Notas da versão do Symantec™ Endpoint Protection 14.3 RU2

Updated: May 5, 2021

Table of Contents

Declaração de direitos autorais

O que há de novo no Symantec Endpoint Protection 14.3 RU2?

Esta seção descreve os novos recursos desta release.

Recursos de proteção

- Inclui proteção em tempo de execução contra ameaças sem arquivo, como macros maliciosos do Excel (XLM) e atividades que usam o WMI (Windows Management Instrumentation - Instrumentação de Gerenciamento do Windows) com nossa integração ampliada com a AMSI (Antimalware Scan Interface - Interface de Verificação Antimalware).
- A prevenção e a detecção de comportamento aprimoradas de modificação maliciosa ou remoção dos arquivos de usuário protegem contra famílias de ransomware, como Ryuk e Netwalker.
- O emulador no cliente do Symantec Endpoint Protection foi aprimorado para aumentar a detecção de famílias de malware de mineração de criptomoeda, como o LemonDuck.
- Uma **extensão do navegador** proporciona melhor proteção para o tráfego HTTP e HTTPS bidirecional do navegador Google Chrome. O cliente do Symantec Endpoint Protection impede que os usuários acessem sites maliciosos e os redireciona para uma página inicial padrão. A extensão do navegador depende do IPS. Portanto, a política de IPS deve estar ativada e atribuída ao grupo. Por padrão, a extensão do navegador é obtida por download do LiveUpdate, se o computador estiver adicionado a um domínio do Active Directory. Caso contrário, a extensão do navegador é obtida por download do Google Web Store. Ative ou desative esse conteúdo clicando em **Admin** > **Servidores** > **Editar propriedades do site** > guia **LiveUpdate** > **Tipos de conteúdo para download** > **Extensão do navegador**.
  Por padrão, o instalador do Symantec Endpoint Protection instala a extensão do navegador Google Chrome. No entanto, se desejar usar um Objeto de política de grupo do Active Directory para gerenciar extensões do Chrome, você deverá adicionar a extensão do navegador à sua lista. Consulte: Instalando a extensão do navegador Chrome para o Endpoint Protection usando o Objeto de política de grupo
  Sobre os tipos de conteúdo de que o LiveUpdate faz o download
- Capacidade dos administradores de recuperar arquivos em quarentena em clientes do SEP remoto a partir do console do Symantec Endpoint Protection Manager. Esses arquivos maliciosos podem ser usados para outras investigações e criação de área restrita. Para fazer upload do arquivo em quarentena, marque a opção **Admin** > **Domínios** > **Editar propriedades de domínio** > guia **Geral** > **Fazer upload dos arquivos em quarentena dos clientes**. Essa opção faz o upload automaticamente de todos os arquivos em quarentena dos clientes. Você pode selecionar e recuperar arquivos individuais do Log de riscos usando o comando **Fazer download do arquivo que o cliente colocou em quarentena**. O servidor de gerenciamento não oferece mais suporte a versões antigas do Servidor da quarentena central, de modo que as opções política de Proteção contra vírus e spywares > **Quarentena > Itens em quarentena** foram removidas.
  Gerenciando a quarentena para clientes Windows
- O conteúdo da IPS (Intrusion Prevention - Prevenção contra Intrusões) foi otimizado consideravelmente para reduzir o tamanho do conteúdo e melhorar a taxa de transferência da rede. Essa melhoria está disponível para todas as versões suportadas do Symantec Endpoint Protection.
- O Redirecionamento de tráfego de rede foi renomeado para Proteção de acesso à web e nuvem no Symantec Endpoint Protection Manager, cliente Windows e cliente Mac. No cliente, os usuários podem clicar em um botão **Reconnect** no menu **Proteção de acesso à web e nuvem** > **Opções**. Os usuários do cliente deverão usar essa opção se o cliente não detectar que a conexão com o Symantec WSS foi interrompida.
  Configurando a Proteção de acesso à web e nuvem

Symantec Endpoint Protection Manager

- Inclui o LiveUpdate automático para correções críticas e atualizações de segurança. A partir do SEP 14.3 RU2, os patches críticos e as correções de segurança serão entregues automaticamente aos clientes via LiveUpdate para reduzir a carga administrativa de gerenciar atualizações do agente. Esses patches incluem apenas correções críticas; novos recursos serão entregues separadamente por meio de RUs (Release Updates - Atualizações de Release).A fim

de garantir que os patches de cliente e as atualizações de produto do cliente sejam transferidos por download de um servidor do LiveUpdate para o Symantec Endpoint Protection Manager, vá para as propriedades do site e selecione **Patches de cliente** e **Atualizações de produto do cliente**. Essas opções são ativadas por padrão.

Como fazer download do conteúdo do LiveUpdate para o Symantec Endpoint Protection Manager

– Para fazer download de patches do cliente do Symantec Endpoint Protection Manager para os clientes, na política de Configurações do LiveUpdate, clique em **Config. avançadas** > **Fazer download dos patches do cliente**. A política do LiveUpdate faz o download do patch do cliente no cliente como qualquer outro conteúdo; o patch do cliente é um arquivo delta incremental.

  Instalando patches de cliente do Endpoint Protection em clientes Windows

– Para fazer download de atualizações do produto, selecione **Fazer download do conteúdo delta de um servidor do LiveUpdate quando estiver disponível**. O cliente tenta obter uma quantidade menor de conteúdo do LiveUpdate se o Symantec Endpoint Protection Manager tiver apenas conteúdo completo. Use essa opção se não desejar ativar os patches do cliente. A opção atualizações do produto garante que as compilações de patches estejam disponíveis na atualização automática. O LiveUpdate faz download de um pacote completo de instalação do cliente no servidor de gerenciamento, onde o pacote aparece na tabela **Admin** > **Pacotes de Instalação** > **Pacote de Instalação do Cliente** e no assistente da atualização automática.Essa opção está ativada por padrão. A versão do cliente não é alterada, apenas o número da compilação. Use essa opção para que o cliente receba um conteúdo menor do LiveUpdate se o servidor de gerenciamento tiver apenas conteúdo completo.

  Como fazer upgrade do software cliente com a Atualização automática

– Em releases anteriores, essas opções eram **Fazer download de patches de segurança do cliente** e **Fazer download de conteúdo menor dos patches do cliente de um servidor do LiveUpdate quando estiver disponível**. A opção **Propriedades do site** > guia **LiveUpdate** > **Tipos de conteúdo para download** > **Patches do cliente** era **Patches de segurança do cliente**.

- O assistente para configuração do servidor de gerenciamento não solicita mais as credenciais para verificar se o FILESTREAM do SQL Server está ou não ativado. Os upgrades de um banco de dados incorporado (14.3 e anteriores) ativam automaticamente o FILESTREAM. Upgrades a partir da versão 14.3 RU1/RU1 MP1 mantêm a configuração de FILESTREAM existente. O assistente solicitará as credenciais apenas se o FILESTREAM ainda não estiver ativado no banco de dados do SQL Server Express.

  Como ativar o FILESTREAM para o banco de dados do Microsoft SQL Server
- Tanto os clientes do Symantec Endpoint Protection quanto o Symantec Endpoint Protection Manager estão localizados apenas nestes cinco idiomas: inglês, francês, espanhol, português e japonês. Se você estiver usando um dos cinco idiomas suportados, nenhuma ação será necessária; é possível fazer upgrade normalmente. Você poderá fazer upgrade automaticamente do idioma do cliente para o inglês se o idioma dos clientes anteriores não estiver disponível. Caso não escolha o inglês, não será feito o upgrade do cliente com um idioma não suportado. Essa opção está desativada por padrão. Para ativar essa opção, clique na página **Clientes** > página **Pacotes de instalação**, clique em **Adicionar pacote de instalação do cliente** > **Upgrade to English if unsupported language is unavailable**. Essa opção aplica-se apenas a clientes Windows.

  Fazendo upgrade do Symantec Endpoint Protection 14.3 RU2+ para um idioma suportado
- A conscientização de local tem quatro novos critérios: o nome do host do computador, o nome do usuário e grupo, sistema operacional e se um determinado arquivo é executado no cliente.

  Como adicionar um local para um grupo
- Adição de níveis de permissão extras para acessar as APIs REST do SEPM. Antigamente, apenas os administradores de sistema podiam executar qualquer tipo de operação POST. Agora, os administradores de domínio e os administradores limitados podem monitorar a integridade de seus computadores usando a API. Os analistas do SOC podem usar ferramentas de terceiros para integração à API.
- Na página **Admin** > **Administradores** > guia **Direitos de acesso**, o comando **Permitir a edição de políticas compartilhadas** foi alterado de **Não permitir edição de políticas compartilhadas**. A caixa de seleção **Não permitir edição de políticas compartilhadas** não era marcada por padrão, o que fazia com que os administradores concedessem explicitamente permissões, em vez de negar explicitamente as permissões.
- Os componentes de terceiros a seguir foram atualizados ou adicionados: Apache Commons FileUpload, jQuery, PHP com extensões zip ativadas, drivers Microsoft para PHP para Microsoft SQL Server e OpenSSL.

Atualizações de cliente e plataforma

Cliente de Windows:

- O cliente do Symantec Endpoint Protection para cliente Windows oferece suporte ao Citrix Studio versão 2009.0.0 e Nutanix AOS 5.15 (LTS).

Cliente Mac:

- O Symantec Endpoint Protection Manager 14.3 RU2 é fornecido com a última release do cliente do Symantec Endpoint Protection para Mac 14.3 RU1 MP1. Quando o cliente Mac 14.3 RU2 estiver disponível, o LiveUpdate fará download do pacote de instalação do cliente Mac na página **Admin** > **Pacotes de instalação** > **Pacote de instalação do cliente** do Symantec Endpoint Protection Manager. Adicionando uma notificação **Novo pacote de software** à página Monitores, você receberá uma notificação quando o pacote de instalação estiver pronto. Esse recurso permite o upgrade para o último Symantec Endpoint Protection Manager mais cedo.

  NOTE
  A release do cliente do Symantec Endpoint Protection para Mac está planejada para junho de 2021.
- Quando o cliente Mac estiver disponível, ele incluirá os seguintes recursos:
  - Suportado em dispositivos com o chip Apple M1.
  - A integração do AppleScript ao cliente Mac permite criar e executar scripts do AppleScript para consultar ou controlar o cliente Mac.
  - O pacote de instalação do cliente Mac contém uma ferramenta que permite remover a compilação NLOK do cliente Mac (versão 14.3 e anteriores) do dispositivo Mac e fazer upgrade silenciosamente para uma versão mais recente do cliente Mac.
  - As melhorias de desempenho no cliente Mac incluem: taxa de transferência de rede altamente aprimorada ao usar o cliente Mac; um tamanho menor para o instalador do cliente; e uso de CPU e memória otimizado.
  - Suporte para a pesquisa Evidência de comprometimento e o comando Colocar arquivo em quarentena para correção. Esses recursos são suportados nos clientes que são gerenciados pelo console de nuvem do Symantec Endpoint Security ou pelo Symantec EDR a partir da versão 4.6.5.

Cliente Linux:

- O cliente do Symantec Endpoint Protection para Linux oferece suporte ao Debian 9 e Debian 10.
- A ferramenta de linha de comando (sav) do cliente do Symantec Endpoint Protection para Linux permite controlar e verificar o cliente Linux.
  Como importar as configurações de comunicação entre o cliente e o servidor no cliente Linux

Recursos removidos

- Suporte estendido para 12.1.x encerrado em 3 de abril de 2021.
  Fim do suporte para o Endpoint Protection 12.1
- O servidor de gerenciamento não oferece mais suporte a versões antigas do Servidor da quarentena central. As opções na página da política de Proteção contra vírus e spywares > **Quarentena > itens em quarentena** foram removidas.

Documentação

- Os arquivos de ajuda do cliente Windows foram convertidos em arquivos HTML5, que exibem um formato atualizado e as cores da Broadcom.
- É possível fazer download de arquivos PDF das notas de versão para cada release na seguinte página:
  Documentos relacionados

Esquema de banco de dados

O esquema de banco de dados apresenta as alterações a seguir.

Tabela	Alteração de coluna
HPP_APPLICATION	Adição da coluna NONPE.
Adição de uma nova tabela, REQUESTED_FILES	Adição das seguintes colunas: • ID • APP_HASH • COMMAND_ID • BINARY_FILE_ID • TIME_STAMP • USN • RETRY_COUNT • DELETED

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

Problemas conhecidos e soluções alternativas para o SEP (Symantec Endpoint Protection)

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

Table 1: Problemas de upgrade

Problema	Descrição e solução
A seguinte mensagem de erro é exibida: "Symantec Endpoint Protection version 14.3 RU2 for Win64bit is the latest package. You cannot delete it." [14.3 RU2]	Não é possível excluir o pacote de instalação do cliente quando pacotes de várias compilações são exibidos no Symantec Endpoint Protection Manager. A partir da versão 14.3 RU2, o LiveUpdate pode fazer download de vários pacotes de instalação do cliente com um número de compilação diferente, que é exibido na página **Admin** > **Pacotes de instalação** > tabela **Pacote de instalação do cliente**. [SEP-72531]
A atualização automática falhará se você usar a opção **Faça upgrade para o inglês se o idioma do cliente instalado no momento não for suportado** da versão 14.3 RU2 para fazer upgrade de clientes com um idioma não suportado para o inglês. [14.3 RU2]	Essa situação ocorre quando você faz upgrade de clientes manualmente de um idioma suportado para um idioma não suportado na versão 14.3 RU1 MP1 e anterior; por exemplo, fazer upgrade de um cliente tcheco para um cliente japonês em um sistema operacional japonês. E, em seguida, usa a opção **Faça upgrade para o inglês se o idioma do cliente instalado no momento não for suportado** para fazer upgrade do idioma não suportado para o inglês na versão 14.3 RU2. [SEP-72490] Esse problema ocorre porque o idioma do cliente usa o idioma do sistema operacional suportado (nesse caso, japonês). A atualização automática espera usar o idioma suportado, e não o inglês. Para contornar esse problema, tente executar a atualização automática novamente e desative a opção **Faça upgrade para o inglês se o idioma do cliente instalado no momento não for suportado**.
Ao exportar um pacote de instalação do cliente de um SEPM (Symantec Endpoint Protection Manager) 14.3 RU2, o seguinte aviso é exibido: "O pacote de instalação do cliente não tem conteúdo".	Isso ocorre porque a comunicação entre o Symantec Endpoint Protection Manager e o console que está sendo usado para exportar o pacote foi interrompida. "O pacote de instalação do cliente não tem conteúdo." Aviso ao exportar um pacote de instalação do Endpoint Protection Manager
Um erro é exibido durante a importação dos pacotes de instalação de cliente mais recentes em uma versão mais antiga do Symantec Endpoint Protection Manager. [14.3 RU2]	Os clientes do Symantec Endpoint Protection 14.3 RU2 não podem ser gerenciados por uma versão 14.3 RU1 MP1 ou anterior do Symantec Endpoint Protection Manager. [SEP-72292]
Um Symantec Endpoint Protection Manager em uma rede obscura faz download do conteúdo antigo do CIDS (Client Intrusion Detection System - Sistema de Detecção de Invasão de Cliente) para novos clientes, pois o LiveUpdate não é executado durante um upgrade [14.3 RU1]	Quando um Symantec Endpoint Protection Manager 14.3 RU1 não pode acessar a internet ou um servidor do LUA (LiveUpdate Administrator - Administrador do LiveUpdate), ele mantém conteúdo antigo e incompatível no cache. Esse conteúdo antigo é normalmente entregue aos novos clientes.Para atualizar o conteúdo no cache do servidor de gerenciamento, faça download manual das definições de vírus e dos arquivos .jdb do CIDS. [SEP-69125] Para certificar-se de que os clientes novos não recebam conteúdo antigo, instale manualmente um arquivo .jdb do CIDS no SEPM antes de instalar novos clientes ou fazer upgrade de clientes antigos. Fazer o download de arquivos .jdb para atualizar as definições do Endpoint Protection Manager

Problema	Descrição e solução
Não é possível fazer login no Symantec Endpoint Protection Manager (SEPM) quando a placa de interface de rede está desativada [14.3 RU1]	Se depois você instalar o Symantec Endpoint Protection Manager, não será possível fazer login no console, e a seguinte mensagem de erro será exibida: `Erro inesperado do servidor` Esse problema pode ocorrer se a placa de interface de rede do computador estiver desativada quando você instalou o SEPM, o que impede que o certificado de servidor seja gerado. [SEP-67040] Para descobrir se o SEPM foi instalado com uma placa de interface de rede desativada, verifique o certificado de servidor. Erro inesperado do servidor no logon do SEPM se ele foi instalado em um servidor sem uma NIC ativada
Quando você desinstala o SEPM e usa a opção para remover o banco de dados padrão e deixar a instância do SQL Server Express, o seguinte erro é exibido: "`Ocorreu um erro ao tentar conectar com o servidor de banco de dados` " [14.3 RU1]	Se você desinstalar o Symantec Endpoint Protection Manager e selecionar a opção **Remover somente o banco de dados e deixar a instância do SQL Server Express instalada com o SEPM**, será possível ver o seguinte erro: "`Ocorreu um erro ao tentar conectar com o servidor de banco de dados` ".Esse problema ocorre depois que você adiciona as credenciais para o usuário DBA padrão e pode estar relacionado aos privilégios do usuário. [SEP-68670] Para contornar esse problema, execute a desinstalação executando o arquivo setup.exe do SEPM e clique no botão **Remover somente o banco de dados e deixar a instância do SQL Server Express instalada com o SEPM (não recomendado)** durante a desinstalação.
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
Alguns eventos do EDR não são exibidos no cliente [14.3 RU1]	O cliente do Symantec Endpoint Protection deve ser executado no Windows 10 compilação 14393 ou posterior para coletar eventos do Rastreamento de eventos para Windows (ETW, Event Tracing for Windows) do Symantec EDR. [SEP-67175]
O recurso Redirecionamento de tráfego de rede tem algumas limitações [14.3 RU1]	• O Symantec Web Security Service é fornecido em IPv4, e não em IPv6. [SEP-68700] • O método de redirecionamento de encapsulamento: – É executado apenas no Windows 10 versão 1703 x64 e posteriores (Canal de manutenção semestral). Esse método não suporta outros sistemas operacionais Windows nem o cliente Mac. [SEP-67927] – Não suporta dispositivos com Windows 10 de 64 bits habilitados para HVCI. [SEP-67648] – Redireciona o tráfego de saída do cliente do Symantec Endpoint Protection para o WSS antes que ele seja avaliado pelo firewall do cliente ou pelas regras de reputação do URL. Esse tráfego é avaliado pelas regras de URL e pelo firewall do WSS. Por exemplo, se uma regra de firewall do cliente SEP bloquear o google.com e uma regra do WSS autorizá-lo, o cliente permitirá que os usuários acessem o site.O tráfego local de entrada para o cliente ainda é processado pelo firewall do Symantec Endpoint Protection. [SEP-67488] – O Portal cativo do WSS não está disponível para o método de encapsulamento, e o cliente ignora as credenciais do desafio.Em uma release futura, a autenticação do SAML no WSS Agent substituirá o Portal cativo e estará disponível no cliente do Symantec Endpoint Protection. – Se um computador cliente se conectar ao WSS usando o método de encapsulamento e hospedar máquinas virtuais, cada usuário convidado precisará instalar o certificado SSL fornecido no portal do WSS. – O tráfego da rede local, como do diretório principal ou da autenticação do Active Directory, não é redirecionado. – Não é compatível com o Microsoft DirectAccess VPN. Atualmente, o método de encapsulamento é considerado um recurso de release de usuários pioneiros.
Entradas duplicadas de registro do cliente após upgrade de 14.2.x para 14.3 MP1 e posterior [14.3 RU1]	O upgrade dos clientes do Symantec Endpoint Protection 14.2.x para 14.3 MP1 ou mais recente cria entradas duplicadas de registro do agente para esses clientes na página **Clientes** do Symantec Endpoint Protection Manager. Não há impacto funcional, e você pode continuar trabalhando com as novas entradas para os clientes da versão 14.3 RU1. O Symantec Endpoint Protection Manager removerá as entradas mais antigas do agente.
Permitir URLs no Symantec Endpoint Security se você usar a opção de gerenciamento híbrido, servidores proxy ou um firewall de perímetro [14.3]	Com a 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. Você permite os URLs em agentes totalmente gerenciados na nuvem ou com gerenciamento híbrido, permite seu servidor proxy e/ou firewall de perímetro. Consulte URLs que permitem que o SEP e o SES se conectem aos servidores Symantec Consulte Upgrade cloud-managed Symantec Agents to version 14.2 RU2 MP1 or later (em inglês).

Problema	Descrição e solução
O console remoto do Symantec Endpoint Protection Manager não oferece mais suporte à plataforma Windows de 32 bits [14.3]	Na versão 14.3 e posterior, não será possível fazer login 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."
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
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
Se você fizer upgrade automaticamente de um cliente com um idioma não suportado para o inglês, o cliente continuará exibindo as configurações de data para definições em inglês [14.3 RU1 e posterior]	Para contornar esse problema, desinstale o cliente legado e instale manualmente um novo pacote de instalação de cliente em inglês. Além disso, uma correção é esperada para os upgrades de clientes feitos automaticamente. [SEP-72481]

Problema	Descrição e solução
O Symantec WSS Agent autônomo bloqueia a instalação do cliente do Symantec Endpoint Protection se você instala o SEP no mesmo computador que o WSS Agent	O componente NTR (Network Traffic Redirection - Redirecionamento de Tráfego de Rede) usa os mesmos arquivos que o Symantec WSSA (WSS Agent) autônomo. O NTR é instalado por padrão no Symantec Endpoint Protection e no console de nuvem do Symantec Endpoint Security. Se o recurso NTR estiver instalado em um endpoint, o WSSA não poderá ser instalado. Da mesma forma, se o WSSA estiver instalado, o recurso NTR não será instalado. Você pode remover o recurso Redirecionamento de tráfego de rede de endpoints existentes sem precisar desinstalar o cliente inteiro usando um dos seguintes métodos: • No Symantec Endpoint Protection Manager, crie um conjunto de recursos de instalação do cliente que não inclua o NTR e aplique-o aos endpoints. Adicionar ou remover recursos em clientes existentes do Endpoint Protection • A seguinte opção de linha de comando usa o arquivo de instalação do cliente para remover o NTR: `setup.exe /s /v" REMOVE=NTR /qn"`
O pacote de instalação de atualização usado para a instalação limpa instala o conjunto de recursos padrão. [14.3 RU1 MP1 e anteriores]	Se você criar um pacote de instalação de atualização com a opção **Manter os recursos atuais do cliente ao atualizar** marcada e usá-lo para fazer uma instalação limpa, o conjunto de recursos padrão será instalado no dispositivo cliente. Se você deseja instalar um conjunto de recursos personalizados, é necessário criar um pacote de instalação separado para a instalação limpa.
Caminho de upgrade não suportado cria dispositivos duplicados no console de nuvem. [14.3 RU1]	O upgrade do seu macOS, de 10.15 para 11.0, antes do upgrade do Symantec Agent para Mac, de 14.2/14.3 para 14.3 RU1, cria dispositivos duplicados no console de nuvem. Para evitar duplicações, você deve fazer upgrade do cliente antes de fazer upgrade do sistema operacional (isto é, fazer upgrade do Symantec Agent para Mac, de 14.2/14.3 para 14.3 RU1, e depois fazer upgrade do macOS, de 10.15 para 11.0).
Mensagens incorretas no log do instalador do Symantec Agent for Linux. [14.3 RU1]	Em alguns casos, o instalador do agente registra mensagens incorretas relacionadas a uma versão do driver sem correspondência ou a uma reinicialização necessária. Essas mensagens não afetam a funcionalidade do agente.
Em um dispositivo SuSe Linux, o zypper remove os pacotes do cliente Linux do SEP ao remover o pacote "at". [14.3 RU1]	Em um dispositivo SuSe Linux, o comando "zypper remove at" remove os pacotes do cliente Linux para SEP, pois o pacote "at" é adicionado como um pacote dependente necessário e os comandos do zypper tentam remover automaticamente os pacotes "sdcss-kmod" e "sdcss-sepagent" do cliente do SEP como pacotes com dependências não utilizadas. **Solução alternativa:** Para remover o pacote "at", execute o seguinte comando: rpm -e --nodeps at
Problema de upgrade no macOS 10.15 e posteriores [14.3 MP1]	No macOS 10.15 e posteriores, o recurso **Instalar o Symantec Endpoint Protection em computadores remotos** no Assistente de Implementação de cliente falha ao fazer upgrade do cliente do Symantec Endpoint Protection a partir de versões mais antigas para a versão 14.3 MP1. **Solução alternativa:** Use o **Upgrade automático do Symantec Endpoint Protection Manager** para executar o upgrade do cliente do Symantec Endpoint Protection no macOS 10.15 e posterior.
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

Problema	Descrição e solução
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 que foram resolvidos, consulte:

Novas correções e componentes no Symantec Endpoint Protection 14.3 RU1 MP1

New fixes and components for Symantec Endpoint Protection 14.3 RU1 (em inglês)

New fixes and components for Symantec Endpoint Protection 14.3 MP1 (em inglês)

New fixes and components for Symantec Endpoint Protection 14.3 (em inglês)

Requisitos do sistema do SEP (Symantec Endpoint Protection) 14.3 RU2

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 na versão 14.2x e anteriores.
Navegador da Web	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 com base no Chromium (versão 14.3 e posteriores) • Microsoft Edge Nota: A versão de 32 bits do Windows 10 não suporta o acesso do console da Web no navegador Edge. • Microsoft Internet Explorer 11 (14.2.x e anteriores) • Mozilla Firefox 5.x até 83 • Google Chrome 87

Componente	Requisitos
Banco de dados	O Symantec Endpoint Protection Manager inclui um banco de dados padrão: • Microsoft SQL Server Express 2014 (para Windows Server 2008 R2) • Microsoft SQL Server Express 2017 • Banco de dados incorporado Sybase (apenas a versão 14.3 MP.x e anteriores) 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 SP1, SP2 • SQL Server 2017 RTM • SQL Server 2019 RTM (14.3 e posteriores) **Note:** Bancos de dados SQL Server hospedados no Amazon RDS são suportados (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 física	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 de 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 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

Componente	Requisitos
Unidade de disco rígido ao instalar em uma unidade alternativa	Com 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
Outros	Uma placa de interface de rede ativada

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 que unidade o SQL Server usa, dos requisitos de manutenção do banco de dados e de outras configurações deste.

Table 7: Requisitos do sistema de software do 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 bits, 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) (14.3 e posteriores) • Windows 10 20H2 (Windows 10 versão 2009) (a partir da 14.3 RU1)
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) • Windows Server, versão 2004 • Windows Server, versão 20H2 (14.3 RU1) Para obter uma lista dos sistemas operacionais suportados para releases anteriores, consulte: Windows compatibility with the Endpoint Protection client (em inglês) Endpoint Protection support for Windows 10 updates and Windows Server 2016 / Server 2019 (em inglês)
Prevenção contra intrusão no navegador	O suporte de prevenção contra intrusão no navegador é baseado na 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 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 suportados.
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 física	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. **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 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 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 Symantec Endpoint Protection do Windows Embedded

Componente	Requisitos
Processador	Intel Pentium de 1 GHz
RAM física	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.
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.

Componente	Requisitos
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 do Symantec Endpoint Protection para Mac

Componente	Requisitos
Processador	Intel Core 2 Duo de 64 bits ou superior Chip Apple M1 (a partir da 14.3 RU2)
RAM física	2 GB de RAM
Unidade de disco rígido	1 GB de espaço disponível em disco rígido para a instalação
Tela	800 x 600
Sistema operacional	• macOS 10.15 a 10.15.7 • macOS 11 (Big Sur) 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 do Symantec Endpoint Protection para Linux

Componente	Requisitos
Hardware	• Processador Intel Pentium 4 (2 GHz) ou posterior • 500 MB de RAM disponível (o recomendado é 4 GB de RAM) • 2 GB de espaço disponível no disco, caso `/var`, `/opt` e `/tmp` compartilhem o mesmo sistema de arquivos ou volume • 500 MB de espaço disponível no disco em cada uma (`/var`, `/opt` e `/tmp`), caso estejam em volumes diferentes
Sistemas operacionais	Sistemas operacionais suportados a partir da versão 14.3 RU1: • Amazon Linux 2 • CentOS 6, 7, 8 • Debian 9, 10 (14.3 RU2 e posterior) • Oracle Enterprise Linux 6, 7, 8 • Red Hat Enterprise Linux 6, 7, 8 • SuSE Linux Enterprise Server 12.x, 15.x • Ubuntu 14.04 LTS, 16.04 LTS, 18.04 LTS, 20.04 LTS Kernels suportados do agente Linux da Symantec (também lista as versões secundárias suportadas do sistema operacional Linux) Sistemas operacionais suportados para a versão 14.3 MP1 e anteriores: • 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 de kernels de sistemas operacionais suportados para releases anteriores, consulte List of Linux Distributions and Kernels with Precompiled Auto-Protect Drivers/Modules for Symantec Endpoint Protection for Linux 14.x (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 O Symantec Agent for Linux 14.3 RU1 não tem uma interface gráfica.

Componente	Requisitos

Outros requisitos ambientais (14.3 MP1 e anteriores)	• Glibc
	Nenhum sistema operacional que execute uma versão do glibc anterior à 2.6 é compatível.
	• net-tools ou iproute2
	O Symantec Endpoint Protection usa uma dessas duas ferramentas, dependendo do que já está instalado no computador.
	• OpenSSL 1.0.2k-fips ou posteriores
	• 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)
	• 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 baseados 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 no Red Hat: `sudo yum install glibc.i686 libgcc.i686 libX11.i686 libnsl.i686`
	– Para distribuições com base no 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`

Release versions, notes, new fixes, and system requirements for Endpoint Security and all versions of Endpoint Protection (em inglês)

Caminhos de upgrade suportados e não suportados com a versão mais recente do Symantec Endpoint Protection 14.x

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.

Release versions, notes, new fixes, and system requirements for Endpoint Security and all versions of Endpoint Protection (em inglês)

Caminhos de upgrade suportados

- O Symantec Endpoint Protection Manager versão 12.1.6 MP10 e posterior com o banco de dados incorporado é atualizado sem problemas com o banco de dados do Microsoft SQL Server Express, versão 14.3 RU1 MP1. As atualizações do 12.1.6 MP9 e anteriores para a versão 14.3 RU1 MP1 estão bloqueadas.
- O upgrade do Symantec Endpoint Protection Manager 14.x a partir do 12.1.x é realizado perfeitamente, exceto quando não houver suporte, como: Windows Server 2003, sistemas operacionais de computador e sistemas operacionais de 32 bits, bem como algumas versões do SQL Server.
- O upgrade do cliente do Symantec Endpoint Protection 14.x é realizado perfeitamente a partir de todas as versões do cliente anteriores a 12.1 e 11 instaladas em sistemas operacionais suportados. A exceção é o cliente Mac anterior ao 12.1.4, cujo upgrade deve ser feito para a versão 12.1.4 ou posteriores, ou deve ser desinstalado.

Symantec Endpoint Protection 14 Migration Considerations (em inglês)

Symantec Endpoint Protection Managercliente Windows e

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
- 14.3, 14.3 MP1
- 14.3 RU1
- 14.3 RU1 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 RU1 MP2

O cliente do Symantec Endpoint Protection para Mac não foi atualizado para o 14.0.1 MP2.
- 14.2, 14.2 MP1
- 14.2 RU1, 14.2 RU1 MP1
- 14.2 RU2, 14.2 RU2 MP1
- 14.3, 14.3 MP1
- 14.3 RU1
- 14.3 RU1 MP1 (disponível em junho de 2021)

Cliente Linux

> **NOTE**
> O Symantec Agent for Linux 14.3 RU1 detecta e desinstala o cliente antigo do Symantec Endpoint Protection para Linux e, em seguida, executa uma nova instalação. As configurações antigas não serão mantidas.

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
- 14.3, 14.3 MP1
- 14.3 RU1
- 14.3 RU1 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 não suportados

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

- Symantec AntiVirus e Symantec Client Security, que não são suportados.
- Todos os produtos Norton da Symantec
- Symantec Endpoint Protection para Windows XP Embedded 5.1
- Qualquer Symantec Endpoint Protection para cliente Mac anterior a 12.1.4.Ou você pode fazer upgrade para 12.1.4 ou posteriores.

Observações:

- Qualquer migração de cliente do Symantec Endpoint Protection para uma versão anterior à 12.1.x não é suportada.
- Não é possível fazer upgrade do Symantec Endpoint Protection Manager 11.0.x ou do Symantec Endpoint Protection Manager Small Business Edition 12.0.x diretamente para qualquer versão do Symantec Endpoint Protection Manager 14. É preciso desinstalar essas versões ou executar um upgrade para a versão 12.1.x antes de fazer um upgrade para a release 14.x mais recente.
- 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 upgrade da versão 12.1.6 MP7 para a 14 MP1 ou posterior.
- A versão 14.0.x removeu o suporte para Windows XP, Server 2003 e qualquer sistema operacional Windows Embedded com base no Windows XP. O Symantec Endpoint Protection Manager 14.2 RU1 pode gerenciar esses

computadores como clientes 12.1.x legados, embora os clientes 12.1.x sejam EOL. Para esses clientes, convém usar um produto da Symantec que ainda suporte esses sistemas operacionais legados, como o Data Center Security (DCS).

- Fazer upgrade da versão 14 MP1 (14.0.2332.0100) para a compilação de atualização 14 MP1 (14.0.2349.0100) não é suportado.
- Os caminhos de downgrade não são suportados. Por exemplo, se quiser migrar do Symantec Endpoint Protection 14.2.1.1 para o 12.1.6 MP10, primeiramente, você deve desinstalar o Symantec Endpoint Protection 14.2.1.
- Se você tiver um número de compilação, mas não tiver certeza de como ele se traduz para a versão de liberação, consulte:
  Sobre os tipos de release e versões do Endpoint Protection

Onde obter mais informações

A tabela abaixo exibe os sites nos quais você pode obter as melhores práticas, informações adicionais e outros recursos para ajudá-lo a usar o produto.

Table 14: Informações do site do Endpoint Protection

Tipos de informações	Link do Web 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)
Suporte técnico	Endpoint Protection Technical Support (em inglês) Inclui artigos da base de conhecimento, detalhes de 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