



Notas da versão do Symantec[™] Endpoint Protection 14.3 RU1

Atualizado: dezembro de 2020

Table of Contents

Declaração de direitos autorais.....	3
O que há de novo no Symantec Endpoint Protection 14.3 RU1?.....	4
Problemas conhecidos e soluções alternativas para o Symantec Endpoint Protection.....	9
Requisitos de sistema para o Symantec Endpoint Protection (SEP).....	15
Caminhos de upgrade suportados e não suportados com a versão mais recente do Symantec Endpoint Protection 14.x.....	24
Onde obter mais informações.....	27

Declaração de direitos autorais

Declaração de direitos autorais

Broadcom, o logotipo pulse, Connecting everything e Symantec estão entre as marcas comerciais da Broadcom.

Copyright ©2020 Broadcom. Todos os direitos reservados.

O termo "Broadcom" refere-se à Broadcom Inc. e/ou a suas subsidiárias. Para obter mais informações, visite www.broadcom.com.

A Broadcom reserva-se o direito de fazer mudanças sem aviso prévio em quaisquer produtos ou dados contidos aqui para melhorar a confiabilidade, a função ou o design. As informações fornecidas pela Broadcom são consideradas exatas e confiáveis. Porém, o Broadcom não assume nenhuma responsabilidade decorrente da aplicação ou do uso dessas informações, nem da aplicação ou do uso de qualquer produto ou circuito aqui descrito, nem concede nenhuma licença sob seus direitos de patente nem os direitos de outros.

O que há de novo no Symantec Endpoint Protection 14.3 RU1?

Esta seção descreve os novos recursos desta release.

Recursos de proteção

- Inclui o novo Symantec Mac Agent e o Symantec Linux Agent, os quais podem ser instalados e gerenciados pelo Symantec Endpoint Protection Manager local ou pelo console de nuvem do gerenciador da defesa cibernética integrada.
[Como instalar o cliente do Symantec Endpoint Protection para Mac](#)
[Como instalar o Symantec Agent for Linux 14.3 RU1](#)
- Impede ameaças novas e desconhecidas no macOS monitorando quase 1.400 comportamentos de arquivo em tempo real. O novo agente Mac inclui esses recursos de proteção comportamental. A proteção comportamental, ou SONAR, usa inteligência artificial e aprendizado de máquina avançado para proteção de dia zero com o intuito de barrar novas ameaças.
[Como gerenciar o SONAR](#)
- Bloqueia arquivos não PE (Portable Executable - Portáteis Executáveis) não confiáveis, como arquivos PDF e scripts que ainda não foram identificados como uma ameaça. Na Política de exceções, clique em **Exceções do Windows > Acesso ao arquivo**.
- Impede as ameaças da web com base na pontuação de reputação de uma página da web. A política de Prevenção contra intrusões inclui a filtragem de reputação de URL, que bloqueia as páginas da web com pontuações de reputação abaixo de um limite específico. As pontuações de reputação variam de -10 (ruim) a +10 (boa). A opção **Ativar a reputação do URL** está ativada por padrão.
- Você pode forçar o Symantec Endpoint Protection a reconhecer um aplicativo com base no valor de hash do aplicativo. Na Política de exceções, clique em **Exceções do Windows > Aplicativo > Adicionar um aplicativo por impressão digital**.
- Protege os endpoints e os usuários contra ataques provenientes da web em sites maliciosos usando o recurso de Redirecionamento de tráfego de rede. O Redirecionamento de tráfego de rede redireciona todo o tráfego de rede (qualquer porta) ou apenas tráfego da web (portas 80 e 443) para o serviço Symantec Web Security Service, que permite ou bloqueia o tráfego de rede e o acesso a aplicativos SaaS com base na política corporativa. A política de Redirecionamento de tráfego de rede tem um novo método de redirecionamento chamado método de encapsulamento. O método de encapsulamento redireciona automaticamente todo o tráfego da internet para o Symantec WSS, no qual o tráfego é permitido ou bloqueado com base nas políticas do Symantec Web Security Service. O método de encapsulamento é considerado um recurso beta. Você deve executar testes completos com seus aplicativos em relação às políticas do WSS. A Broadcom tem um site beta que oferece um guia de testes e um local para deixar comentários sobre sua experiência. Faça login no seguinte site usando suas credenciais da Broadcom: [Validate.broadcom.com](https://validate.broadcom.com).
[Como configurar o Redirecionamento de tráfego de rede](#)
- A política de Integrações foi renomeada para política de Redirecionamento de tráfego de rede.
- Oferece suporte a eventos aprimorados pelo MITRE no Symantec EDR. Aproveite a estrutura do MITRE ATT&CK para fornecer contexto sobre o que está acontecendo em seu ambiente.
- Fornece suporte aos seguintes eventos do Symantec EDR, que expõem mais visibilidade dos endpoints:
 - Os eventos AMSI fornecem visibilidade dos métodos de agente de ameaças que podem enganar os métodos tradicionais de interrogação de linha de comando.
 - Os eventos ETW fornecem visibilidade dos eventos que ocorrem em endpoints gerenciados do Windows.
- Inclui a capacidade de executar o Windows Defender e o Symantec Endpoint Protection no mesmo computador. A verificação do Auto-Protect é executada após o Windows Defender e pode detectar as ameaças que o Windows Defender não tem. A opção **Coexistir com o Windows Defender** assegura que o Auto-Protect seja executado caso

o Microsoft Defender seja desativado. Para desativar a opção, clique na guia Política de proteção contra vírus e spyware > **Diversos** > guia **Diversos**.

- A mitigação da cadeia de ataque agora é suportada para clientes gerenciados de forma híbrida.

Symantec Endpoint Protection Manager

- O banco de dados incorporado foi atualizado para o banco de dados do Microsoft SQL Express. O banco de dados do SQL Server Express armazena políticas e eventos de segurança de modo mais eficiente do que o banco de dados incorporado padrão e é instalado automaticamente com o Symantec Endpoint Protection Manager.

[Melhores práticas de upgrade do banco de dados incorporado para o banco de dados do Microsoft SQL Server Express](#)

- Durante a instalação ou o upgrade do Symantec Endpoint Protection Manager, o Assistente para configuração do servidor de gerenciamento:
 - Instala automaticamente o conteúdo do LiveUpdate.
 - Fornece uma opção para usar o certificado TLS para comunicação segura entre o SQL Server e o Symantec Endpoint Protection Manager.
- O LiveUpdate usa um novo mecanismo no Symantec Endpoint Protection Manager, que é otimizado para execução no console de nuvem.
- A opção **Desinstalar automaticamente o software de segurança de terceiros existente** que não estava disponível na versão 14.3 MP1 está disponível novamente na 14.3 RU1 com uma versão atualizada. Essa opção é usada para desinstalar software de segurança de terceiros. Para acessar essa opção, clique na página **Admin > Pacotes > Configurações de instalação do cliente**.

[LiveUpdate Administrator release notes and new fixes](#) (em inglês)

[Remoção de software de segurança de terceiros no Endpoint Protection 14](#)

- [Remoção de software de segurança de terceiros no Endpoint Protection 14.3 RU1](#)
- O Assistente de Implementação de Cliente, que é usado para implementar os pacotes de cliente, deve ter suas credenciais verificadas e capazes de se conectar ao Symantec Endpoint Protection Manager. Se o processo de verificação falhar, o processo de implementação do cliente será interrompido para evitar que as contas de usuário do Active Directory sejam bloqueadas.

[Como instalar clientes do Symantec Endpoint Protection com instalação remota por envio](#)

- Agora, os logs e relatórios de Status do computador permitem selecionar um intervalo para os campos **Versão do cliente** e **Versão do IPS**. O filtro **Versão do produto** foi renomeado para **Versão do cliente**.
- A opção **Disable the notification tray icon** está disponível para clientes que são executados em um servidor de terminal e que causam alta utilização da CPU e uso da memória. Agora, é possível desativar o ícone da área de notificação, também conhecido como ícone da bandeja do sistema, de modo a evitar que várias instâncias de processos de sessão de usuário (como SmcGui.exe e ccSvcHost.exe) sejam executadas. Essa opção é ativada em **Clientes > guia Políticas > Configurações de segurança > guia Geral**.
- Atualizado o modo de lista branca e negra para refletir a funcionalidade de permissão e bloqueio. Na página **Clientes > guia Políticas > caixa de diálogo Bloqueio do sistema**, as listas de arquivo de aplicativo mudaram de **Modo de whitelist** e **Modo de blacklist** para **Modo permitir** e **Modo de negação**.
- Na página **Admin**, guia > **Servidores > Configurar registro em log externo > guia Geral**, a opção **Master Logging Server** foi alterada para **Servidor principal de registro em log**.
- O tipo de log de **Sistema > log Administrativo** e log de **Auditoria** lista o nome do computador.
- Os logs do firewall do cliente são coletados para que você receba menos notificações no console de nuvem.
- Substituição do Oracle Java SE pelo OpenJDK.
- Atualização do JQuery de componentes de terceiros para uma versão mais recente.

Atualizações de cliente e plataforma

- O cliente Windows suporta o Windows 10 20H2 (Windows 10 versão 2009).
- O cliente Mac suporta o macOS versão 10.15.7.
- Movidos os pacotes de instalação do cliente Mac herdados para a pasta Additional Packages.

Recursos removidos

- As opções **Gravidade do risco** e **Distribuição de riscos por gravidade** foram removidas das notificações e dos relatórios.
- A guia **CASMA** e o comando **Analyze** foram removidos, pois essa funcionalidade se tornou obsoleta na versão 14.3.
- O cliente Mac não oferece mais suporte ao macOS 10.13.

Documentação

A ajuda do Symantec Endpoint Protection Manager agora está online e localizada no: [Guia de Instalação e Administração do Symantec Endpoint Protection](#)

Esquema de banco de dados

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

Tabela	Alteração de coluna
ALERTS	Adição da coluna ENRICHED_DATA.
AGENT_BEHAVIOR_LOG1 AGENT_BEHAVIOR_LOG2 AGENT_PACKET_LOG_1 AGENT_PACKET_LOG_2 AGENT_SECURITY_LOG_1 AGENT_SECURITY_LOG_2 AGENT_SYSTEM_LOG_1 AGENT_SYSTEM_LOG_2 AGENT_TRAFFIC_LOG_1 AGENT_TRAFFIC_LOG_2 BASIC_METADATA COMMAND COMPUTER_APPLICATION ENFORCER_CLIENT_LOG_1 ENFORCER_CLIENT_LOG_2 ENFORCER_SYSTEM_LOG_1 ENFORCER_SYSTEM_LOG_2 ENFORCER_TRAFFIC_LOG_1 ENFORCER_TRAFFIC_LOG_2 IDENTITY_MAP LAN_DEVICE_DETECTED LAN_DEVICE_EXCLUDED LEGACY_AGENT LOCAL_METADATA LOG_CONFIG REPORTS SEM_APPLICATION SEM_CLIENT SEM_COMPUTER SEM_JOB SEM_SVA_CLIENT SEM_SVA_COMPUTER SERVER_ADMIN_LOG_1 SERVER_ADMIN_LOG_2 SERVER_CLIENT_LOG_1 SERVER_CLIENT_LOG_2 SERVER_ENFORCER_LOG_1 SERVER_ENFORCER_LOG_2 SERVER_POLICY_LOG_1 SERVER_POLICY_LOG_2 SERVER_SYSTEM_LOG_1 SERVER_SYSTEM_LOG_2 SYSTEM_STATE V_AGENT_BEHAVIOR_LOG V_AGENT_PACKET_LOG V_AGENT_SECURITY_LOG V_AGENT_SYSTEM_LOG V_AGENT_TRAFFIC_LOG V_DOMAINS V_ENFORCER_CLIENT_LOG V_ENFORCER_SYSTEM_LOG V_ENFORCER_TRAFFIC_LOG V_GROUPS V_LAN_DEVICE_DETECTED V_LAN_DEVICE_EXCLUDED V_SEM_COMPUTER	Removidas as colunas a seguir de cada tabela: RESERVED_INT1 RESERVED_INT2 RESERVED_BIGINT1 RESERVED_BIGINT2 RESERVED_CHAR1 RESERVED_CHAR2 RESERVED_VARCHAR1 RESERVED_BINARY

Tabela	Alteração de coluna
BINARY_FILE SERVER_POLICY_LOG_1 SERVER_POLICY_LOG_2 V_SERVER_POLICY_LOG	<ul style="list-style-type: none"> • A coluna CONTENT alterou seu tipo de "image" para "varbinary" • Adição de uma coluna indexada FILESTREAM_ID • Adição de um índice FILESTREAM_ID • Remoção das seguintes colunas: <ul style="list-style-type: none"> – RESERVED_INT1 – RESERVED_INT2 – RESERVED_BIGINT1 – RESERVED_BIGINT2 – RESERVED_CHAR1 – RESERVED_CHAR2 – RESERVED_VARCHAR1 – RESERVED_BINARY
INVENTORYREPORT	Adição das seguintes colunas: <ul style="list-style-type: none"> • PRODUCTVERSIONFROM • PRODUCTVERSIONTO • IDS_VERSIONFROM • IDS_VERSIONTO
SEM_AGENT	<ul style="list-style-type: none"> • Adição da coluna NTR_MESSAGE. • Remoção das seguintes colunas: <ul style="list-style-type: none"> – RESERVED_INT1 – RESERVED_INT2 – RESERVED_BIGINT1 – RESERVED_BIGINT2 – RESERVED_CHAR1 – RESERVED_CHAR2 – RESERVED_VARCHAR1 – RESERVED_BINARY
SEM_AGENT_VERSION	Adição das seguintes colunas: <ul style="list-style-type: none"> • VERSION • FORMATTED_VERSION • REFRESH_USN • AGENT_VERSION_FORMAT_REFRESH • VERSION1 • VERSION2 • VERSION3 • VERSION4
SEM_SVA	Remoção das seguintes colunas: <ul style="list-style-type: none"> • RESERVED_INT1 • RESERVED_INT2 • RESERVED_BIGINT1 • RESERVED_BIGINT2 • RESERVED_CHAR1 • RESERVED_CHAR2 • RESERVED_VARCHAR1
V_ALERTS	Adição da coluna ENRICHED_DATA.

[O que há de novo em todas as releases do Symantec Endpoint Protection](#)

Problemas conhecidos e soluções alternativas para o Symantec Endpoint Protection

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

Table 1: Problemas de upgrade

Problema	Descrição e solução
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
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. Consulte: SEPM install will fail if no network connections are available
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".	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.

Problema	Descrição e solução
Um upgrade do SQL Server da versão 2017 para a versão 2019 falha com o modo FIPS ativado [14.3]	<p>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]</p> <p>Para solucionar esse problema, desative o FIPS no nível do sistema operacional:</p> <ol style="list-style-type: none"> 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. <p>O upgrade do SQL 2017 para 2019 falha com o modo FIPS ativado</p>
Nomes personalizados podem impedir que a política de firewall seja atualizada durante um upgrade para a versão 14.2 ou posterior	<p>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.</p> <p>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.</p>

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]	<ul style="list-style-type: none"> • O Symantec Web Security Service é fornecido em IPv4, e não em IPv6. [SEP-68700] • O método de redirecionamento de encapsulamento: <ul style="list-style-type: none"> – 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 do SEP bloquear google.com e uma regra do WSS permitir google.com, o cliente permitirá que os usuários acessem google.com. O tráfego local de entrada para o cliente continua sendo 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. <p>No momento, o método de encapsulamento é considerado um recurso beta.</p>
Duplicação de entradas de registro do agente após upgrade de 14.2.x para 14.3 MP1 e versões posteriores [14.3 RU1]	O upgrade dos clientes do Symantec Endpoint Protection 14.2.x para 14.3 MP1 e versões posteriores cria entradas duplicadas de registro do agente para esses clientes na página Dispositivos 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 <ul style="list-style-type: none"> • 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. <p>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).</p>

Problema	Descrição e solução
O console remoto do Symantec Endpoint Protection Manager não suporta mais a 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 login 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> WinHttpRequest: 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
Mensagens incorretas no log do instalador do Symantec Agent para 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 para 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	Descrição e solução
Problema de upgrade no macOS 10.15 e posteriores [14.3 MP1]	<p>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.</p> <p>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.</p>
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]	<p>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]</p> <p>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)</p> <p>A instalação do cliente Windows do Symantec Endpoint Protection 14.3 pode falhar, a menos que o suporte a SHA-2 esteja instalado</p>
O cliente Windows do Symantec Endpoint Protection não é executado quando instalado no Windows 10 1803 com o UWF ativado [14.3]	<p>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.</p> <p>Para solucionar esse problema:</p> <ul style="list-style-type: none"> • Faça upgrade para outra versão do sistema operacional que não contenha o defeito. • Desative o UWF. Consulte: Endpoint Protection is malfunctioning when installed on Windows 10 1803 with UWF enabled (em inglês)
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]	<p>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.</p> <p>Para contornar esse problema, use somente configurações personalizadas de proxy para o LiveUpdate quando o redirecionamento de tráfego do WSS estiver desativado.</p>
O Microsoft Edge, inesperadamente, permite downloads de arquivos PDF com o Hardening ativado [14.2 RU1 MP1 e posteriores]	<p>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.</p> <p>Uma correção para esse problema está planejada para uma versão futura.</p>

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:

[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 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 anteriores não podem 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	<ul style="list-style-type: none"> • Windows Server 2008 R2 • Windows Server 2012 • Windows Server 2012 R2 • Windows Server 2016 • Windows Server 2019 <p>Note: Os sistemas operacionais de desktop não são suportados.</p> <p>Note: O Windows Server Core Edition não é suportado na versão 14.2x e anteriores.</p>
Navegador	<p>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:</p> <ul style="list-style-type: none"> • Microsoft Edge com base no Chromium (versão 14.3 e posteriores) • Microsoft Edge <p>Nota: A versão de 32 bits do Windows 10 não suporta o acesso do console web no navegador Edge.</p> <ul style="list-style-type: none"> • Microsoft Internet Explorer 11 (14.2.x e anteriores) • Mozilla Firefox 5.x até 83 • Google Chrome 87

Componente	Requisitos
Banco de dados	<p>O Symantec Endpoint Protection Manager inclui um banco de dados padrão:</p> <ul style="list-style-type: none"> • 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) <p>Em vez disso, você pode escolher um banco de dados de uma das seguintes versões do Microsoft SQL Server:</p> <ul style="list-style-type: none"> • SQL Server 2008 SP4 • SQL Server 2008 R2, SP3 • SQL Server 2012 RTM - SP4 • SQL Server 2014 RTM - SP3 • SQL Server 2016 RTM, SP1, SP2 • SQL Server 2017 RTM • SQL Server 2019 RTM (14.3 e posteriores) <p>Note: Bancos de dados SQL Server hospedados no Amazon RDS são suportados (a partir da 14.0.1 MP2).</p> <p>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.</p> <p>Note: Suporte a TLS 1.2 para o Microsoft SQL Server</p>
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 suportados.
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 local do SQL Server: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none">• 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: <ul style="list-style-type: none">• 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 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)	<ul style="list-style-type: none"> • 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 LTSC • 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 LTSC • 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 posteriores) • 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)	<ul style="list-style-type: none"> • 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 posteriores) • Windows Server, versão 2004 • Windows Server, versão 20H2 (14.3 RU1)
Prevenção contra intrusões no navegador	<p>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.</p> <p>Consulte Supported browsers for Browser Intrusion Prevention in Endpoint Protection (em inglês)</p>

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

Componente	Requisitos
Processador (para computadores físicos)	<ul style="list-style-type: none"> 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 <p>Note: Os processadores Itanium não são compatíveis.</p>
Processador (para computadores virtuais)	<p>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)</p> <p>Note: A reserva de recurso do hipervisor deve ser ativada.</p>
RAM físico	1 GB (2 GB recomendado) ou mais, caso exigido pelo sistema operacional
Tela	800 x 600 ou superior
Unidade de disco rígido	<p>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.</p> <p>O espaço livre em disco é exigido sempre na unidade do sistema, independentemente da unidade de instalação que você escolher.</p> <p>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.</p>

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	<p>Com a pasta de dados do programa situada na unidade do sistema:</p> <ul style="list-style-type: none"> 395 MB* <p>Com a pasta de dados do programa situada em uma unidade alternativa:</p> <ul style="list-style-type: none"> Unidade do sistema: 180 MB Unidade alternativa da instalação: 350 MB
VDI/embutido	<p>Com a pasta de dados do programa situada na unidade do sistema:</p> <ul style="list-style-type: none"> 245 MB* <p>Com a pasta de dados do programa situada em uma unidade alternativa:</p> <ul style="list-style-type: none"> Unidade do sistema: 180 MB Unidade alternativa da instalação: 200 MB
Rede obscura	<p>Com a pasta de dados do programa situada na unidade do sistema:</p> <ul style="list-style-type: none"> 545 MB* <p>Com a pasta de dados do programa situada em uma unidade alternativa:</p> <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> • Unidade do sistema: 380 MB • Unidade alternativa da instalação: 15 MB* Com a pasta de dados do programa situada em uma unidade alternativa: ** <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • Unidade do sistema: 230 MB • Unidade alternativa da instalação: 15 MB* Com a pasta de dados do programa situada em uma unidade alternativa: ** <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • Unidade do sistema: 530 MB • Unidade alternativa da instalação: 15 MB* Com a pasta de dados do programa situada em uma unidade alternativa: ** <ul style="list-style-type: none"> • 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.
Unidade de disco rígido	O cliente VDI/embutido do Symantec Endpoint Protection exige o seguinte espaço em disco rígido disponível: <ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Gerenciador de filtro (FitMgr.sys) Auxiliar de dados de desempenho (pdh.dll) Serviço Windows Installer
Modelos	<ul style="list-style-type: none"> Compatibilidade do aplicativo (padrão) Sinalização digital Automação industrial IE, Media Player, RDP Decodificador de sinais Cliente limitado <p>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.</p>

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	1 GB de espaço disponível em disco rígido para a instalação
Tela	800 x 600
Sistema operacional	<ul style="list-style-type: none"> macOS 10.14 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). macOS 10.15 a 10.15.7 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	<ul style="list-style-type: none"> • Processador Intel Pentium 4 (2 GHz) ou posterior • 500 MB de RAM • 2 GB de espaço disponível em disco, se /var, /opt e /tmp compartilharem o mesmo sistema de arquivos/volume • 500 MB de espaço em disco disponível em cada/var,/opt e /tmp se estiverem em volumes diferentes
Sistemas operacionais	<p>Sistemas operacionais suportados a partir da versão 14.3 RU1:</p> <ul style="list-style-type: none"> • Amazon Linux 2 • CentOS 6.x, 7.x, 8.x • Oracle Enterprise Linux 6.x, 7.x, 8.x • Red Hat Enterprise Linux 6.x, 7.x, 8.x • SuSE Linux Enterprise Server 12.x, 15.x • Ubuntu 14.04 LTS, 16.04 LTS, 18.04 LTS, 20.04 LTS <p>Sistemas operacionais suportados para a versão 14.3 e anteriores:</p> <ul style="list-style-type: none"> • 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 <p>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).</p>
Ambientes gráficos da área de trabalho	<p>Você pode usar os seguintes ambientes gráficos da área de trabalho para exibir o cliente do Symantec Endpoint Protection:</p> <ul style="list-style-type: none"> • KDE • Gnome • Unity <p>O Symantec Agent for Linux 14.3 RU1 não tem uma interface gráfica.</p>

Componente	Requisitos
Outros requisitos ambientais (14.3 MP1 e anteriores)	<ul style="list-style-type: none"> • 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 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 <code>sudo</code>: <ul style="list-style-type: none"> – Para distribuições com base em Red Hat: <code>sudo yum install glibc.i686 libgcc.i686 libX11.i686 libnsl.i686</code> – Para distribuições com base em Debian: <code>sudo apt-get install ia32-libs</code> – Para distribuições com base em Ubuntu: <pre>sudo dpkg --add-architecture i386 sudo apt-get update sudo apt-get install gcc-multilib libx11-6:i386</pre>

[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 para o banco de dados do Microsoft SQL Server Express, versão 14.3 RU1. As atualizações do 12.1.6 MP9 e anteriores para a versão 14.3 RU1 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)

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
- 14.3, 14.3 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
- 14.2, 14.2 MP1
- 14.2 RU1, 14.2 RU1 MP1
- 14.2 RU2, 14.2 RU2 MP1
- 14.3, 14.3 MP1

NOTE

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

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

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 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 o upgrade 12.1.6 MP7 para 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 compatível.
- 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 site
Versões de teste	Entre em contato com o representante da sua conta.
Atualizações de manuais e documentação	<ul style="list-style-type: none"> • 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 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

