Notas de la versión de Symantec™ Endpoint Protection 14.3 RU1

Actualizado: Diciembre de 2020

Table of Contents

Declaración de Copyright

Novedades en Symantec Endpoint Protection 14.3 RU1?

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

Funciones de protección

- Incluye el nuevo Agente de Symantec para Mac y el nuevo Agente de Symantec para Linux que se pueden instalar y administrar desde Symantec Endpoint Protection Manager en las instalaciones o desde la consola en la nube de Integrated Cyber Defense Manager.
  Instalación del cliente de Symantec Endpoint Protection para Mac
  Instalación del Agente de Symantec para Linux 14.3 RU1
- Evita las amenazas nuevas y desconocidas en macOS supervisando casi 1400 comportamientos de archivos en tiempo real. El nuevo Agente para Mac incluye estas funcionalidades de protección del comportamiento. La protección del comportamiento, o SONAR, utiliza inteligencia artificial y aprendizaje automático avanzado para la protección de día cero para detener las nuevas amenazas con eficacia.
  Administración de SONAR
- Bloquea los archivos ejecutables no portables (PE) en los que no se puede confiar como, por ejemplo, archivos PDF y scripts que aún no se han identificado como amenazas. En la política excepciones, haga clic en **Excepciones de Windows** > **Acceso a archivos**.
- Evita las amenazas web en función de la puntuación de la reputación de una página web. La política de prevención de intrusiones incluye el filtrado de la reputación de las direcciones URL, lo que bloquea las páginas web con puntuaciones de la reputación por debajo de un umbral específico. Los puntuaciones de reputación van desde el -10 (mala) hasta el +10 (buena). La opción **Activar reputación de direcciones URL** está activada de forma predeterminada.
- Se puede forzar Symantec Endpoint Protection para que aprenda una aplicación basada en el valor hash de la aplicación. En la política de excepciones, haga clic en **Excepciones de Windows** > **Aplicación** > **Agregar una aplicación por huella digital**.
- Protege endpoints y usuarios contra ataques basados en Web en sitios maliciosos usando la función Redirección de tráfico de red. La redirección de tráfico de red redirecciona todo el tráfico de red (cualquier puerto) o solo el tráfico basado en Web (puertos 80 y 443) a Symantec Web Security Service, que permite o bloquea el tráfico de red y el acceso a las aplicaciones de SaaS en función de la política empresarial. La política de la redirección de tráfico de red tiene un nuevo método de redirección llamado método de túnel. El método de túnel redirige automáticamente todo el tráfico de Internet a Symantec WSS, en el que se permite o se bloquea el tráfico en función de las políticas de Symantec Web Security Service. El método de túnel se considera una función beta. Se debe realizar una prueba exhaustiva con las aplicaciones en las políticas de WSS. Broadcom tiene un sitio web beta que ofrece una guía de pruebas y un sitio en el que puede dejar comentarios sobre su experiencia. Inicie sesión en el siguiente sitio web con las credenciales de Broadcom: Validate.broadcom.com
  Configuración de redirección de tráfico de red
- Se ha cambiado el nombre de la política de integraciones a la política de redireccionamiento del tráfico de red.
- Proporciona compatibilidad con eventos enriquecidos con MITRE en Symantec EDR. Aprovecha el marco MITRE ATT&CK para proporcionar contexto sobre lo que sucede en el entorno.
- Proporciona compatibilidad para los siguientes eventos de Symantec EDR, que exponen más visibilidad en los endpoints:
  - Los eventos de AMSI proporcionan visibilidad de los métodos de actor de amenazas que pueden eludir los métodos de interrogación de la línea de comandos tradicionales.
  - Los eventos de ETW proporcionan visibilidad de los eventos que ocurren en puntos finales de Windows administrados.
- Incluye la capacidad de ejecutar Windows Defender y Symantec Endpoint Protection en el mismo equipo. El análisis de Auto-Protect se ejecuta después de Windows Defender y puede detectar cualquier amenaza que Windows

Defender no identifique. La opción **Coexistencia con Windows Defender** garantiza que Auto-Protect se ejecute en caso de que se deshabilite Microsoft Defender. Para deshabilitar la opción, haga clic en la ficha de la política Protección antivirus y antispyware > **Varios** > **Varios**.

- La mitigación de cadenas de ataques ahora se admite para los clientes administrados de forma híbrida.

Symantec Endpoint Protection Manager

- La base de datos integrada se ha actualizado a la base de datos de Microsoft SQL Express. La base de datos de SQL Server Express almacena las políticas y los eventos de seguridad de forma más eficiente que la base de datos integrada predeterminada y se instala automáticamente con Symantec Endpoint Protection Manager.
  Prácticas recomendadas para actualizar desde la base de datos integrada a la base de datos de Microsoft SQL Server Express
- Durante la instalación o actualización de Symantec Endpoint Protection Manager, el Asistente para la configuración del servidor de administración realiza lo siguiente:
  - Instala automáticamente el contenido de LiveUpdate.
  - Proporciona una opción para usar el certificado TLS para la comunicación segura entre SQL Server y Symantec Endpoint Protection Manager.
- LiveUpdate utiliza un nuevo motor en Symantec Endpoint Protection Manager, que se ha optimizado para ejecutarse en la consola en la nube.
  Notas de la versión del administrador de LiveUpdate y nuevas correcciones
- La opción **Desinstalar automáticamente el software de seguridad de terceros existente** que no estaba disponible en 14.3 MP1 está disponible de nuevo en 14.3 RU1 con una versión actualizada. Esta opción se utiliza para desinstalar el software de seguridad de terceros. Para acceder a esta opción, haga clic en la página **Administrador** > **Paquetes** > **Valores de configuración de instalación de clientes**.
  Eliminación de software de seguridad de terceros en Endpoint Protection 14
  Eliminación de software de seguridad de terceros en Endpoint Protection 14.3 RU1
- El Asistente de implementación del cliente que se usa para implementar los paquetes del cliente debe verificar las credenciales y debe poder conectarse a Symantec Endpoint Protection Manager. Si se produce un error en el proceso de verificación, el proceso de implementación del cliente se detiene para evitar que se bloqueen las cuentas de usuario de Active Directory.
  Instalación de clientes de Symantec Endpoint Protection con la transferencia remota
- Los registros e informes de estado del equipo ahora permiten seleccionar un intervalo para los campos **Versión del cliente** y **Versión de IPS**. Se ha cambiado el nombre del filtro **Versión del producto** a **Versión del cliente**.
- La opción **Desactivar el icono de la bandeja de notificación** está disponible para los clientes que se ejecutan en un servidor de terminal y que provocan un uso elevado de la CPU y el uso de la memoria. Ahora se puede deshabilitar el icono del área de notificación, también conocido como el icono de la bandeja del sistema, para evitar que se ejecuten varias instancias de procesos de sesión de usuario (como SmcGui.exe y ccSvcHost.exe). Esta opción se activa en **Clientes** > ficha **Políticas** > **Configuración de seguridad** > ficha **General**.
- Se ha actualizado el modo de lista blanca y lista negra para reflejar la funcionalidad de permitir y bloquear. En la página **Clientes** > ficha **Políticas** > cuadro de diálogo **Bloqueo de sistema**, las listas del archivo de aplicación han cambiado del **Modo de lista blanca** y **Modo de lista negra** al **Modo de aceptación** y **Modo de denegación**.
- En la página **Administrador** > ficha **Servidores** > **Configuración de registro externo** > **General**, la opción **Servidor de registro maestro** ha cambiado a **Servidor de registro principal**.
- El tipo de registro **Sistema** > Registro **administrativo** y el registro de **auditoría** enumera el nombre del equipo.
- Los registros del firewall del cliente se recopilan para que se obtengan menos notificaciones en la consola en la nube.
- Se ha reemplazado Oracle Java SE con OpenJDK.
- Se han actualizado los componente de otros fabricantes de JQuery a una versión más reciente.

Actualizaciones del cliente y de la plataforma

- El cliente de Windows es compatible con Windows 10 20H2 (Windows 10 versión 2009)
- El cliente de Mac es compatible con macOS 10.15.7.
- Se han movido los paquetes de instalación de clientes de Mac de versión anteriores a la carpeta Paquetes adicionales.

Funciones eliminadas

- Las opciones **Gravedad del riesgo** y **Distribución de riesgos por gravedad** se han eliminado de las notificaciones y los informes.
- La ficha **CASMA** y el comando **Analyze** se han eliminado, ya que esta funcionalidad se ha rechazado en la versión 14.3.
- El cliente de Mac ya no admite macOS 10.13.

Documentación

La ayuda de Symantec Endpoint Protection Manager ahora está en línea y se encuentra en la Guía de instalación y administración de Symantec Endpoint Protection.

Esquema de la base de datos

El esquema de la base de datos tiene los cambios siguientes.

Tabla	Cambio de columna
ALERTS	Se ha agregado la columna ENRICHED_DATA.
AGENT_BEHAVIOR_LOG1 AGENT_BEHAVIOR_LOG2 AGENT_PACKET_LOG_1 AGENT_PACKET_LOG_2 AGENT_SECURITY_LOG_1 AGENT_SECURITY_LOG_2 AGENT_SYSTEM_LOG_1 AGENT_SYSTEM_LOG_2 AGENT_TRAFFIC_LOG_1 AGENT_TRAFFIC_LOG_2 BASIC_METADATA COMMAND COMPUTER_APPLICATION ENFORCER_CLIENT_LOG_1 ENFORCER_CLIENT_LOG_2 ENFORCER_SYSTEM_LOG_1 ENFORCER_SYSTEM_LOG_2 ENFORCER_TRAFFIC_LOG_1 ENFORCER_TRAFFIC_LOG_2 IDENTITY_MAP LAN_DEVICE_DETECTED LAN_DEVICE_EXCLUDED LEGACY_AGENT LOCAL_METADATA LOG_CONFIG REPORTS SEM_APPLICATION SEM_CLIENT SEM_COMPUTER SEM_JOB SEM_SVA_CLIENT SEM_SVA_COMPUTER SERVER_ADMIN_LOG_1 SERVER_ADMIN_LOG_2 SERVER_CLIENT_LOG_1 SERVER_CLIENT_LOG_2 SERVER_ENFORCER_LOG_1 SERVER_ENFORCER_LOG_2 SERVER_POLICY_LOG_1 SERVER_POLICY_LOG_2 SERVER_SYSTEM_LOG_1 SERVER_SYSTEM_LOG_2 SYSTEM_STATE V_AGENT_BEHAVIOR_LOG V_AGENT_PACKET_LOG V_AGENT_SECURITY_LOG V_AGENT_SYSTEM_LOG V_AGENT_TRAFFIC_LOG V_DOMAINS V_ENFORCER_CLIENT_LOG V_ENFORCER_SYSTEM_LOG V_ENFORCER_TRAFFIC_LOG V_GROUPS V_LAN_DEVICE_DETECTED V_LAN_DEVICE_EXCLUDED V_SEM_COMPUTER	Se han eliminado las columnas siguientes de cada tabla: RESERVED_INT1 RESERVED_INT2 RESERVED_BIGINT1 RESERVED_BIGINT2 RESERVED_CHAR1 RESERVED_CHAR2 RESERVED_VARCHAR1 RESERVED_BINARY

Tabla	Cambio de columna
BINARY_FILE SERVER_POLICY_LOG_1 SERVER_POLICY_LOG_2 V_SERVER_POLICY_LOG	• La columna CONTENT ha cambiado su tipo de "image" a "varbinary" • Se ha agregado una columna indexada FILESTREAM_ID • Se ha agregado un índice FILESTREAM_ID • Se han eliminado las columnas siguientes: – RESERVED_INT1 – RESERVED_INT2 – RESERVED_BIGINT1 – RESERVED_BIGINT2 – RESERVED_CHAR1 – RESERVED_CHAR2 – RESERVED_VARCHAR1 – RESERVED_BINARY
INVENTORYREPORT	Se han agregado las siguientes columnas: • PRODUCTVERSIONFROM • PRODUCTVERSIONTO • IDS_VERSIONFROM • IDS_VERSIONTO
SEM_AGENT	• Se ha agregado la columna NTR_MESSAGE. • Se han eliminado las columnas siguientes: – RESERVED_INT1 – RESERVED_INT2 – RESERVED_BIGINT1 – RESERVED_BIGINT2 – RESERVED_CHAR1 – RESERVED_CHAR2 – RESERVED_VARCHAR1 – RESERVED_BINARY
SEM_AGENT_VERSION	Se han agregado las siguientes columnas: • VERSION • FORMATTED_VERSION • REFRESH_USN • AGENT_VERSION_FORMAT_REFRESH • VERSION1 • VERSION2 • VERSION3 • VERSION4
SEM_SVA	Se han eliminado las columnas siguientes: • RESERVED_INT1 • RESERVED_INT2 • RESERVED_BIGINT1 • RESERVED_BIGINT2 • RESERVED_CHAR1 • RESERVED_CHAR2 • RESERVED_VARCHAR1
V_ALERTS	Se ha agregado la columna ENRICHED_DATA.

Novedades en todas las versiones de Symantec Endpoint Protection

Problemas conocidos y soluciones alternativas para Symantec Endpoint Protection

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

Table 1: Problemas de actualización

Problema	Descripción y solución
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. 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 Se producirá un error en la instalación de SEPM si no hay conexiones de red disponibles
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`"	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. 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
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]
La función de redireccionamiento del tráfico de red 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 WSS admite a 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 omiten 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. El método de túnel se considera actualmente una función beta.
Entradas de registro de agente 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 **Dispositivos** 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 Consulte 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 [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 mensaje "Se ha producido un error al instalar Microsoft Visual C++ Runtime" al instalar Symantec Endpoint Protection Manager [14.3]	Es posible que aparezca el siguiente error al instalar Symantec Endpoint Protection Manager en Windows 2012 R2: "Se ha producido un 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.

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

Problema	Descripción y solución
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

Problema	Descripción y solución
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 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.
Microsoft Edge permite inesperadamente 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 las incidencias resueltas, consulte:

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

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:** Windows Server Core Edition no es compatible con 14.2x ni en versiones anteriores.
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: • Navegador Microsoft Edge basado en Chromium (14.3 y versiones posteriores) • Microsoft Edge Nota: 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 RTM, 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 (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 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 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) (14.2 RU1 y versiones posteriores) • Windows 10 20H1 (Windows 10 versión 2004) (14.3 y versiones posteriores) • Windows 10 20H2 (Windows 10 versión 2009) (a partir de la versión 14.3 RU1)
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) (14.2 RU1 y versiones posteriores) • Windows Server, versión 2004 • Windows Server, versión 20H2 (14.3 RU1)
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. **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	1 GB de espacio libre en el disco duro disponible para la instalación
Pantalla	800 x 600
Sistema operativo	• macOS 10.14 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. • macOS 10.15 a 10.15.7 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 • 500 MB 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.x, 7.x, 8.x • Oracle Enterprise Linux 6.x, 7.x, 8.x • Red Hat Enterprise Linux 6.x, 7.x, 8.x • SuSE Linux Enterprise Server 12.x, 15.x • Ubuntu 14.04 LTS, 16.04 LTS, 18.04 LTS, 20.04 LTS Sistemas operativos compatibles con 14.3 y versiones 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; 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 kernels de sistemas operativos compatibles con versiones anteriores, consulte la Lista de distribuciones y kernels de Linux con controladores/módulos de protección automática precompilados para Symantec Endpoint Protection para Linux 14.x.
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.

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 2.6.
	• net-tools o iproute2
	Symantec Endpoint Protection usa una de estas dos herramientas, dependiendo de cuál está instalada en el equipo.
	• OpenSSL 1.0.2k-fips o versiones posteriores
	• 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
	• 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`

Versiones de lanzamiento, notas, nuevas correcciones 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.

Versiones de lanzamiento, notas, nuevas correcciones 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. Se bloquean las actualizaciones de 12.1.6 MP9 y anteriores en la versión 14.3 RU1.
- 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 de cliente 12.1 y 11 instaladas en sistemas operativos compatibles. La excepción es el cliente de Mac anterior a la versión 12.1.4, que se debe actualizar a la versión 12.1.4 o posteriores, o desinstalarlo.

Consideraciones sobre la migración de Symantec Endpoint Protection 14

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
- 14.3, 14.3 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 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

NOTE

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

Cliente para Linux

NOTE
El agente de Symantec para Linux 14.3 RU1 detecta y desinstala el cliente Symantec Endpoint Protection anterior para Linux y, a continuación, realiza una nueva instalación. Las configuraciones antiguas no se conservarán.

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 ha actualizado para la versión 12.1.6 MP10.t
- 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

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.

Notas:

- 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

La siguiente tabla muestra los sitios web en donde 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)
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