Notas da versão do Symantec™ Endpoint Protection 14.3

Última atualização: junho de 2020

Table of Contents

Declaração de direitos autorais

O que há de novo no Symantec Endpoint Protection 14.3

Esta seção descreve os novos recursos da release 14.3.

Recursos de proteção

- Os desenvolvedores de aplicativos de terceiros podem proteger seus clientes contra malware dinâmico com base em scripts e contra caminhos não tradicionais de ataque pela internet.O aplicativo de terceiros chama a interface AMSI do Windows para solicitar uma verificação do script fornecido pelo usuário, que é roteado para o cliente do Symantec Endpoint Protection. O cliente responde com um veredito para indicar se o comportamento do script é ou não malicioso. Se o comportamento não for malicioso, a execução do script prosseguirá. Se o comportamento do script for malicioso, o aplicativo não o executará.No cliente, a caixa de diálogo de resultados da detecção exibe o status Acesso negado.Exemplos de scripts de terceiros incluem o Windows PowerShell, JavaScript e VBScript. O Auto-Protect deve estar ativado. Essa funcionalidade funciona para computadores Windows 10 e posteriores.
  Como a AMSI (Antimalware Scan Interface - Interface de Verificação de Antimalware) ajuda você a se defender contra malware
  AMSI (Antimalware Scan Interface - Interface de Verificação de Antimalware)

Symantec Endpoint Protection Manager

- O console remoto do Symantec Endpoint Protection agora oferece suporte ao Java 11 em vez do Java 8.Para acessar o console remoto, abra um navegador suportado, digite o seguinte endereço na caixa de endereço: `http://SEPMServer:9090/Symantec.html` e faça download do novo pacote do console remoto. Siga as instruções mencionadas. A versão anterior do console remoto do Symantec Endpoint Protection Manager não é mais suportada.
  Como fazer logon no Symantec Endpoint Protection
- Você pode configurar um dos gerenciadores do Symantec Endpoint Protection no site como um servidor mestre de registro em log para encaminhar os logs para o servidor Syslog. Se o servidor mestre de registro em log ficar offline, um segundo servidor de gerenciamento assumirá e encaminhará os logs para o servidor Syslog. Quando o servidor mestre de registro em log ficar online novamente, ele continuará a encaminhar os logs.
  Como configurar um servidor de failover para registro em log externo
- A política de integrações tem uma nova opção para o Redirecionamento de tráfego do WSS, **Ativar arquivo PAC personalizado do LPS**.Essa opção permite substituir o arquivo PAC (Proxy Auto Configuration - Configuração Automática de Proxy) padrão hospedado pelo servidor LPS (Local Proxy Service - Serviço de Proxy Local) no cliente por um arquivo PAC personalizado. O arquivo PAC personalizado resolve problemas de compatibilidade com aplicativos de terceiros que não funcionam com um servidor proxy local que escuta no adaptador de loopback.
  Como configurar o redirecionamento de tráfego do WSS
- Suporte ao banco de dados Microsoft SQL Server 2019.
- Agora, o processo de verificação antivírus usa um serviço separado do serviço principal não relacionado à segurança. Esse novo processo de verificação traz mais eficiência no uso da memória, proteção contínua e menos dependência de problemas com o serviço principal.
- O esquema de banco de dados inclui novas colunas como parte de um recurso para uma release futura. (tabelas AGENT_SECURITY_LOG_1, AGENT_SECURITY_LOG_2, SEM_AGENT)
- A API REST tem os seguintes campos no JSON de resposta da API /sepm/api/v1/computers para chamar e baixar o relatório Status do computador: quarantineStatus, quarantineCode, wssStatus, pskVersion.
- Os seguintes componentes de terceiros foram atualizados para versões mais novas: 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 e sqlite.
- Para registrar o domínio do Symantec Endpoint Protection Manager no console de nuvem, é necessário primeiro obter o token de registro por meio do console do Symantec Endpoint Security. Anteriormente, o token de registro era obtido clicando-se em **Introdução** na página **Nuvem**.

Atualizações de cliente e plataforma

- O cliente Windows oferece suporte ao Windows 10 20H1 (Windows 10 versão 2004)
- O cliente Linux agora oferece suporte ao Ubuntu 18.04, RHEL 8 e CentOS 8.
- A ferramenta AppRemover foi atualizada para uma versão mais recente.A ferramenta AppRemover remove os aplicativos de terceiros para que você possa instalar o cliente Windows.Para obter mais informações sobre os aplicativos que ele remove, consulte: Third-party security software removal in Endpoint Protection 14.3 (em inglês)

Recursos removidos

- As seguintes notificações não mostram mais os campos **Gravidade do risco** e **Tipo de risco** : Epidemia de risco, Evento com risco único e Novo risco detectado.

O que há de novo em todas as releases do Symantec Endpoint Protection

Problemas conhecidos e soluções alternativas

Os itens desta seção aplicam-se a esta release do Symantec Endpoint Protection.

Table 1: Problemas de upgrade

Problema	Descrição e solução
Um upgrade do SQL Server da versão 2017 para a versão 2019 falha com o modo FIPS ativado [14.3]	Talvez você veja a mensagem de erro: "The following error has occurred. An error occurred while installing extensibility feature with error message: AppContainer Creation Failed with error message NONE, state. This implementation is not part of the Windows Platform FIPS validated cryptographic algorithms." Isso ocorrerá se você tiver o Symantec Endpoint Protection Manager 14.3 ativado para FIPS e atualizar do Microsoft SQL Server 2017 para 2019. [SEP-61473] Para solucionar esse problema, desative o FIPS no nível do sistema operacional: 1. Em `C:\ProgramData\Microsoft\Windows\Menu Iniciar\Programas\Ferramentas Administrativas`, clique em **Política de Segurança Local** > **Políticas locais** > **Opções de segurança** e desative **Criptografia de sistema: usar algoritmos compatíveis com FIPS para criptografia, hash e assinatura** 2. Atualize o SQL Server versão 2017 para a versão 2019. 3. Após a atualização bem-sucedida do SQL Server, ative novamente o FIPS. O upgrade do SQL 2017 para 2019 falha com o modo FIPS ativado
Nomes personalizados podem impedir que a política de firewall seja atualizada durante um upgrade para a versão 14.2 ou posterior	Para um upgrade para o Symantec Endpoint Protection 14.2 ou posterior, as políticas de firewall não poderão incorporar as alterações para IPv6 se alguns nomes padrão forem alterados. Os nomes padrão incluem os nomes das políticas padrão e os nomes de regras padrão. Se as regras não puderem ser atualizadas durante o upgrade, as opções do IPv6 não serão exibidas. As novas políticas ou regras criadas após o upgrade não serão afetadas. Se possível, reverta todos os nomes alterados de volta ao padrão. Caso contrário, verifique se todas as regras personalizadas que você adicionou a uma política padrão não bloqueiam a comunicação IPv6 de alguma maneira. Também faça essa verificação para as novas políticas ou regras que você adicionar.

Table 2: Problemas do Symantec Endpoint Protection Manager

Problema	Descrição e solução
URLs adicionais da whitelist no Symantec Endpoint Security caso a opção de gerenciamento híbrido e os servidores proxy [14.2.2.1 ou posterior] sejam usados	Com a recente aquisição do Symantec Enterprise Security pela Broadcom, os URLs para a comunicação entre o cliente e a nuvem foram alterados na versão 14.2.2.1. [CDM-42467] Você deve atualizar os clientes para a compilação 14.2.5569.2100 da versão ou posterior na situação a seguir • Você usa o Symantec Endpoint Security para gerenciar seus clientes e políticas quando os domínios do Symantec Endpoint Protection Manager no local estão registrados no console da nuvem • Você usa servidores proxy. Os URLs da whitelist em agentes totalmente gerenciados na nuvem ou com gerenciamento híbrido podem ser adicionados à whitelist no Symantec Endpoint Security: 1. No Symantec Endpoint Security, vá para **Endpoint > Políticas > [nome da política] Política de whitelist**. 2. Na Política de whitelist, ao lado de **Excluded by Domain**, selecione **Adicionar**, adicione os seguintes URLs, um de cada vez, e selecione **Adicionar**: `us.spoc.securitycloud.symantec.com` `eu.spoc.securitycloud.symantec.com` (adicione se você tiver dispositivos na Europa). Mantenha spoc.norton.com se continuar a gerenciar clientes com uma versão mais recente. 3. Selecione **Save Policy** e **Sim** para atualizar a política e aplicá-la aos grupos existentes. Consulte URLs para a whitelist do Symantec Endpoint Security. Consulte Como fazer upgrade de agentes Symantec gerenciados na nuvem para a versão 14.2 RU2 MP1 ou posterior em 4 de maio de 2020.
O console remoto do Symantec Endpoint Protection Manager não oferece mais suporte à plataforma Windows de 32 bits [14.3]	A partir da versão 14.3, não será possível fazer logon no console remoto do Symantec Endpoint Protection Manager se uma versão de 32 bits do Windows estiver sendo executada. O Oracle Java SE Runtime Environment não oferece mais suporte às versões de 32 bits do Microsoft Windows. [SEP-61106] Se você vir a mensagem a seguir, faça logon no Symantec Endpoint Protection Manager localmente: "This version of C:\Users\Administrator\Downloads\Symantec Endpoint Protection Manager Console\bin\javaw.exe is not compatible with the version of Windows you're running. Check your computer's system information and then contact the software publisher." Como fazer logon no Symantec Endpoint Protection Manager
O erro "Failed to install Microsoft Visual C++ Runtime" é exibido durante a instalação do Symantec Endpoint Protection Manager [14.3]	O seguinte erro pode ser exibido durante a instalação do Symantec Endpoint Protection Manager no Windows 2012 R2: "Failed to install Microsoft Visual C++ Runtime" [SEP-60396] Para solucionar esse problema, ative o Windows e instale as atualizações do Windows. A atualização do Windows instala o Visual C++ 2017 redistribuível, que é um pré-requisito para a instalação do Symantec Endpoint Protection Manager 14.3 no Windows 2012 R2.
Atualizar para ativar o TLS 1.1 e o TLS 1.2 como protocolos seguros padrão no WinHTTP no Windows [14.3]	Após instalar o Symantec Endpoint Protection Manager versão 14.3 ou atualizar para essa versão, que está registrada no console na nuvem, o servidor de gerenciamento não carregará mais os logs com êxito na nuvem. No arquivo uploader.log, você poderá ver a seguinte mensagem de erro: `<SEVERE> WinHttpSendRequest: 12175: A security error occurred` Esse problema é causado pela falta de uma atualização da Microsoft que fornece suporte a TLS 1.1 e 1.2. Para resolver o problema, instale a atualização da Microsoft: KB3140245. Para obter mais informações, consulte: Atualizar para ativar o TLS 1.1 e o TLS 1.2 como protocolos seguros padrão no WinHTTP no Windows

Problema	Descrição e solução
O status "Implementação em progresso" ainda é exibido no Symantec Endpoint Protection Manager depois que o cliente recebe uma política atualizada para o Endpoint Threat Defense para AD [14.2 RU1 MP1 e posterior]	Esse comportamento é esperado. As políticas do Endpoint Threat Defense para AD 3.3 são suportadas apenas no cliente a partir da versão 14.2 RU1 MP1. Aplique uma política do Symantec Endpoint Threat Defense for Active Directory 3.3 a um grupo. Esse grupo contém alguns clientes que executam o Symantec Endpoint Protection 14.2 RU1 ou anterior. Esses clientes recebem e aplicam a política como esperado, mas o status no Symantec Endpoint Protection Manager continua a mostrar a mensagem Implementação em progresso.

Table 3: Problemas de cliente Windows, Mac e Linux

Problema	Descrição e solução
A instalação do cliente Windows do Symantec Endpoint Protection 14.3 pode falhar, a menos que você primeiro instale o suporte a SHA-2 [14.3]	Se você executar versões herdadas do sistema operacional (Windows 7 RTM ou SP1, Windows Server 2008 R2 ou R2 SP1 ou R2 SP2), será necessário ter o suporte de assinatura de código SHA-2 instalado nos dispositivos para instalar as atualizações do Windows lançadas em julho de 2019 ou depois disso. Sem o suporte a SHA-2, a instalação do cliente Windows às vezes falha. A instalação pode falhar se você instalar clientes pela primeira vez ou atualizar automaticamente a partir de uma release anterior. [SEP-61175/61403] Para obter suporte à assinatura de código SHA-2 imposta pela Microsoft, consulte: 2019 SHA-2 Code Signing Support requirement for Windows and WSUS (em inglês) A instalação do cliente Windows do Symantec Endpoint Protection 14.3 pode falhar, a menos que o suporte a SHA-2 esteja instalado
O cliente Windows do Symantec Endpoint Protection não é executado quando instalado no Windows 10 1803 com o UWF ativado [14.3]	Se o cliente do Symantec Endpoint Protection for executado no sistema operacional Windows 10 RS4 1803 de 32 bits quando o UWF (Unified Write Filter - Filtro de Gravação Unificado) estiver ativado e protegendo a unidade em que o cliente Windows estiver instalado, o cliente não será executado corretamente. Este sistema operacional Windows contém um defeito do UWF que impede que o cliente Windows seja executado. Para solucionar esse problema: • Atualize para outra versão do sistema operacional que não contenha o defeito. • Desative o UWF.Consulte: O Endpoint Protection apresenta mau funcionamento quando instalado no Windows 10 1803 com o UWF ativado
Os clientes Mac que permitem o Redirecionamento de tráfego do WSS não honram as configurações personalizadas de proxy para o LiveUpdate [14.2 RU1 MP1 e posterior]	Você configurou seus clientes Mac gerenciados para o Symantec Endpoint Protection 14.2 RU1 MP1 ou posterior usar configurações personalizadas de proxy para o LiveUpdate por meio das Configurações de comunicações externas. Depois de ativar o WTR (WSS Traffic Redirection - Redirecionamento de tráfego do WSS) para seus clientes Mac por meio da política do Symantec Endpoint Protection Manager, você descobre que o tráfego do LiveUpdate não honra mais suas configurações personalizadas de proxy. Em vez disso, o LiveUpdate tenta uma conexão direta. Para contornar esse problema, use somente configurações personalizadas de proxy para o LiveUpdate quando o redirecionamento de tráfego do WSS estiver desativado.
O Microsoft Edge, inesperadamente, permite downloads de arquivos PDF com o reforço ativado [14.2 RU1 MP1 e posterior]	Com o Reforço do aplicativo ativado no cliente do Symantec Endpoint Protection, será possível fazer o download de arquivos PDF de maneira inesperada se você usar o navegador Microsoft Edge. A prevenção do download de arquivos PDF funciona como esperado com outros navegadores. Uma correção para esse problema está planejada para uma versão futura.

Com o recente anúncio da Broadcom de que o Symantec Enterprise Protection passou a integrar a Broadcom, a Symantec migrou a documentação para o portal de documentação técnica do Symantec Security da Broadcom.

Para localizar a documentação do Endpoint Protection, clique na guia **Symantec Security Software** e clique em **Endpoint Security and Management** > **Endpoint Protection**.

Table 4: Problemas na documentação

Problema	Descrição e solução
Os artigos HOWTO expiraram.	Os artigos HOWTO, que eram duplicações dos tópicos da Ajuda do Symantec Endpoint Protection Manager, foram republicados no site do Endpoint Protection e agora têm um URL diferente. Para localizar um artigo, use o **Campo de pesquisa**.
Arquivos PDF	A Symantec publicou todos os arquivos PDF nos artigos DOC. Essas páginas expiraram. Para localizar a versão mais recente da release do arquivo PDF, vá para a página Documentos relacionados. Futuramente, a Broadcom adicionará os arquivos PDF herdados e os arquivos PDF traduzidos.

Para ver os problemas resolvidos, consulte: Novas correções e componentes do Symantec Endpoint Protection 14.3

Requisitos de sistema para o Symantec Endpoint Protection (SEP)

Em geral, os requisitos de sistema para os produtos a seguir são os mesmos dos sistemas operacionais com os quais eles são compatíveis.

> **NOTE**
> Uma versão anterior do Symantec Endpoint Protection Manager talvez não consiga gerenciar corretamente um cliente com uma versão mais recente. Podem ocorrer problemas com atualizações de conteúdo e gerenciamento de clientes.Por exemplo, o Symantec Endpoint Protection Manager 14.0.1 ou anterior não pode fornecer corretamente um cliente da versão 14.2 com seus monikers específicos da versão. O Symantec Endpoint Protection Manager para versões anteriores a 14 MP2 não pode fornecer corretamente versões de cliente posteriores a 14.0.1 com seus monikers específicos da versão.

As tabelas a seguir descrevem os requisitos de software e hardware do Symantec Endpoint Protection.

Table 5: Requisitos de sistema de software do Symantec Endpoint Protection Manager (SEPM)

Componente	Requisitos
Sistema operacional	• Windows Server 2008 R2 • Windows Server 2012 • Windows Server 2012 R2 • Windows Server 2016 • Windows Server 2019 **Note:** Os sistemas operacionais de desktop não são suportados. **Note:** O Windows Server Core Edition não é suportado. O Windows Server Core não inclui o Internet Explorer, necessário para que o Symantec Endpoint Protection Manager funcione.
Navegador	Os seguintes navegadores são compatíveis para o acesso do console web ao Symantec Endpoint Protection Manager e para exibir a Ajuda do Symantec Endpoint Protection Manager: • Microsoft Edge Nota: A versão de 32 bits do Windows 10 não suporta o acesso do console web no navegador Edge. • Microsoft Internet Explorer 11 • Mozilla Firefox da versão 5.x até a 68.x • Google Chrome 75.x

Componente	Requisitos
Banco de dados	**O Symantec Endpoint Protection Manager inclui um banco de dados interno. Em vez disso, você pode escolher um banco de dados de uma das seguintes versões do 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 da 14.3) **Note:** O banco de dados do SQL Server Express Edition não é compatível.Bancos de dados SQL Server hospedados no Amazon RDS são compatíveis (a partir da 14.0.1 MP2). **Note:** Caso o Symantec Endpoint Protection use um banco de dados SQL Server e seu ambiente use somente TLS 1.2, certifique-se de que o SQL Server seja compatível com TLS 1.2. Talvez seja necessário aplicar um patch ao SQL Server. Essa recomendação se aplica ao SQL Server 2008, 2012 e 2014. Sem o patch do SQL Server para dar suporte ao TLS 1.2, você poderá ter problemas ao fazer upgrade do Symantec Endpoint Protection 12.1 para o 14. **Note:** Suporte a TLS 1.2 para o Microsoft SQL Server
Outros requisitos ambientais	Em redes puramente IPv6, a pilha de IPv4 ainda precisa estar instalada e desabilitada. Se a pilha de IPv4 estiver desinstalada, o Symantec Endpoint Protection Manager não funcionará.

Table 6: Requisitos do sistema do hardware do Symantec Endpoint Protection Manager

Componente	Requisitos
Processador	Mínimo Intel Pentium Dual-Core ou equivalente, 8-core ou superior recomendado **Note:** Processadores Intel Itanium IA-64 não são compatíveis.
RAM físico	Mínimo de 2 GB RAM disponíveis; recomendados 8 GB ou mais **Note:** O servidor do Symantec Endpoint Protection Manager pode exigir RAM adicional, dependendo dos requisitos de RAM dos outros aplicativos já instalados. Por exemplo, se o Microsoft SQL Server estiver instalado no servidor do Symantec Endpoint Protection Manager, o servidor deverá ter um mínimo de 8 GB disponíveis.
Tela	1024 x 768 ou maior
Unidade de disco rígido ao instalar na unidade do sistema	**Com um banco de dados incorporado ou um banco de dados local do SQL Server:** • Mínimo de 40 GB disponíveis (200 GB recomendados) para o servidor de gerenciamento e o banco de dados **Com um banco de dados remoto do SQL Server:** • Mínimo de 40 GB disponíveis (o recomendado é 100 GB) para o servidor de gerenciamento • Espaço livre em disco adicional no servidor remoto para o banco de dados
Unidade de disco rígido ao instalar em uma unidade alternativa	**Com um banco de dados incorporado ou um banco de dados local do SQL Server:** • A unidade do sistema exige, no mínimo, 15 GB disponíveis (100 GB recomendados) • A unidade da instalação exige, no mínimo, 25 GB disponíveis (100 GB recomendados) **Com um banco de dados remoto do SQL Server:** • A unidade do sistema exige, no mínimo, 15 GB disponíveis (100 GB recomendados) • A unidade da instalação exige, no mínimo, 25 GB disponíveis (100 GB recomendados) • Espaço livre em disco adicional no servidor remoto para o banco de dados

Se você usa um banco de dados de SQL Server, pode precisar liberar mais espaço em disco. A quantidade e o local do espaço adicional dependem de qual unidade é usada pelo SQL Server, dos requisitos de manutenção do banco de dados e de outras configurações.

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

Componente	Requisitos
Sistema operacional (desktop)	• Windows 7 (32 bits, 64 bits, RTM e SP1) • Windows Embedded 7 Standard, POSReady e Enterprise (32 e 64 bits) • Windows 8 (32 bits, 64 bits) • Windows Embedded 8 Standard (32 e 64 bits) • Windows 8.1 (32 bits, 64 bits), incluindo Windows To Go • Windows 8.1 atualização de abril, 2014 (32 bits, 64 bits) • Windows 8.1 atualização de agosto, 2014 (32 bits, 64 bits) • Windows Embedded 8.1 Pro, Industry Pro e Industry Enterprise (32 e 64 bits) • Windows 10 (versão 1507) (32 e 64 bits), incluindo Windows 10 Enterprise 2015 LTSB • Windows 10 atualização de novembro (versão 1511) (32 e 64 bits) • Windows 10 Anniversary Update (versão 1607) (32 e 64 bits), incluindo Windows 10 Enterprise 2016 LTSB • Atualização do Windows 10 para Criadores (versão 1703) (32 bits, 64 bits) • Atualização de outono do Windows 10 para Criadores (versão 1709) (32 bits, 64 bits) • Atualização de abril de 2018 do Windows 10 (versão 1803) (32 bits, 64 bits) • Atualização de outubro de 2018 do Windows 10 (versão 1809) (32 e 64 bits), incluindo o Windows 10 Enterprise 2019 LTSC. • Atualização de maio de 2019 do Windows 10 (versão 1903) (32 e 64 bits) • Atualização de novembro de 2019 do Windows 10 (versão 1909) (32 e 64 bits) (14.2 RU1 e posterior) • Windows 10 20H1 (Windows 10 versão 2004) (a partir da 14.3)
Sistema operacional (servidor)	• Windows Server 2008 R2 • Windows Small Business Server 2011 • Windows Server 2012 • Windows Server 2012 R2 • Windows Server 2012 R2 atualização de abril, 2014 • Windows Server 2012 R2 atualização de agosto, 2014 • Windows Server 2016 • Windows Server 2019 • Windows Server, versão 1803 (Server Core) (14.2 e posterior) • Windows Server, versão 1809 (Server Core) • Windows Server, versão 1903 (Server Core) (14.2 RU1 e posterior) • Windows Server, versão 1909 (Server Core) (14.2 RU1 e posterior)
Prevenção contra intrusões no navegador	O suporte de prevenção contra intrusão no navegador tem como base a versão do mecanismo de Sistema de detecção de intrusões (CIDS, Client Intrusion Detection System) do cliente. Consulte Supported browsers for Browser Intrusion Prevention in Endpoint Protection (em inglês).

Table 8: Requisitos do sistema de hardware do cliente do Symantec Endpoint Protection para Windows

Componente	Requisitos
Processador (para computadores físicos)	• Processador de 32 bits: Intel Pentium 4 de 2 GHz ou equivalente mínimo (recomendado Intel Pentium 4 ou equivalente) • Processador de 64 bits: Pentium 4 de 2 GHz com suporte para x86-64 ou equivalente **Note:** Os processadores Itanium não são compatíveis.
Processador (para computadores virtuais)	Um soquete virtual e um núcleo por soquete com no mínimo 1 GHz (recomenda-se um soquete virtual e dois núcleos por soquete de 2 GHz) **Note:** A reserva de recurso do hipervisor deve ser ativada.
RAM físico	1 GB (2 GB recomendado) ou mais, caso exigido pelo sistema operacional
Tela	800 x 600 ou superior
Unidade de disco rígido	Os requisitos de espaço em disco dependem do tipo de cliente que você instala, da unidade em que o instala e de onde o arquivo de dados do programa reside. A pasta de dados do programa está geralmente na unidade do sistema no local padrão C:\ProgramData. O espaço livre em disco é exigido sempre na unidade do sistema, independentemente da unidade de instalação que você escolher. **Requisitos do sistema da unidade de disco rígido:** • O tópico Requisitos do sistema da unidade de disco rígido disponível do cliente Symantec Endpoint Protection para Windows quando instalado na unidade do sistema descreve os requisitos de sistema de disco rígido quando o Symantec Endpoint Protection é instalado na unidade do sistema. • O tópico Requisitos do sistema da unidade de disco rígido disponível do cliente Symantec Endpoint Protection para Windows quando instalado em uma unidade alternativa descreve os requisitos do sistema da unidade de disco rígido quando o Symantec Endpoint Protection é instalado em uma unidade alternativa. **Note:** Os requisitos de espaço são com base em sistemas de arquivos NTFS. O espaço adicional também é exigido para atualizações de conteúdo e logs.

Table 9: Requisitos do sistema da unidade de disco rígido disponível do cliente Symantec Endpoint Protection para Windows quando instalado na unidade do sistema

Tipo de cliente	Requisitos
Padrão	**Com a pasta de dados do programa situada na unidade do sistema:** • 395 MB* **Com a pasta de dados do programa situada em uma unidade alternativa:** • Unidade do sistema: 180 MB • Unidade alternativa da instalação: 350 MB
VDI/embutido	**Com a pasta de dados do programa situada na unidade do sistema:** • 245 MB* **Com a pasta de dados do programa situada em uma unidade alternativa:** • Unidade do sistema: 180 MB • Unidade alternativa da instalação: 200 MB
Rede obscura	**Com a pasta de dados do programa situada na unidade do sistema:** • 545 MB* **Com a pasta de dados do programa situada em uma unidade alternativa:** • Unidade do sistema: 180 MB • Unidade alternativa da instalação: 500 MB

*135 MB adicionais são exigidos durante a instalação.

Table 10: Requisitos do sistema da unidade de disco rígido disponível do cliente do Symantec Endpoint Protection para Windows quando instalado em uma unidade alternativa

Tipo de cliente	Requisitos
Padrão	**Com a pasta de dados do programa situada na unidade do sistema:** • Unidade do sistema: 380 MB • Unidade alternativa da instalação: 15 MB* **Com a pasta de dados do programa situada em uma unidade alternativa: **** • Unidade do sistema: 30 MB • Unidade de dados do programa: 350 MB • Unidade alternativa da instalação: 150 MB
VDI/embutido	**Com a pasta de dados do programa situada na unidade do sistema:** • Unidade do sistema: 230 MB • Unidade alternativa da instalação: 15 MB* **Com a pasta de dados do programa situada em uma unidade alternativa: **** • Unidade do sistema: 30 MB • Unidade de dados do programa: 200 MB • Unidade alternativa da instalação: 150 MB
Rede obscura	**Com a pasta de dados do programa situada na unidade do sistema:** • Unidade do sistema: 530 MB • Unidade alternativa da instalação: 15 MB* **Com a pasta de dados do programa situada em uma unidade alternativa: **** • Unidade do sistema: 30 MB • Unidade de dados do programa: 500 MB • Unidade alternativa da instalação: 150 MB

*135 MB adicionais são exigidos durante a instalação.

**Se a pasta de dados do programa for a mesma que a da unidade alternativa da instalação, adicione 15 MB à unidade de dados do programa para seu total. Contudo, o instalador ainda precisa de 150 MB disponíveis na unidade alternativa de instalação durante a instalação.

Table 11: Requisitos do sistema do cliente do Symantec Endpoint Protection para Windows Embedded

Componente	Requisitos
Processador	Intel Pentium de 1 GHz
RAM físico	256 MB **Note:** Esta figura é destinada a uma instalação do cliente incorporado ao Symantec Endpoint Protection. Se você também implementar recursos adicionais de uma solução integrada, como a EDR, será necessário ter mais RAM física.

Componente	Requisitos
Unidade de disco rígido	O cliente VDI/embutido do Symantec Endpoint Protection exige o seguinte espaço em disco rígido disponível: • Instalado na unidade do sistema: 245 MB • Instalado em uma unidade alternativa: 230 MB na unidade do sistema e 15 MB na unidade alternativa São necessários 135 MB adicionais durante a instalação. Esses números presumem que a pasta de dados do programa está na unidade do sistema. Para obter informações mais detalhadas ou requisitos para outros tipos de cliente, consulte os requisitos do sistema para clientes Windows do Symantec Endpoint Protection.
Sistema operacional Embedded	• Windows Embedded Standard 7 (32 e 64 bits) • Windows Embedded POSReady 7 (32 e 64 bits) • Windows Embedded Enterprise 7 (32 e 64 bits) • Windows Embedded 8 Standard (32 e 64 bits) • Windows Embedded 8.1 Industry Pro (32 e 64 bits) • Windows Embedded 8.1 Industry Enterprise (32 e 64 bits) • Windows Embedded 8.1 Pro (32 e 64 bits)
Componentes mínimos exigidos	• Gerenciador de filtro (FltMgr.sys) • Auxiliar de dados de desempenho (pdh.dll) • Serviço Windows Installer
Modelos	• Compatibilidade do aplicativo (padrão) • Sinalização digital • Automação industrial • IE, Media Player, RDP • Decodificador de sinais • Cliente limitado O modelo de configuração mínimo não é suportado. O Filtro de gravação avançado (EWF, Enhanced Write Filter) e o Filtro de gravação unificado (UWF, Unified Write Filter) não são suportados. O filtro de gravação recomendado é o Filtro de gravação com base em arquivo (FBWF) instalado junto com o filtro de registro.

Table 12: Requisitos do sistema do cliente Symantec Endpoint Protection para Mac

Componente	Requisitos
Processador	Intel Core 2 Duo de 64 bits ou superior
RAM físico	2 GB de RAM
Unidade de disco rígido	500 MB de espaço disponível em disco rígido para a instalação
Tela	800 x 600
Sistema operacional	• macOS 10.13 • macOS 10.14 • macOS de 10.15 a 10.15.5 macOS 10.14.5 e posteriores suportam os requisitos de recibo de autenticação kext. Consulte Endpoint Protection 14.2 RU1 and kext notarization for macOS 10.14.5 (em inglês). Para obter uma lista de sistemas operacionais suportados pelas releases anteriores, consulte Mac compatibility with the Endpoint Protection client (em inglês).

Table 13: Requisitos do sistema do cliente Symantec Endpoint Protection para Linux

Componente	Requisitos
Hardware	• Processador Intel Pentium 4 (2 GHz) ou posterior • 1 GB de RAM • 7 GB de espaço em disco rígido disponível
Sistemas operacionais	• Amazon Linux • CentOS de 6U3 a 6U9, de 7 a 7U7, 8; 32 e 64 bits • Debian 6.0.5 Squeeze, Debian 8 Jessie; 32 e 64 bits • Fedora 16, 17; 32 bits e 64 bits • Oracle Linux (OEL) 6U2, 6U4, 6U5, 6U8; 7, 7U1, 7U2, 7U3, 7U4 • Red Hat Enterprise Linux Server (RHEL) de 6U2 a 6U9, de 7 a 7U8, de 8 a 8U2 • SUSE Linux Enterprise Server (SLES) 11 SP1 - 11 SP4, 32 e 64 bits; 12, 12 SP1, 12 SP3, 64 bits • SUSE Linux Enterprise Desktop (SLED) 11 SP1 - 11 SP4, 32 e 64 bits; 12 SP3, 64 bits • Ubuntu 12.04, 14.04, 16.04, 18.04 (a partir da 14.3); 32 e 64 bits Para obter uma lista dos kernels de sistema operacional suportados pelas releases anteriores, consulte Supported Linux kernels for Symantec Endpoint Protection (em inglês).
Ambientes gráficos da área de trabalho	Você pode usar os seguintes ambientes gráficos da área de trabalho para exibir o cliente do Symantec Endpoint Protection: • KDE • Gnome • Unity

Outros requisitos ambientais	• Glibc
	Nenhum sistema operacional que execute uma versão do glibc anterior à 2.6 é compatível.
	• Pacotes dependentes com base em i686 em computadores de 64 bits
	Muitos dos arquivos executáveis no cliente Linux são programas de 32 bits. Para computadores de 64 bits, você deve instalar os pacotes dependentes com base em i686 para poder instalar o cliente Linux.
	Se ainda não instalou os pacotes dependentes com base em i686, você poderá instalá-los pela linha de comando. Essa instalação exige privilégios de superusuário, que os comandos a seguir demonstram com `sudo`:
	– Para distribuições com base em Red Hat: `sudo yum install glibc.i686 libgcc.i686 libX11.i686 libnsl.i686`
	– Para distribuições com base em Debian: `sudo apt-get install ia32-libs`
	– Para distribuições com base em Ubuntu:
	`sudo dpkg --add-architecture i386`
	`sudo apt-get update`
	`sudo apt-get install gcc-multilib libx11-6:i386`
	• net-tools ou iproute2
	O Symantec Endpoint Protection usa uma dessas duas ferramentas, dependendo do que já está instalado no computador.
	• Ferramentas de desenvolvedor
	A compilação automática e o processo de compilação manual do módulo de kernel do Auto-Protect exigem que você instale certas ferramentas de desenvolvedor. Essas ferramentas de desenvolvedor incluem gcc e os arquivos de origem e cabeçalho do kernel. Para obter detalhes sobre o que instalar e como fazer essa instalação para versões específicas do Linux, consulte: Manually compile Auto-Protect kernel modules for Endpoint Protection for Linux (em inglês)

Release notes and system requirements for all versions of Symantec Endpoint Protection (em inglês)

Caminhos de upgrade suportados para a versão mais recente do Symantec Endpoint Protection 14.x

NOTE

Geralmente, todas as versões que aparecem antes da versão mais recente do Symantec Endpoint Protection na lista são compatíveis. Contudo, você deve confirmar consultando as notas de versão para a versão específica.

Notas de versão, novas correções e requisitos do sistema para todas as versões do Endpoint Protection

cliente do Windows e Symantec Endpoint Protection Manager

As seguintes versões do Symantec Endpoint Protection Manager e do cliente Windows do Symantec Endpoint Protection podem receber upgrade diretamente da versão atual:

- 11.x e Small Business Edition 12.0 (apenas clientes Symantec Endpoint Protection em sistemas operacionais suportados)
- 12.1.x até 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 Mac

As seguintes versões do cliente do Symantec Endpoint Protection para Mac podem receber upgrade diretamente para a versão atual:

- 12.1.4 – 12.1.6 MP9
  O cliente Mac não atualizou para a versão 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

O cliente do Symantec Endpoint Protection para Mac não foi atualizado para o 14.0.1 MP2.

Cliente Linux

As seguintes versões do cliente do Symantec Endpoint Protection para Linux podem receber upgrade diretamente para a versão atual:

- 12.1.x até 12.1.6 MP9
  O cliente Linux não atualizou para a versão 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

O Symantec AntiVirus para Linux 1.0.14 é a única versão que você pode migrar diretamente para o Symantec Endpoint Protection. Você deve primeiramente desinstalar todas as outras versões do Symantec AntiVirus para Linux. Você não pode migrar um cliente gerenciado para um cliente não gerenciado.

Caminhos de upgrade incompatíveis

Não é possível migrar para o Symantec Endpoint Protection de todos os produtos da Symantec. Você deve desinstalar os seguintes produtos para instalar o cliente Symantec Endpoint Protection:

- Os produtos Symantec AntiVirus e Symantec Client Security sem suporte
- Todos os produtos Norton™ da Symantec
- Symantec Endpoint Protection para Windows XP Embedded 5.1
- Versões do Symantec Endpoint Protection para Mac anteriores à versão 12.1.4

Você não pode fazer upgrade o Symantec Endpoint Protection Manager 11.0.x ou Symantec Endpoint Protection Manager Small Business Edition 12.0.x diretamente em alguma versão do Symantec Endpoint Protection Manager 14. Para fazer o upgrade para a versão 14.x, primeiro desinstale essas versões ou faça upgrade para a versão 12.1.x.

Você não pode fazer upgrade do Symantec Endpoint Protection Manager 12.1.6 MP7 para a versão 14, pois a versão do esquema do banco de dados da versão 12.1.6 MP7 é posterior à da versão 14. Em vez disso, você deve fazer o upgrade 12.1.6 MP7 para 14 MP1 ou posterior.

Fazer upgrade da versão 14 MP1 (14.0.2332.0100) para a compilação de atualização 14 MP1 (14.0.2349.0100) não é compatível.

Os caminhos de downgrade não são suportados. Por exemplo, se você quiser migrar do Symantec Endpoint Protection 14.2.1.1 para o 12.1.6 MP10, deve primeiramente desinstalar o Symantec Endpoint Protection 14.2.1.1.

Se você tiver um número de compilação, mas não tiver certeza de como ele se traduz para a versão de liberação, consulte:

- Released versions of Symantec Endpoint Protection (em inglês)
- Sobre os tipos de release e versões do Endpoint Protection

Onde obter mais informações

Informações sobre o Endpoint Protection exibe os sites nos quais você pode obter as melhores práticas, informações sobre solução de problemas e outros recursos para ajudá-lo a usar o produto.

Table 14: Informações do site do Endpoint Protection

Tipos de informações	Link do site
Versões de teste	Entre em contato com o representante da sua conta.
Atualizações de manuais e documentação	• Product guides for the latest release (em inglês) • Guias do produto para a release mais recente (outros idiomas) • Guias do produto para todas as versões do Symantec Endpoint Protection 14.x (em inglês) **Outros idiomas:**
Suporte técnico	Endpoint Protection Technical Support (em inglês) Inclui artigos da base de conhecimento, detalhes da release do produto, atualizações, patches e opções de contato do suporte.
Informações e atualizações da ameaça	Symantec Security Center
Treinamento	Education Services Acesse os cursos de treinamento, o eLibrary e muito mais.
Fóruns do Symantec Connect	Endpoint Protection


Symantec
A Division of Broadcom