 14.2 RU1 MP1
- 14.2 RU2, 14.2 RU2 MP1
- 14.3, 14.3 MP1
- 14.3 RU1, 14.3 RU1 MP1 (disponible en junio de 2021), 14.3 RU2

Cliente para Linux

> **NOTE**
> A partir de la versión 14.3 RU1, el instalador del cliente de Linux detecta y desinstala el cliente de Linux heredado (anterior a la versión 14.3 RU1) y, a continuación, realiza una nueva instalación del nuevo cliente. Las configuraciones antiguas no se conservan.

Las siguientes versiones del cliente de Symantec Endpoint Protection para Linux se pueden actualizar directamente a la versión actual:

- 12.1.x, hasta 12.1.6 MP9
  El cliente de Linux no se actualizó para la versión 12.1.6 MP10.
- 14, 14 MP1, 14 MP2
- 14 RU1, 14 RU1 MP1, 14 RU1 MP2
- 14.2, 14.2 MP1
- 14.2 RU1, 14.2 RU1 MP1
- 14.2 RU2, 14.2 RU2 MP1
- 14.3, 14.3 MP1
- 14.3 RU1, 14.3 RU1 MP1, 14.3 RU2

Symantec AntiVirus para Linux 1.0.14 es la única versión que se puede migrar directamente a Symantec Endpoint Protection. Se debe primero desinstalar el resto de las versiones de Symantec AntiVirus para Linux. No es posible migrar un cliente administrado a un cliente no administrado.

Rutas de la actualización no admitidas

No es posible migrar a Symantec Endpoint Protection de todos los productos de Symantec. Es necesario desinstalar los siguientes productos antes de instalar el cliente de Symantec Endpoint Protection.

- Symantec AntiVirus y Symantec Client Security, los cuales no son compatibles.
- Todos los productos Norton de Symantec
- Symantec Endpoint Protection para Windows XP Embedded 5.1
- Cualquier Symantec Endpoint Protection para el cliente de Mac anterior a 12.1.4.O se puede actualizar a 12.1.4 o versiones posteriores.

Información adicional

- No se admite ninguna migración de cliente de Symantec Endpoint Protection para la versión anterior a 12.1.x.
- No se puede actualizar directamente Symantec Endpoint Protection Manager 11.0.x o Symantec Endpoint Protection Manager Small Business Edition 12.0.x a cualquier versión de Symantec Endpoint Protection Manager 14. Primero,

es necesario desinstalar estas versiones o realizar una actualización a la versión 12.1.x antes de actualizar a la última versión 14.x.

- No es posible actualizar Symantec Endpoint Protection Manager 12.1.6 MP7 a la versión 14 porque la versión del esquema de base de datos en 12.1.6 MP7 es posterior a la de 14. En cambio, es necesario actualizar 12.1.6 MP7 a 14 MP1 o posterior.
- Se ha eliminado la compatibilidad de la versión 14.0.x con Windows XP, Server 2003 y con cualquier sistema operativo Windows Embedded que esté basado en Windows XP. Symantec Endpoint Protection Manager 14.2 RU1 puede administrar estos equipos como clientes heredados de la versión 12.1.x, aunque los clientes de la versión 12.1.x son EOL. Para estos clientes, es posible que desee utilizar un producto Symantec que siga siendo compatible con estos sistemas operativos heredados como, por ejemplo, Data Center Security (DCS).
- No se admite la actualización desde 14 MP1 (14.0.2332.0100) a 14 MP1 versión actualizada (14.0.2349.0100).
- No se admiten las rutas de degradación. Por ejemplo, si desea migrar de Symantec Endpoint Protection 14.2.1.1 a 12.1.6 MP10, primero deberá desinstalar Symantec Endpoint Protection 14.2.1.
- Si tiene un número de compilación, pero no está seguro de cómo se traduce en versión de lanzamiento, consulte: Acerca de las versiones y los tipos de lanzamientos de Endpoint Protection

Sitios donde se puede obtener más información

En la siguiente tabla se incluyen los sitios web en donde poder consultar las prácticas recomendadas, la información de solución de problemas y otros recursos para ayudar a utilizar el producto.

Table 13: Información del sitio web de Endpoint Protection

Tipo de información	Vínculo del sitio web
Versiones de prueba	Póngase en contacto con el representante de cuentas.
Actualizaciones de la documentación y manuales	Página Documentos relacionados Para otros idiomas, haga clic en el menú desplegable **Español**.
Soporte técnico	Soporte técnico para Endpoint Protection Incluye los artículos de la base de conocimientos, los detalles de la versión de producto, las actualizaciones, los parches y las opciones de contacto para obtener soporte.
Información de amenazas y actualizaciones	Symantec Security Center
Aprendizaje	Education Services Acceso a los cursos de aprendizaje, eLibrary y mucho más.
Foros de Symantec Connect	Endpoint Protection


Symantec
A Division of Broadcom