Notas de la versión de Symantec™ Endpoint Protection 14.3

Última actualización: Junio de 2020

Table of Contents

Declaración de Copyright

Novedades en Symantec Endpoint Protection 14.3

En esta sección se describen las nuevas funciones de la versión 14.3.

Funciones de protección

- Los desarrolladores de aplicaciones de otros fabricantes pueden proteger a sus clientes del software malicioso dinámico basado en scripts y de otras vías no tradicionales de ciberataque.La aplicación de otro fabricante llama a la interfaz de Windows AMSI para solicitar un análisis del script proporcionado por el usuario y que se envía al cliente de Symantec Endpoint Protection. El cliente responde con un veredicto para indicar si el comportamiento del script es malicioso o no. Si el comportamiento no es malicioso, se continúa ejecutando el script. Si el comportamiento del script es malicioso, la aplicación no lo ejecutará.En el cliente de, el cuadro de diálogo Resultados de la detección muestra el estado "Acceso denegado".Algunos ejemplos de scripts de otros fabricantes son Windows PowerShell, JavaScript y VBScript. Auto-Protect se debe habilitar. Esta funcionalidad funciona con equipos con Windows 10 y versiones posteriores.
  Cómo Antimalware Scan Interface (AMSI) le ayuda a defenderse contra el software malicioso
  Antimalware Scan Interface (AMSI)

Symantec Endpoint Protection Manager

- La consola remota de Symantec Endpoint Protection ahora es compatible con Java 11 en lugar de Java 8.Para acceder a la consola remota, abra un navegador web compatible, escriba la dirección siguiente en el cuadro de dirección: `http://SEPMServer:9090/Symantec.html` y descargue el nuevo paquete de la consola remota. Siga las instrucciones que se especifican. La versión anterior de la consola remota de Symantec Endpoint Protection Manager ya no es compatible.
  Registro en Symantec Endpoint Protection
- Se puede configurar uno de los administradores de Symantec Endpoint Protection en el sitio como un servidor de registro principal para reenviar los registros al servidor de syslog. Si el servidor de registro principal se desconecta, un segundo servidor de administración toma los registros y los reenvía al servidor de syslog. Cuando el servidor de registro principal vuelve a estar en línea, reanuda el reenvío de los registros.
  Configuración de un servidor de conmutación por error para el registro externo
- La política de integraciones tiene una nueva opción para la Redirección de tráfico de WSS, **Habilitar el archivo PAC personalizado de LPS**. Esta opción permite reemplazar el archivo PAC predeterminado que aloja el servidor de LPS en el cliente con un archivo PAC personalizado. El archivo PAC personalizado soluciona incidencias de compatibilidad con aplicaciones de otros fabricantes que no funcionan con un servidor proxy local que escucha en el adaptador de loopback.

Configuración de redirección de tráfico de WSS

- Compatibilidad para la base de datos de Microsoft SQL Server 2019.
- El proceso de análisis antivirus utiliza ahora un servicio independiente del servicio principal que no es de seguridad. Este nuevo proceso de análisis proporciona un uso de memoria más eficaz, una protección continua y una menor dependencia de las incidencias con el servicio principal.
- El esquema de la base de datos incluye nuevas columnas como parte de una nueva función de una versión futura. (Tablas AGENT_SECURITY_LOG_1, AGENT_SECURITY_LOG_2 y SEM_AGENT)
- La API de REST tiene los campos siguientes en el JSON de respuesta de la API de /sepm/api/v1/computers para llamar y descargar el informe de estado del equipo: quarantineStatus, quarantineCode, wssStatus y pskVersion.
- Se han actualizado los siguientes componentes de otros fabricantes a las versiones más recientes: Apache Tomcat, Boost C++ Libraries, cURL, Jackson-core, jackson-databind, Jakarta Activation, Java, logback, Microsoft JDBC Driver for SQL Server, OpenSC, OpenSSL, Spring Security, spring-framework, sqlite.
- Para inscribir el dominio de Symantec Endpoint Protection Manager en la consola en la nube, primero se debe obtener el token de inscripción a través de la consola de Symantec Endpoint Security. Anteriormente, el token de inscripción se obtuvo haciendo clic en el botón **Introducción** en la página **Nube**.

Actualizaciones del cliente y de la plataforma

- El cliente de Windows es compatible con Windows 10 20H1 (Windows 10 versión 2004)
- El cliente de Linux ahora es compatible con Ubuntu 18.04, RHEL 8 y CentOS 8.
- La herramienta AppRemover se ha actualizado a una versión más reciente.La herramienta AppRemover elimina las aplicaciones de otros fabricantes antes de poder instalar el cliente de Windows.Para obtener más información sobre qué aplicaciones elimina, consulte: Eliminación de software de seguridad de otros fabricantes en Endpoint Protection 14.3

Funciones eliminadas

- Las siguientes notificaciones ya no muestran los campos **Gravedad del riesgo** y **Tipo de riesgo**: Ataque de riesgo, Evento de riesgo simple y Nuevo riesgo detectado.

Novedades en todas las versiones de Symantec Endpoint Protection

Problemas conocidos y soluciones alternativas

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

Table 1: Problemas de actualización

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. 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.

Table 2: Problemas de Symantec Endpoint Protection Manager

Problema	Descripción y solución
Lista blanca de direcciones URL adicionales en Symantec Endpoint Security si se utiliza la opción de administración híbrida y los servidores proxy [versión 14.2.2.1 o posterior]	Gracias a la reciente 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. Para incluir en la lista blanca las direcciones URL en agentes administrados totalmente en la nube o administrados de forma híbrida, se pueden incluir en la lista blanca de Symantec Endpoint Security: 1. En Symantec Endpoint Security, vaya a **Endpoint > Políticas > Política de la lista blanca [nombre de política]**. 2. En la política de la lista blanca, junto a **Excluido por dominio**, seleccione **Agregar**, agregue las siguientes direcciones URL de una en una y seleccione **Agregar**: `us.spoc.securitycloud.symantec.com` `eu.spoc.securitycloud.symantec.com` (agregue esta dirección URL si tiene dispositivos en Europa). Mantenga spoc.norton.com si sigue administrando clientes con una versión posterior. 3. Seleccione **Guardar política** y, a continuación, **Sí** para actualizar la política y aplicarla a los grupos existentes. Consulte Direcciones URL a la lista blanca de Symantec Endpoint Security. Consulte Actualización de los agentes de Symantec administrados en la nube a la versión 14.2 RU2 MP1 o posterior antes del 4 de mayo de 2020.
La consola remota de Symantec Endpoint Protection Manager ya no es compatible con la plataforma Windows de 32 bits [versión 14.3]	A partir de la versión 14.3, 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." Registro en Symantec Endpoint Protection Manager
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.

Problema	Descripción y solución
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.

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

Problema	Descripción y solución
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 no funciona correctamente cuando se instala en Windows 10 1803 con UWF habilitado.
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.

Problema	Descripción y solución
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.

Con el reciente anuncio de Broadcom que Symantec Enterprise Protection se ha unido oficialmente a Broadcom, Symantec ha migrado la documentación al Portal de Tech Docs de Symantec Security 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**.

Table 4: Problemas de la documentación

Problema	Descripción y solución
Los artículos explicativos (HOWTO) han caducado.	Los artículos explicativos, que eran duplicados de los temas de la ayuda de Symantec Endpoint Protection Manager, se han vuelto a publicar en el sitio de Endpoint Protection y ahora tienen una dirección URL diferente. Para encontrar un artículo, utilice el **campo de búsqueda**.
Archivos PDF	Symantec ha publicado todos los archivos PDF en los artículos de la documentación. Estas páginas han caducado. Para encontrar la versión más reciente del archivo PDF, diríjase a la página Documentos relacionados. En el futuro, Broadcom agregará los archivos PDF heredados y los archivos PDF traducidos.

Para obtener una lista de los problemas solucionados, consulte: Nuevas correcciones y componentes para Symantec Endpoint Protection 14.3

Requisitos del sistema para Symantec Endpoint Protection (SEP)

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 nombres 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 nombres específicos de la versión.

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

Table 5: Requisitos del sistema del 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 **Note:** No se admiten sistemas operativos de equipos de escritorio. **Note:** La edición Windows Server Core no se admite. Windows Server Core no incluye Internet Explorer, que Symantec Endpoint Protection Manager requiere para funcionar.
Navegador web	Los siguientes navegadores son compatibles para que la consola web acceda a Symantec Endpoint Protection Manager y para consultar la Ayuda de Symantec Endpoint Protection Manager: • Microsoft Edge Nota: Windows 10 de 32 bits no admite el acceso a la consola web en el navegador Edge. • Microsoft Internet Explorer 11 • Mozilla Firefox 5.x a 68.x • Google Chrome 75.x

Componente	Requisitos
Base de datos	**Symantec Endpoint Protection Manager incluye una base de datos integrada. 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, RTM, SP1, SP2 • SQL Server 2017, RTM • SQL Server 2019, RTM (a partir de la versión 14.3) **Note:** La base de datos de la edición SQL Server Express no se admite.Se admiten las bases de datos de SQL Server que se alojan en Amazon RDS (a partir de la versión 14.0.1 MP2). **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. Sin el parche de SQL Server que permite admitir TLS 1.2, es posible que surjan problemas al realizar la actualización de Symantec Endpoint Protection 12.1 a 14. **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.

Table 6: Requisitos de sistema del hardware de 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 ya 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	1024 x 768 o superior
Disco duro al instalar en la unidad del sistema	**Con una base de datos integrada o una base de datos de SQL Server local:** • 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
Disco duro al instalar en una unidad alternativa	**Con una base de datos integrada o una base de datos de SQL Server local:** • 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

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 use, de los requisitos de mantenimiento de base de datos y de otras configuraciones de la base de datos.

Table 7: Requisitos del sistema de software del cliente de Symantec Endpoint Protection para Windows

Componente	Requisitos
Sistema operativo (escritorio)	• Windows 7 (de 32 bits, de 64 bits, RTM y SP1) • Windows Embedded 7 Standard, POSReady y Enterprise (de 32 bits y 64 bits) • Windows 8 (de 32 bits y 64 bits) • Windows Embedded 8 Standard (de 32 y 64 bits) • Windows 8.1 (de 32 bits, 64 bits), incluyendo Windows To Go • Actualización de Windows 8.1 para abril de 2014 (de 32 bits, 64 bits) • Actualización de Windows 8.1 para agosto de 2014 (de 32 bits, 64 bits) • Windows Embedded 8.1 Pro, Industry Pro e Industry Enterprise (de 32 bits y 64 bits) • Windows 10 (versión 1507) (de 32 y 64 bits), incluyendo Windows 10 Enterprise 2015 LTSB • Actualización de noviembre de Windows 10 (versión 1511) (de 32 y 64 bits) • Actualización aniversario de Windows 10 (versión 1607) (de 32 y 64 bits), incluyendo Windows 10 Enterprise 2016 LTSB • Actualización de los creadores de Windows 10 (versión 1703) (de 32 y 64 bits) • Actualización de otoño de los creadores de Windows 10 (versión 1709) (de 32 y 64 bits) • Actualización de abril de 2018 de Windows 10 (versión 1803) (de 32 y 64 bits) • Actualización de octubre de 2018 de Windows 10 (versión 1809) (de 32 y 64 bits), incluido Windows 10 Enterprise 2019 LTSC. • Actualización de mayo de 2019 de Windows 10 (versión 1903) (de 32 y 64 bits) • Actualización de noviembre de 2019 de Windows 10 (versión 1909) (de 32 y 64 bits) (a partir de la versión 14.2 RU1 y posterior) • Windows 10 20H1 (Windows 10 versión 2004) (a partir de la versión 14.3)
Sistema operativo (servidor)	• Windows Server 2008 R2 • Windows Small Business Server 2011 • Windows Server 2012 • Windows Server 2012 R2 • Actualización de Windows Server 2012 R2 para abril de 2014 • Actualización de Windows Server 2012 R2 para agosto de 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)
Prevención contra intrusiones de navegador	La compatibilidad con la prevención contra intrusiones de navegador se basa en la versión del motor del sistema de detección de intrusiones de clientes (CIDS). Consulte Navegadores compatibles para Prevención contra intrusiones de navegador en Endpoint Protection.

Table 8: Requisitos del sistema de hardware del 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	800 x 600 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. **Requisitos del sistema para el disco duro:** • Los requisitos del sistema de unidad de disco duro disponible del cliente Symantec Endpoint Protection para Windows al instalarse en la unidad del sistema describen los requisitos del sistema del disco duro al instalarse Symantec Endpoint Protection en la unidad del sistema. • Los requisitos del sistema de unidad de disco duro disponible del cliente Symantec Endpoint Protection para Windows al instalarse en una unidad alternativa describen los requisitos del sistema del disco duro al instalarse Symantec Endpoint Protection en una unidad alternativa. **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 9: 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 10: 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 11: 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 (de 32 y 64 bits) • Windows Embedded 8.1 Industry Pro (de 32 y 64 bits) • Windows Embedded 8.1 Industry Enterprise (de 32 y 64 bits) • Windows Embedded 8.1 Pro (de 32 y 64 bits)
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 12: Requisitos del sistema del cliente de Symantec Endpoint Protection para Mac

Componente	Requisitos
Procesador	Intel Core 2 Duo de 64 bits o posterior
RAM física	2 GB de RAM
Disco duro	500 MB de espacio libre en el disco duro disponible para la instalación
Pantalla	800 x 600
Sistema operativo	• macOS 10.13 • macOS 10.14 • macOS 10.15 a 10.15.5 macOS 10.14.5 y versiones posteriores son compatibles con los requisitos de la certificación notarial de kext. Consulte Endpoint Protection 14.2 RU1 y certificación notarial de kext para macOS 10.14.5. Para obtener una lista de los sistemas operativos compatibles con las versiones anteriores, consulte: Compatibilidad de Mac con el cliente de Endpoint Protection.

Table 13: Requisitos del 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 • 7 GB de espacio libre en disco duro disponible
Sistemas operativos	• 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; 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 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 kernel de sistemas operativos compatibles de las versiones anteriores, consulte Kernel de Linux compatibles para Symantec Endpoint Protection.
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

Otros requisitos del entorno	• Glibc
	No se admiten sistemas operativos que ejecuten una versión de Glibc anterior a 2.6.
	• Paquetes dependientes basados en i686 en equipos de 64 bits
	Muchos de los archivos ejecutables del cliente de 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 distribuciones basadas en Red Hat: `sudo yum install glibc.i686 libgcc.i686 libX11.i686 libnsl.i686`
	– Para 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`
	• 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:
	Compilar manualmente los módulos del kernel Auto-Protect para Endpoint Protection para Linux

Notas de la versión y requisitos del sistema para todas las versiones de Symantec Endpoint Protection

Rutas de actualización compatibles con la última versión de Symantec Endpoint Protection 14.x

NOTE

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.

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

Symantec Endpoint Protection Manager y el cliente para 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

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
- 14.2
- 14.2 MP1
- 14.2 RU1
- 14.2 RU1 MP1
- 14.2 RU2
- 14.2 RU2 MP1

NOTE

El cliente de Symantec Endpoint Protection for Mac no se actualizó a 14.0.1 MP2.

Cliente para Linux

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

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:

- Los productos de Symantec no admitidos, Symantec AntiVirus y Symantec Client Security
- Todos los productos Norton™ de Symantec
- Symantec Endpoint Protection para Windows XP Embedded 5.1
- Versiones de Symantec Endpoint Protection for Mac anteriores a 12.1.4

No es posible actualizar Symantec Endpoint Protection Manager 11.0.x o Symantec Endpoint Protection Manager Small Business Edition 12.0.x directamente desde cualquier versión de Symantec Endpoint Protection Manager 14. Primero, debe desinstalar estas versiones o realizar una actualización a la versión 12.1.x antes de actualizar a la versión 14.

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.

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, debe desinstalar Symantec Endpoint Protection 14.2.1.1.

Si tiene un número de compilación, pero no está seguro de cómo se traduce en versión de lanzamiento, consulte:

- Versiones publicadas de Symantec Endpoint Protection
- Acerca de las versiones y los tipos de lanzamientos de Endpoint Protection

Sitios donde se puede obtener más información

Información de Endpoint Protection muestra los sitios web en donde se puede consultar las prácticas recomendadas, la información de solución de problemas y otros recursos para ayudarle a utilizar el producto.

Table 14: 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 documentación y manuales	• Guías del producto para la última versión (inglés) • Guías del producto para la última versión (otros idiomas) • Guías del producto para todas las versiones de Symantec Endpoint Protection 14.x (inglés) **Otros idiomas:**
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
Capacitación	Education Services Acceso a los cursos de formación, eLibrary y mucho más.
Foros de Symantec Connect	Endpoint Protection


Symantec
A Division of Broadcom